Telecommunications and Information Assurance: America's Achilles' Heel?

Paul F. Capasso

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

Telecommunications and Information Assurance: America's Achilles' Heel?

Paul F. Capasso
March 1997, P-97-1

Project Director
Anthony G. Oettinger

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

Paul F. Capasso is currently the Assistant Executive Officer to the Chief of Staff, United States Air Force. His previous positions in the Air Force have been in the field of Communications–Computers. This report was prepared while he was serving as an Air Force National Defense Fellow with the Program in 1995–96.

 ISBN 1-879716-40-2

Printing 5 4 3 2 1

March 1997

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Apple Computer, Inc.
AT&T Corp.
Australian Telecommunications Users Group
Bell Canada
BellSouth Corp.
The Boeing Company
Cable & Wireless (U.K.)
Carvajal S.A., (Colombia)
Center for Excellence in Education
Centro Studi San Salvador, Telecom Italia (Italy)
CIRCIT (Australia)
The College Board
Commission of the European Communities
Computer & Communications Industry Assoc.
CSC Index (U.K.)
CyberMedia Group
DACOM (Korea)
Deloitte & Touche Consulting Group
ETRI (Korea)
European Parliament
FaxNet Corp.
First Data Corp.
France Telecom
Fujitsu Research Institute (Japan)
GNB Technologies
Grupo Clarin (Argentina)
GTE Corp.
Hitachi Research Institute (Japan)
IBM Corp.
Investment Company Institute
Knight-Ridder Information, Inc.
Korea Mobile Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Lincoln Laboratory, MIT
John and Mary R. Markle Foundation
Microsoft Corp.
MicroUnity Systems Engineering, Inc.
MITRE Corp.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
The New York Times Co.
Nippon Telegraph & Telephone Corp. (Japan)
NMC/Northwestern University
NYNEX
OSCOM Communications, Inc.
Pacific Bell
Pacific Bell Directory
Pacific Telesis Group
The Post Office (U.K.)
Research Institute of Telecommunications and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
Scaife Family Charitable Trusts
Scientific-Atlanta, Inc.
Siemens Corp.
Sprint Communications Co. L.P.
State of California Public Utilities Commission
Strategy Assistance Services
TRW, Inc.
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency

United States Postal Service
Venturist, Inc.
Viacom Broadcasting
VideoSoft Solutions, Inc.
Weyerhaeuser

Acknowledgements

The author gratefully acknowledges the following people who reviewed and commented critically on the draft version of this report. Without their consideration, input, and encouragement, this study could not have been completed:

Raymond M. Alden
William B. Black, Jr.
Dan Caldwell
Alan D. Campen
Tom Fuhrman
James J. Hearn
Ethan B. Kapstein
Martin C. Libicki
John C. Ruess
Frank M. Snyder
Paul A. Strassmann

These reviewers and the Program's affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

For last-minute assistance, special thanks to John A. Collins, of the Reference Department of the Harvard University Libraries, and to Professor Robert D. Blackwill and his assistant, Jennifer Powell, at the John F. Kennedy School of Government at Harvard.

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the Department of Defense, the U.S. Air Force, or any other governmental agency or department.

Executive Summary

Cyberspace...Information Warfare...InfoSpace...Net War...Battlespace Dominance... Cyber War.... Vast technological changes within the United States's business complex have opened the doors to new interpretations of the art of warfare. The quest for information dominance has taken on increased meaning as major power brokers try to define how to exist and survive in the reality of an information-based society.

As an information-dependent society, the United States must be prepared to deal with the broad range of potential issues surrounding information warfare which cut across every aspect of society. To provide effectively for a national level defense against the threat of information warfare, the government must come to terms on who is in charge of emergency telecommunications policy in the event of an attack on the information infrastructure, which requires dealing with the following issues:

- The United States needs to adopt a states-first approach to resolving issues of information assurance. The Communications Act of 1934, as reinforced by the Telecommunications Act of 1996, gives the states the right to proceed in these matters. Private and public interests demand state involvement in the development of an information assurance policy.

- The U.S. could look toward the Basle Concordat and Basle Accord, developed for the financial world, as a starting point to provide such a states-first approach.

- The U.S. needs to adopt a crisis prevention, as opposed to crisis management, policy for dealing with information assurance issues.

- The U.S. needs to create a full-time team to oversee the government's information assurance efforts within the executive branch. With the creation of such a team, the National Security Telecommunications Advisory Committee (NSTAC) could be moved out of the Department of Defense and placed within this core team. The team could be made responsible for providing states with information about the threat of information warfare, resolving issues of the uses for and the effectiveness of measures to protect information resources. It could also act as a clearinghouse for information about technological issues potentially useful to protect U.S. information resources.

Contents

Chapter One

Emergency Telecommunications: A Piece of the Information Warfare Puzzle

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

— Niccolo Machiavelli[1]

Cyberspace...Information Warfare...InfoSpace...Net War...Battlespace Dominance... Cyber War.... Vast technological changes within the United States's business complex have opened the doors to new interpretations of the art of warfare. The quest for information dominance has taken on increased meaning as major power brokers try to define how to exist and survive in the reality of an information-based society.

> We have moved into an era of strategy that is very different to what was assumed by the advocates of air-atomic power—the "revolutionaries" of the past era. The strategy now being developed by our opponents is inspired by the dual idea of evading and hamstringing superior air-power. Ironically, the further we have developed the "massive" effect of the bombing weapon, the more we have helped the progress of this new guerrilla-type strategy.[2]

Liddell Hart's words are truer in 1996 than they were when he wrote them in 1954. The United States's technological advantages on the battlefield have unleashed the development of new warfighting strategies by its enemies. As the Chief of Staff of the United States Air Force, General Ronald R. Fogleman, stated in December 1995:

> Given our success in the Gulf War, we can expect a shrewd foe to attack our information systems and data bases as a means to undercut our technological advantages. Such an adversary would likely be able to recruit a small cell of experienced computer and software engineers to launch such an attack. These could be individuals who are looking to make a buck, or who have an axe to grind within the U.S. And they could make themselves extremely difficult to detect by our traditional intelligence systems.[3]

The successful use of land, sea, and airpower in the Gulf War, with its information-based underpinnings, earned a place in history and offered a new interpretation of the traditional

---

[1]*The Wit and Wisdom of Politics*, compiled by Chuck Henning (Golden, Colo.: Fulcrum Press, 1992), 102.

[2]Basil Liddell Hart, *Strategy* (N.Y.: Meridian, 1991 rpt.; 2nd rev. ed., 1929, 1967), xix.

[3]"Information Warfare Squadron Stands Up," *Policy Letter Digest*, Policy Issues and News from the Office of the Secretary of the Air Force, Dept. of the Air Force, December 1995, 4.

American way of war—mass on mass. "By leveraging *information*, U.S. and allied forces brought to warfare a degree of flexibility, synchronization, speed and precision heretofore unknown."[4]

Traditionally, the U.S. Armed Forces, working in close cooperation with other executive agencies, have had the primary responsibility for providing for national defense. Throughout the two hundred year history of the United States, this structure has proved sufficient to meet all threats to national security. Information-based warfare, however, is changing the assumptions and rules upon which this defense structure is built. The United States can no longer assume that its geographical location provides sanctuary from a possible enemy, just as it can no longer assume it can identify who might or might not, in the realm of information warfare, become an enemy. Certainly, since World War II it can no longer assume that only military targets will be the source of opportunity for its enemies. Information warfare could strike at any time, at any place, without warning. The traditional rules of engagement have been altered.

As an information-dependent society, the United States must be prepared to deal with the possibility and consequences of an attack on its information infrastructure. The broad range of potential issues surrounding information warfare cuts across every aspect of society. From constitutional rights to national security to foreign relations to domestic policy, in early 1996 discussions were taking place at all levels of government on how to address these diverse issues.

To provide effectively for a national level defense against the threat of information warfare, the government must, in particular, come to terms on who is in charge of emergency telecommunications policy in the event of an attack on the information infrastructure. As of the mid-1990s, the job of providing emergency telecommunications support during times of need is scattered among several government agencies and is, as always, the product of past decisionmakers' personalities, societal expectations, government policies, and world politics. Is this present organizational structure adequate to handle an information attack on U.S. society? Will this scattering of authority be in the best interests of the country for providing emergency assistance during times of need? Might it cause communications and restoration problems during emergencies and natural disasters? This report examines the requirement for a national level defense effort against threats of information warfare. Although the possibility of information warfare may threaten many aspects of society, including electrical power, transportation, financial services, and energy supplies, telecommunications is the vital link

---

[4]Alan D. Campen, Contributing Editor, *The First Information War* (Fairfax, Va.: AFCEA International Press, 1992), ix.

they share. For that reason, the focus of this report is on telecommunications, rather than all the aspects.

After looking at where the United States has been, where we are today, and after analyzing the effects of previous decisions, the report describes a framework for thinking about how the United States could organize its efforts to meet the future defense challenges of information warfare.

Chapter Two

Where We Have Been: The History of a Policy

A generation which ignores history has no past—and no future.
— Robert A. Heinlein[1]

To understand the evolution of the United States's emergency telecommunications policy requires stepping back to the birth of the telephone in 1875 and of the radio in 1896. Not even Alexander Graham Bell or Marchese Guglielmo Marconi could possibly have foreseen the effects their inventions would have on the development of a national telecommunications policy. Although the telegraph was extensively used during the American Civil War, the history of U.S. telecommunications policy "begins in the dawn of the federal regulatory era, with the Interstate Commerce Act of 1887, and embraces numerous major amendments to that act over the next fifty years. To complicate matters, most of the provisions that came to govern telephone-telegraph services were not designed for communication services but for the railroads."[2]

2.1 Before World War I

For both the radio and the telephone industries, the demands of the public and competition, as well as the expiration of patents, spawned the need for telecommunications policy. According to Arthur Holcombe, an instructor at Harvard in 1911:

> competition in the telephone business has existed for a score of years in a large part of the United States. By the expiration of the fundamental telephone patents in 1893 the legal barrier to active telephone competition was removed, and to the American public at that time competition seemed the promptest and most effective method of regulating the then existing telephone monopoly.[3]

The first modern military occurrences of information warfare in the United States probably occurred with the disruption and cutting of telegraph lines during the Civil War. As the information infrastructure of the United States grew, so too did the threat of war against information. An early example, although only a prank, suggested what could happen. In

---

[1]*The Wit and Wisdom of Politics*, compiled by Chuck Henning (Golden, Colo.: Fulcrum Press, 1992), 95.

[2]Max D. Paglin, ed., *A Legislative History of the Communications Act of 1934* (N.Y.: Oxford University Press, 1989), 5.

[3]Carol L. Weinhaus and Anthony G. Oettinger, *Behind the Telephone Debates* (Norwood, N.J.: Ablex Publ. Corp., 1988), 5.

1878, during the Bell company's first year of operation, teenage boys hired as telephone operators often "played clever tricks with the switchboard plugs: disconnecting calls, crossing lines so that customers found themselves talking to strangers and so forth."[4] Although such incidents were perhaps the result of a "combination of power, technical mastery and effective anonymity,"[5] it was not until 1909 that the first truly national emergency telecommunications policy was legislated. At that time, the significance of the telecommunications infrastructure began to take shape, and Congress made it a crime to injure or destroy or otherwise interfere with any means of communication owned by the United States or used for the country's military or civil defense functions.

> Whoever willfully or maliciously injures or destroys or attempts willfully or maliciously to injure or destroy any of the works, property, or material of any radio, telegraph, telephone, or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, shall be fined under this title or imprisoned not more than ten years or both.[6]

The first attempt by the federal government to regulate the telephone industry came in 1910, with the Mann-Elkins Act. The Act amended the Interstate Commerce Act of 1887 and provided the Interstate Commerce Commission (ICC) jurisdiction over interstate rates charged by the telephone, telegraph and undersea cable industries. Given the infancy of telecommunications technology, this Act made no provision for a national emergency telecommunications policy.

Although the importance of radio for general emergency purposes was realized as early as 1906, during the San Francisco earthquake, when the *U.S.S. Chicago* interconnected her radio equipment with that of local Army signal units and transmitted emergency communications up and down the Pacific coast,[7] "early radio legislation was strongly colored by the

---

[4]Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (N.Y.: Bantam Books, 1992), 14.

[5]Ibid., 14.

[6]18 U.S.C., §1362, 116.

[7]Thomas E. Will, *Telecommunications Structure and Management in the Executive Branch of Government, 1900-1970* (Boulder: Westview Press, 1978), 3.

only significant use for wireless telegraphy then conceived—safety on the high seas."[8] The Wireless Ship Act of 1910 required installation of radio communication equipment on all passenger vessels carrying fifty or more people:

> ...it shall be unlawful for any ocean-going steamer of the United States, or of any foreign country, carrying passengers and carrying fifty or more persons, including passengers and crew, to leave or attempt to leave any port of the United States unless such steamer shall be equipped with an efficient apparatus for radio-communication,...which apparatus shall be capable of transmitting and receiving messages over a distance of at least one hundred miles, night or day....[9]

Congress, in an effort to "carry out treaty obligations and to meet public sentiment aroused by the sinking of the *Titanic*,"[10] passed the Radio Act of 1912, which included the 1910 safety provision and as well as other provisions that strengthened the responsibility of the Secretary of Commerce and Labor for enforcing shipboard radiocommunications by providing for a licensing provision for all radio stations. The Radio Act also gave the president a new emergency authority:

> Every such license shall provide that the President of the United States in time of war or public peril or disaster may cause the closing of any station for radio communication and the removal therefrom of all radio apparatus, or may authorize the use or control of any such station or apparatus by any department of the government, upon just compensation to the owners.[11]

Regulation of the radio industry occurred for many of the same reasons as regulation of the telephone industry:

> Until the outbreak of World War I, practically all radio equipment in use in this country had been manufactured by or leased from British Marconi, Ltd., which by United States treaty agreement held all important radio patents.... With the advent of war, therefore, all such broadcast equipment and manufacturing outlets were seized, and under a subsequent governmental program of scientific development...great

---

[8]John M. Kittross, ed., *Administration of American Telecommunications Policy*, Vol. 1 (N.Y.: Arno Press, Collection of Historical Studies in Telecommunications, 1980), 1.

[9]Stat. 7021, Chapter 379 (1910), 629-630.

[10]Kittross, 1.

[11]Stat. 6412, Chapter 287 (1912), 303.

> technical strides resulted in so many new inventions that the radio monopoly held by British Marconi was broken up at the war's end.[12]

2.2 U.S. Entrance into World War I

When relations with Germany were severed in April 1917, President Woodrow Wilson, by proclamation, commandeered all wireless radio stations in the United States and its possessions. Radio authority was formally recognized legislatively, with passage by Congress on July 16, 1918, of Public Resolution No. 38, which authorized executive control of all of the country's telecommunications systems in the event of war[13]:

> That the President during the continuance of the present war is authorized and empowered, whenever he shall deem it necessary for the national security or defense, to supervise or to take possession and assume control of any telegraph, telephone, marine cable, or radio system or systems, or any part thereof, and to operate the same in such a manner as may be needed or desirable for the duration of the war....[14]

This resolution remained in effect until August 1, 1919, when the operation of the country's telecommunications systems reverted to civilian control:

> Between July 31, 1918, and August 1, 1919, all the wire communications facilities in the nation were under Government control and operation.... This authority was exercised by an executive order dated July 22, which placed the Postmaster General in charge of the program and empowered him to perform the duties vested in him through the officers and directors of the various companies under federal control.[15]

Although short-lived, the resolution marked the beginning of the United State's first attempts to build a national emergency telecommunications policy.

> The wartime operation of communications system might well have been an important step towards a reasoned national communications policy. But in fact it was merely a brief, unrelated hiatus in the haphazard accumulation of *ad hoc* legislation made to substitute for policy. A few hours of cursory debate sufficed to hand over to the Executive all the country's facilities for rapid communication. Brief hearings followed by

---

[12]Robert Sears McMahon, *Federal Regulation of the Radio and Television Broadcast Industry in the United States in the United States 1927-1959* (N.Y.: Arno Press, 1979), 24-25.

[13]Will, 5.

[14]H.R.J. 309, 65th Congress, 2d Sess. (1918), 904.

[15]"The Telegraph Industry: Monopoly or Competition," 51 Yale L. J., 1941-42 (New Haven: Yale Law Journal Company, Inc., 1942), 633.

> even less—as well as less relevant—debate marked the end of the experiment.[16]

Regulation of the telephone industry continued with passage of the Transportation (Esch-Cummins) Act of 1920, which again gave the ICC jurisdiction over the telephone, telegraph, and cable companies, and with the Willis-Graham Act (1921), which increased the authority of the ICC in regulating the telecommunications industry. Neither act made any emergency telecommunications policy.

2.3 Between the Wars: 1922–1940

After World War I, as the radio industry grew, the licensing provisions of the Radio Act of 1912 were no longer sufficient to meet increased demands. In 1922, the Interdepartmental Radio Advisory Committee (IRAC) was organized to assist the president in carrying out responsibilities under the Radio Act of 1912. However, the industry continued to grow, and so the did the perceived need for additional regulation.

The Radio Act of 1927 created the Federal Radio Commission, to oversee the licensing provisions, and, like the wartime resolution (see section 2.2), this Act again included, as an outgrowth of the lessons learned during the war, an emergency telecommunications policy that provided presidential authority, during times of war, to suspend or amend rules and regulations applicable to all radio stations to preserve the neutrality of the United States:

> Upon proclamation by the President that there exists war or a threat of war or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations within the jurisdiction of the United States as prescribed by the licensing authority, and may cause the closing of any station for radio communication and the removal therefrom of its apparatus and equipment, or he may authorize use or control of any such station and/or its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners.[17]

"During the first year of the Roosevelt administration [1933], the idea of a unified communications agency was rejuvenated as part of studies of national communications policy

---

[16]Ibid., 636, 637.

[17]H.R.J. 9971, 69th Congress, 2d Sess. (1927), 1165.

by both the administration and Congress."[18] The Study of Communications, to assess the need for a single governing body in the area of telecommunications, was undertaken by an Interdepartmental Committee headed by Daniel C. Roper, and it was the beginning of what was to become the Communications Act of 1934. As a result of it, in a letter to Congress dated February 26, 1934, President Roosevelt emphasized the need for a single government agency to manage the field of communications and recommended the creation of the Federal Communications Commission (FCC) to inherit the responsibilities for the telecommunications industry that were then vested in two different federal agencies, the Interstate Commerce Commission and the Federal Radio Commission:

> I have long felt that for the sake of clarity and effectiveness the relationship of the Federal Government to certain services known as utilities should be divided into three fields: Transportation, power and communications. The problems of transportation are vested in the Interstate Commerce Commission, and the problems of power, its development, transmission, and distribution, in the Federal Power Commission. In the field of communications, however, there is no single Government agency charged with broad authority. The Congress has vested authority over certain forms of communications in the Interstate Commerce Commission and there is in addition the agency known as the Federal Radio Commission. I recommend that the Congress create a new agency to be known as the Federal Communications Commission...to be vested with the authority now lying in the Federal Radio Commission and...the Interstate Commerce Commission—the services affected to be all of those which rely on wires, cables, or radio as a medium of transmission.[19]

As a result of the Navy Department's strong participation in the Study of Communications and its key congressional testimony during the discussions preceding passage of the Communications Act of 1934, the final version of the Act provided the president with the necessary powers to obtain required telecommunications support during war or other national emergencies:

> ...the Navy department believes in national emergency it might become fully as necessary for communication by wire and cable to be administered by the President as it is now authorized for communication by radio. There can be no doubt that control of communications by the Executive is a power which he must necessarily exercise for the public welfare in the time of national emergency. This was proven in the World War. We cannot afford delay on the outbreak of war. To do so

---

[18]Guy Hamilton Loeb, *The Communications Act Policy Toward Competition: A Failure to Communicate* (Cambridge, Mass.: Program on Information Policy Resources, P-77-3, October 1977), 29.

[19]Paglin, 99.

> may mean disaster. We cannot say now that we may give him this power as soon as conditions may appear to be forcing us into war. To pass such an act then would be probably be forcing us into war. To pass such an act then would probably be construed by the other power as an unfriendly act on the part of the representatives of our whole people. It would have far more weight in the minds of a possible adversary than would a precautionary proclamation by the President that a state of public peril existed, and might precipitate hostilities.[20]

The authority given to the president allowed the government to take priority over other users of telecommunications assets to satisfy defense needs in times of emergencies:

> During the continuance of a war in which the United States is engaged, the President is authorized, if he finds it necessary for the national defense and security, to direct that such communications as in his judgement may be essential to the national defense and security shall have preference or priority with any carrier subject to this Act.[21]

It also allowed the use of the armed forces to prevent any obstruction or retardation of communications:

> The President is hereby authorized, whenever in his judgement the public interest requires, to employ the armed forces of the United States to prevent any such obstruction or retardation of communication.[22]

And, finally, it allowed the suspension of the rules and regulation by the FCC and authorization to use or control any company or equipment by any department of the government with just compensation to its owners:

> Upon proclamation by the President that there exists war or a threat of war or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communication and the removal therefrom of its apparatus and equipment, or he may authorize use or control of any such station and/or its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners.[23]

---

[20]H.R. 8301, "A Bill to Provide for the Regulation of Interstate and Foreign Communication by Wireless or Radio, and for Other Purposes, Hearings Before the [House] Committee on Interstate and Foreign Commerce," 73rd Cong., 2d Sess. (April 10, 1934), 22.

[21]Stat. 3285, Chapter 652 (1934), 1104.

[22]Ibid.

[23]Ibid., 1104-1105.

In testimony before the House Committee on Interstate and Foreign Commerce, the Department of the Navy asked for a National Communication Advisory Council to develop broad national communications policy:

> Inasmuch as there is a very close relationship, insofar as availability of facilities concerned, between the departments of the Government operating their communication systems, such as the Army, Navy, Coast Guard and the Airways Division, and the organizations, both domestic and international, which operate public service communication systems, it would seem advisable to establish a national communication advisory council consisting of representatives, appointed by the President, from the various interested Government departments, including the Department of State. This National Advisory Council, together with the civil body responsible for the administration of civil communications, would be charged primarily with the formulation of policies.[24]

But the provisions requested by the Navy were not included in the final bill.

In time, President Roosevelt came to regard the FCC as inadequate in carrying out its responsibilities, as highlighted in a letter of 1939:

> Although considerable progress has been made as a result of efforts to reorganize the work of the Federal Communications Commission under existing law, I am thoroughly dissatisfied with the present legal frame-work and administrative machinery of the Commission. I have come to the definite conclusion that new legislation is necessary to effectuate a satisfactory reorganization of the commission. New legislation is also needed to lay down clearer congressional policies on the substantive side—so clear that the new administrative body will have no difficulty in interpreting and administering them.[25]

In spite of his concerns, the Federal Communications Act of 1934 remained basically unchanged until 1952, when Congress passed the McFarland Amendment. Although "the McFarland Amendments to the Communications Act of 1934 (S. 658) were the result of ten years of congressional effort to improve upon [it], they were to a very large degree procedural in character...and dodged the more important issues involving fundamental weaknesses in the administration of the law by the Commission [FCC] and needlessly hampered the Commission in the performance of certain of its functions."[26]

---

[24]H.R. 8301, "A Bill to Provide for the Regulation of Interstate and Foreign Communication by Wireless..." (April 10, 1934), 34.

[25]*The Public Papers and Addresses of Franklin D. Roosevelt, With a Special Introduction and Explanatory Notes by President Roosevelt*, 1939 Volume, War—and Neutrality (N.Y.: Macmillan, 1941), 96.

[26]McMahon, 216-217.

2.4 From World War II through the Korean War

In September 1940, against the background of World War II, President Roosevelt signed Executive Order 8546, creating the Defense Communications Board, which in June 1942, under Executive Order 9183, became the Board of War Communications. The purpose of this board was to coordinate the most efficient use of the nation's communications assets in a national emergency, which included the following functions:

> ...to determine, coordinate, and prepare plans for the national defense, which plans will enunciate for and during any national emergency a) the needs of the armed forces of the United States, of other governmental agencies, of industry, and of other civilian activities for radio, wire, and cable communication facilities of all kinds. b) the allocation of such portions of governmental and non-governmental radio, wire, and cable facilities as may be required to meet the needs of the armed forces, due consideration being given to the needs of other governmental agencies, of industry, and of other civilian activities and c) the measures of control, the agencies to exercise this control, and the principles under which such control will be exercised over non-military communications to meet defense requirements.[27]

The board was composed of the Chairman, FCC, the Chief Signal Officer of the Army, the Director of Naval Communications, the Assistant Secretary of State in charge of the Division of International Communications, and the Assistant Secretary of the Treasury in charge of the Coast Guard. The board was dissolved on February 24, 1947, following the end of the War, and all its records were transferred to the FCC.

In an effort to better the position of United States in the international community with regard to the allocation of frequencies worldwide and because of the "inability of existing organizations to resolve competing requirements of FCC on behalf of non-government users and government agencies for high frequencies,"[28] Executive Order 10110 (Feb. 17, 1950) established the President's Communications Policy Board (PCPB) to study and make recommendations on the telecommunications policies and practices to be followed by the federal government in order to meet the needs of the public. This mandate included policies regarding

> the most effective use of radio frequencies by governmental and nongovernmental users and alternative administrative arrangements in the Federal Government...international radio and wire communications... and the relationship of Government communications to non-

---

[27]Exec. Order No. 8546, 3C.F.R. (1938-1943), 741-742.

[28]Will, 43.

> government communications and related policy matters as the Board may determine.[29]

Upon the recommendation of the PCPB, Executive Order 10297 (Oct. 9, 1951) was issued, which created the position of Telecommunications Advisor to the President. Located within the Executive Office, the duties of this position included assisting and advising the president about telecommunications matters relating to policy and standards, the assignment and development of frequency requirements, and emergency telecommunications plans and programs during times of emergencies.

> Coordinating the development by the several agencies of the executive branch of telecommunications plans and programs designed to assure maximum security to the United States in time of national emergency with a minimum interference to continuing nongovernmental requirements.[30]

In December 1951, during the Korean War, President Truman invoked emergency telecommunications authority under the Communications Act of 1934 and, by Executive Order 10312, created CONELRAD (Control of Electromagnetic Radiation), an emergency radio communications plan to meet the national security and defense needs. The purpose of CONELRAD was to control the emanations of electromagnetic radiation that could aid the enemy in its use of navigation and missile systems. In the event of hostile activity, radio stations were to switch to predesignated frequencies to pass civil defense information to the public.

Two years later, however, President Eisenhower abolished the position of Telecommunications Advisor to the President with the issuance of Executive Order 10460 (June 16, 1953) and assigned its functions to the Director of the Office of Defense Mobilization. Although all of the duties previously outlined in Executive Order 10297 were transferred to the new position, the accomplishment of these duties "resulted in the execution of the President's telecommunications functions being placed four echelons below the President."[31]

---

[29]Exec. Order No. 10110, 3 C.F.R. (1949-1953), 302.

[30]Exec. Order No. 10297, 3 C.F.R. (1949-1953), 828.

[31]Will, 44.

2.5 Crisis on the Home Front: The 1960s

In June 1961, the Federal Telecommunications System was established, to serve the day-to-day telecommunications needs of the civilian government agencies and to provide engineering support during emergencies. The General Services Administration (GSA) was given the responsibility of administering the system.

In September 1961, Section 1362 of Title 18 of the United States Code, which had come into effect in 1909, was amended to protect the internal security of the telecommunications systems further by providing for stiffer penalties for malicious damage to certain communications systems. The 1909 version of the law had not specified dollar amounts for potential fines, but the amendment specified fines of up to $10,000 for malicious acts against the U.S. telecommunications system.

World War II and the birth of the nuclear age had changed the way emergency telecommunications policy was to be managed and structured in the future. As the need for more involvement in foreign affairs became an integral part of providing for the security and welfare of the United States, so, too, the need for reliable and timely telecommunications. During the Kennedy administration, in an effort to provide and "maintain for an efficient and well planned national and international telecommunications program,"[32] Executive Order 10995 (Feb. 16, 1962) established the position of Director of Telecommunications Management (DTM), which was to be held by an Assistant Director in the Office of Emergency Planning (OEP). Administrative Order No. 42 (June 15, 1962) incorporated the new Office of Telecommunications Management (OTM) into the OEP. "The OTM placement under the OEP made visibility minimal outside the executive branch."[33] Under Executive Order 11051, the Director of OEP was given responsibility to provide for emergency services outside the jurisdiction of other agencies:

> ...for the preparation of nonmilitary plans and preparedness programs with respect to organization and functioning of the Federal Government under emergency conditions and with the respect to specific areas of Federal activity necessary in time of war which are neither performed in the normal operations of the regular departments and agencies....[34]

In the area of telecommunications, this responsibility included activities for "planning for the mobilization of the nation's telecommunication resources in time of national emergency."[35]

---

[32]Exec. Order No. 10995, 3 C.F.R. (1959-1963), 536.

[33]Will, 99.

[34]Exec. Order No. 11051, 3 C.F.R. (1959-1963), 636.

[35]Ibid., 639.

"The Cuban Missile Crisis of October 1962 abruptly altered the communications priorities outlined in Executive Order 10995."[36] In light of procedural and technical delays in the delivery of a message to Soviet Premier Nikita Khrushchev during the crisis, President Kennedy directed a review of national security communications. "To provide the Director [of Telecommunications Management] with broader authority to accomplish this new high priority assignment, the President gave him an additional title of Special Assistant to the President for Telecommunications."[37]

In February 1963, the President signed Executive Orders 11092 and 11093, which assigned emergency telecommunications responsibilities to the FCC and the Administrator of General Services, respectively. Subject to the policy guidance of the Director of OEP, the FCC would

> prepare national emergency plans and develop preparedness programs covering provisions of service by the common carriers, broadcasting facilities, and the safety and special radio services; assignment of radio frequencies to Commission licensees; and the protection, reduction of vulnerability, maintenance, and restoration of facilities operated by its licensees in an emergency.[38]

The Administrator of General Services would "plan for and provide, operate and maintain appropriate telecommunications facilities designed to meet the essential administrative requirements of Federal civilian departments and agencies during an emergency."[39]

The result of a study by an Interdepartmental Committee on Communications was a Presidential Memorandum, "Establishment of the National Communications System," dated August 21, 1963, which directed the establishment of the National Communications System (NCS). The position of Director of OTM, created the previous year, was to be responsible for policy direction of the development and operation of the NCS, while the Secretary of Defense would be the Executive agent for the system. Efficient, redundant, and survivable communications, capable of meeting any challenge, became the goals of the Kennedy administration.

> The objective of the NCS will be to provide necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crises, including nuclear attack. The system will be developed and operated to be responsive to the variety of needs of the national command and user agencies and be capable of meeting priority requirements under

---

[36]National Communications System, *National Communications System: Thirty Years of Progress* [n.d.], 4.

[37]Ibid., 4.

[38]Exec. Order No. 11092, 3 C.F.R. (1959-1963), 734

[39]Exec. Order No. 11093, 3 C.F.R. (1959-1963), 737.

> emergency or war conditions through the use of reserve capacity and additional private facilities. The NCS will also provide the necessary combinations of hardness, mobility, and circuit redundancy to obtain survivability of essential communications in all circumstances.[40]

Under this memorandum, the Federal Telecommunications System was also placed under the direction of the NCS. This document was to play a key role in the future development of emergency telecommunications.

The concept of a unified communications system was fully endorsed by President Lyndon Johnson in 1964. His approval of the National Defense Plan for Emergency Preparedness, which called for a "unified governmental communications system, responsive to a single executive agent, derived from linking together, improving, and extending the communications facilities and components of the various Federal agencies,"[41] followed in the footsteps of the Kennedy administration.

2.6 Responses to the Threat of Nuclear War: The 1970s

"As the decade of the 1970s began, the great expectations of a 'unitary national system' evolving from a bold concept to a growing organization, cutting across Federal Agency lines, and [with] an effective and viable management structure as Defense Secretary McNamara had predicted in 1966, had not been realized."[42] Problems associated with the failure to obtain this unified system were highlighted by several agencies, including a Presidential Communications Task Force under President Johnson, a Bureau of Budget Report, and the General Accounting Office (GAO).

Under President Nixon, the White House provided the following assessment of the situation:

> There is no effective policy-making capability for telecommunications in the Executive Branch. The Administration is therefore largely unable to exert leadership or take initiatives.... [A]ttempts by the DTM to exercise leadership in communications policy have been largely ineffectual. The responsibilities and authority of the DTM are questioned by agencies with operating responsibilities. This situation results from a number of factors including organizational location, inadequate staff, and lack of clear authority.[43]

---

[40]Memorandum of Aug. 21, 1963, "Establishment of the National Communications System," 3 C.F.R. (1959-1963), 858.

[41]*National Communications System*, 9.

[42]Ibid., 16.

[43]Ibid., 17.

President Nixon's attempt to solve the telecommunications management problems such as those that had occurred in the past centered on two executive orders. Executive Order 11490, Assigning Emergency Preparedness Functions to Federal Departments and Agencies assigned emergency preparedness functions across the Federal government. The Director of the Office of Emergency Preparedness was given the responsibility of advising, assisting, developing, and coordinating with the President the national preparedness goals and policies. Emergency communications preparedness was shared by the DOD, the Department of Commerce, the FCC, and the GSA. In an emergency, to include an attack on the homeland, the DOD would "advise of existing communications facilities and furnish military requirements for commercial communications facilities and services."[44] In addition, during emergencies, it would work with other agencies in the area of air-traffic control management and control of electromagnetic radiation. It was to:

> [d]evelop with the Department of Transportation and the Federal Communications Commission plans and programs for the control of air traffic, civil and military, and develop with the FCC and the Office of Telecommunications Management plans and programs for the emergency control of all devices capable of emitting electromagnetic radiation.[45]

Further, the Department of Commerce became responsible for preparing national emergency plans and developing preparedness programs for the use of communication services and facilities[46]; the FCC became responsible for developing emergency policies, plans, and procedures covering common carrier, broadcasting and safety and special radio services, assignment of radio frequencies and closing of radio stations capable of emitting electromagnetic radiation[47]; while the GSA would "plan for and provide, operate, and maintain appropriate telecommunications facilities designed to meet the essential requirements of Federal civilian departments and agencies during an emergency within the framework of the National Communications System."[48]

In an effort to "be better equipped to deal with the issues which arise from telecommunications growth...and to speak with a clear voice and to act as a more effective partner in discussions of communications policy with both the Congress and the Federal

---

[44]Exec. Order. No. 11490, 3 C.F.R. (1966-1970), 825-826.

[45]Ibid., 826.

[46]Ibid., 832.

[47]Ibid., 847-848.

[48]Ibid., 849.

Communications Commission,"[49] President Nixon had abolished the positions of Director of the Office of Telecommunications Management and of Special Assistant to the President for Telecommunications and on September 4, 1970, under Executive Order 11556, Assigning Telecommunications Functions, replaced those positions with the Office of Telecommunications Policy (OTP). The Director of OTP became the president's principal advisor on telecommunications issues, again placing this function in the executive office. Although telecommunications policy issues were centralized in this office, other emergency action policies remained under the Office of Emergency Preparedness, thus fragmenting overall responsibilities for emergency action.

The OTP was abolished as a result of President Carter's Reorganization Plan under Executive Order 12046 (March 27, 1975), which appointed the Secretary of Commerce as the president's principal advisor on telecommunications policies and established the Assistant Secretary for Communications and Information under the Secretary of Commerce. Emergency telecommunications responsibilities were thus once again transferred to various functions within the executive branch, including the National Security Council (NSC), Office of Management and Budget (OMB), Department of Commerce, Department of State, GSA, and the Office of Science and Technology Policy. The DOD retained its responsibilities as the NCS executive agent and manager.

A June 1975 *Report to the President by the Commission on CIA [Central Intelligence Agency] Activities within the United States* indicated that communist countries had

> developed electronic collection of intelligence to an extraordinary degree of technology for use in the United States and elsewhere throughout the world, and...can monitor and record thousands of private telephone conversations.... This raises the real specter that selected American users of telephones are potentially subject to blackmail that can seriously affect their actions, or even lead in some cases to recruitment as espionage agents.[50]

In an effort to enhance communications security, PD/NSC-24,[51] Telecommunications Protection Policy, tasked "the Secretary of Commerce [to be] the Executive Agent for communications protection for government-derived unclassified information and for dealing

---

[49]*Public Papers of the Presidents of the United States: Richard Nixon, Containing the Public Messages, Speeches, and Statements of the President* (Washington, D.C.: U.S. Government Printing Office, 1971), 93-94.

[50]*Report to the President by the Commission on CIA Activities Within the United States*, Nelson A. Rockefeller, Chairman (N.Y. Manor Books, 1975), 8.

[51]Presidential Directive/National Security Council.

with the commercial and private sectors to enhance their communications protection and privacy."[52]

On July 19, 1979, President Carter, by Executive Order 12148, created the Federal Emergency Management Agency (FEMA), "to consolidate disparate agency programs under one central roof and to provide strong leadership focus and attention for emergency management activities."[53] The Director of FEMA was tasked to "establish Federal policies for, and coordinate, all civil defense and civil emergency planning, management, migration, and assistance functions of Executive agencies."[54] A civil emergency was defined under this Executive Order as "any accidental, natural, man caused, or war emergency or threat thereof, which causes or may cause substantial injury or harm to the population or substantial damage to or loss of property."[55] To ensure that civil defense planning remained in line with the nation's strategic policy, however, the Secretary of Defense and the NSC were assigned oversight authority over the Director of FEMA.[56] In addition, the Secretary of Defense was tasked to provide the Director of FEMA, to the extent authorized by law, with "support for civil defense programs in the areas of program development and administration, technical support, research, communications, transportation, intelligence and emergency operations."[57]

In November 1979, President Carter issued Presidential Directive 53, National Security Telecommunications Policy, which placed increased emphasis on the importance of interoperable and survivable communications to support continuity of government and all levels of potential contingencies, ranging from nuclear war to natural disasters. The objectives stressed the use of private industry to accomplish this policy:

> The National Communications System will consult with the Federal Communications Commission on implementing these principles and will place substantial reliance upon the private sector for advice and assistance in achieving national security and preparedness goals.[58]

---

[52]National Security Council Memorandum for the Chairman, Federal Communications Commission, Feb. 9, 1979.

[53]*Rebuilding FEMA: Preparing for the Next Disaster*, Hearings Before the Committee on Governmental Affairs, U.S. Senate, 103rd Congress, 1st Sess. (1993), 1.

[54]Exec. Order No. 12148, 3 C.F.R. (1979), 413.

[55]Ibid., 414.

[56]Ibid.

[57]Ibid.

[58]Presidential Directive/NSC-53, Nov. 15, 1979, 2.

2.7 The 1980s to the Present

In July 1982, National Security Decision Directive (NSDD) 47, Emergency Mobilization Preparedness, "directed the development of a credible and effective capability to harness the mobilization potential of America in support of the Armed Forces, while meeting the needs of the national economy and other civil emergency preparedness requirements."[59] This document specified twelve preparedness areas, including emergency communications, that should be developed to meet the United States's mobilization requirements. NSDD 47 called for adequate resources and funding, for identification and correction of communications deficiencies, for viable communications operations concepts, and for communications plans for the transition from normal to emergency operations.

A month later, on August 24, 1982, Judge Harold H. Greene approved the Modification of Final Judgement (MFJ) settlement of the federal antitrust suit against AT&T. This judgement marked the end of AT&T's monopoly, which had begun in 1876 and until 1982 had "swung like a pendulum between monopoly and competition."[60] The settlement required AT&T to divest itself of its operating companies, which formed new, wholly independent corporate entities, the regional Bell Operating Companies (RBOCs), or "Baby Bells," to provide subscriber interconnections and access to long-distance services. The United States's one-stop-shopping for telecommunications services was dismembered, again opening up a competitive marketplace for new companies to become part of the network that provides national emergency telecommunications support. "With the breakup of the Bell System, however, and the proliferation of telecommunications service providers, there was an urgent need to replace the old AT&T-Government accord for provisioning of emergency Government communications with a broad-based cooperative arrangement involving a number of service providers and equipment manufacturers."[61]

The establishment of the National Security Telecommunications Advisory Committee (NSTAC) became the president's focal point for developing National Security and Emergency Preparedness (NS/EP) telecommunications and for dealing with the breakup of the Bell system. Executive Order 12382 established the president's NSTAC, whose thirty members, representing the nation's telecommunications industry, provide the president and Secretary of Defense with

> information and advice from the perspective of the telecommunications industry with respect to the implementation of Presidential Directive 53

---

[59]Christopher Simpson, *National Security Directives of the Reagan and Bush Administrations: The Declassified History of the U.S. Political and Military Policy, 1981–1991* (Boulder: Westview Press), 1995), 171.

[60]Weinhaus and Oettinger, *Behind the Telephone Debates*, 5.

[61]*National Communications System*, 40.

> (PD/NSC-53), National Security Telecommunications Policy information and advice regarding the feasibility of implementing specific measures to improve the telecommunications aspects of our national security posture...technical information and advice in the identification and solution of problems which the Committee considers will affect national security telecommunications capability...and conduct reviews and assessments of the effectiveness of the implementation of PD/NSC-53, National Security Telecommunications Policy.[62]

NSDD 97, National Security Telecommunications Policy, rescinded Presidential Directive/NSC-53 in August 1983. The new directive called for a national telecommunications infrastructure based upon the fundamental characteristics of connectivity, redundancy, interoperability, restorability, and hardness to support the command and control of all U.S. military forces. It placed heavy demands on the telecommunications industry by requiring

> private telecommunications carriers (principally AT&T) to support... [U.S.] worldwide intelligence collection, threat assessment, military mobilization, and continuity of government programs through provision of communication links, technical consulting, and priority access to communications for government during emergencies.[63]

On April 3, 1984, President Reagan signed Executive Order 12472, "to provide for the consolidation of assignment and responsibility for improved execution of national security and emergency preparedness telecommunications functions."[64] This order created the National Communications System "to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy, and the Director of the Office of Management and Budget...in the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery and reconstitution."[65] NS/EP communications responsibilities were delegated to the Department of Commerce, FEMA, the Department of State, the DOD, the Department of Justice, the Central Intelligence Agency, GSA, and FCC. Superseding the notional Presidential Memorandum of 1963, this document actually offered "an organizational structure and technical path for creating a national security

---

[62]Executive Order 12382, President's National Security Telecommunications Advisory Committee, Sept. 13, 1982.

[63]Simpson, 237.

[64]Exec. Order No. 12472, 3 C.F.R. (rev. Jan. 1, 1985), 193.

[65]Ibid., 193-194.

and emergency preparedness telecommunications capability...to serve the Federal government under all circumstances."[66]

Also in 1984, President Reagan signed NSDD 145, National Policy on Telecommunications and Automated Information System Security, which appointed the Secretary of Defense as the Executive Agent and the Director of the National Security Agency (NSA) as the National Manager for national telecommunications and information systems security. This directive addresses safeguards for federal systems that process unclassified sensitive information. NSA became responsible for examining government telecommunications systems to evaluate system vulnerabilities, as well as for approving all standards, techniques, systems, and equipment for telecommunications and information security.

NSDD 188, Government Coordination for National Security Emergency Preparedness, signed in September 1985, established the NSC as the principal forum for consideration of NS/EP policy and shifted responsibilities for protecting facilities and resources essential to the national defense and national welfare to other federal departments and agencies. FEMA, which previously held this protection responsibility for all assets, was now to serve as a coordinator and advisory agency. In November 1988, this NSDD was turned into Executive Order 12656.

The passage of the Computer Security Act of 1987 (Jan. 8, 1988), which established the need for minimum acceptable technical, management, physical requirements for and administrative guidelines and standards to improve upon the security and privacy of sensitive information of federal computer systems, marked encroachment of the threat of information warfare beyond the bounds of the telecommunications arena and enlarged the United State's vulnerabilities. The act also established the Computer System Security and Privacy Advisory Board within the Department of Commerce, which was to be responsible for identifying emerging security trends and issues and safeguarding related information. Drawing on the advice of this Board, and the technical advice and assistance of the National Security Agency and through close coordination with other agencies (including but not limited to the DOD, GAO, OTA, OMB), responsibility for developing these standards was given to the National Bureau of Standards.[67] The Secretary of Commerce then became responsible for promulgating the standards throughout the federal government.

In April 1989, President Bush issued National Security Directive 1 (NSD-1), which appointed the NSC as "the principal forum for consideration of national security policy issues

---

[66]*National Communication System*, 33.

[67]101 Stat. 1724, Public Law 100-235, Jan. 8, 1988.

requiring presidential determination."[68] It also established the National Security Principals Committees (NSC/PC) for identifying and developing policy issues for consideration by the NSC. In 1989, he signed NSD 10, "Appointments to NSC Policy-Coordinating [PC] Committees," which established the National Security Telecommunications NSC/PC and the Emergency Preparedness/Mobilization Planning NSC/PC, to help in the development of policy issues.

Since the beginning of the twentieth century the management of NS/EP functions has varied from presidency to presidency, and medium to medium, but, as will be clear in the next chapter, it continues to reside in the "top-down" channel. Placement of the NS/EP management within an administration was a direct result of political, social, environmental and economic forces, both on the home front and abroad, with little regard for policies already in place. The quest for an effective and efficient NS/EP system continues today.

---

[68]Simpson, 903.

Chapter Three

Where We Are Now: Status Quo

A virtual alphabet soup of government agencies.
— Kimberly Patch[1]

In the mid-1990s, according to Fred Cate, Associate Professor of Law at Indiana University, "no single agency is vested with primary jurisdiction or responsibility for coordinating information policymaking."[2] Instead:

> information policymaking in the United States involves every cabinet department, more than 100 Executive Branch and independent agencies, two dozen Congressional committees, subcommittees and expert advisory bodies, the federal courts, 51 state utilities commissions, and literally thousands of local regulators. These figures include none of the international policymaking institutions (e.g., International Telecommunications Union, World Intellectual Property Organization), domestic standard-setting bodies (e.g., American National Standards Institute, Institute of Electrical and Electronics Engineers), public interest groups (e.g., Action for Children's Television, Media Access Project), research centers (e.g., The Annenberg Washington Program in Communications Policy Studies, Columbia Institute for Tele-Information), or the many private industry associations (e.g., Information Industry Association, Telecommunications Industry Association), which all seek to influence the shape of the government's information policy.[3]

The emergency telecommunications policy of the Clinton administration is found in Title 47 of the Code of Federal Regulations, the centerpiece of which remains Executive Order 12472, signed by President Reagan in 1984. In a time of need, the "Federal Government is responsible for [emergency telecommunications] resources mobilization, including determination of the need for and the extent of mobilization necessary in all crises and emergencies, wartime and non-wartime."[4] At the same time, it would rely on "State governments and their telecommunications management organizations for management or control of intrastate carrier services and continuity of interconnectivity with interstate carriers

---

[1]Fred H. Cate, "The National Information Infrastructure: Policymaking and Policymakers," in *The Information Revolution*, edited by Donald Altschiller (N.Y.: H.W. Wilson, The Reference Shelf, Vol. 67, No. 5, 1995), 151.

[2]Ibid.

[3]Ibid., 155.

[4]Code of Federal Regulations, Title 47, (Washington, D.C.: U.S. Gov't Printing Office, 1994), 641.

to assure that national objectives and priorities are properly served."[5] For executive branch responsibilities under both wartime and nonwartime emergencies, both the Director of the Office of Science and Technology Policy and the National Security Advisor (also Assistant to the President for National Security Affairs) play key roles in the preparation and execution of plans for telecommunications policy. In the event of wartime emergencies, the Assistant to the President for National Security Affairs "shall provide general policy direction for the exercise of the war power functions of the President,"[6] while the Director of the Office of Science and Technology Policy "shall direct the exercise of the war power functions of the President."[7]

During nonwartime emergency functions, the National Security Advisor

> shall advise and assist the President in coordinating the development of policy, plans, programs and standards within the Federal Government for the identification, allocation and use of the Nation's telecommunications resources by the Federal Government, and by State and local governments, private industry and volunteer organizations...[8] [and] provide policy oversight and the direction of the activities of the NCS.[9]

Also, the Director of the Office of Science and Technology Policy, through the use of a Joint Telecommunications Resources Board,

> shall provide information, advice, guidance and assistance, as appropriate, to the President and to those Federal Departments and agencies with responsibilities for the provision, management or allocation of telecommunications resources.[10]

In addition, planning and oversight responsibilities are further delegated to the Director of the OMB, the Secretary of Commerce, the Director of FEMA, the Secretary of State, the Secretary of Defense, the Attorney General, the Director of the CIA, the Administrator of General Services, the Secretary of the Interior, the FCC, the National Communications System, the Executive Agent for the NCS, the Manager of the NCS, the NCS Committee of Principals, and all federal departments and agencies.

---

[5]Ibid., 641-642.

[6]Ibid., 644-645.

[7]Ibid., 645.

[8]Ibid.

[9]Ibid.

[10]Ibid.

Another crucial aspect of the Clinton administration's telecommunications policy lies in its *Agenda for Action*[11] and the call for the development of the National Information Infrastructure (NII). To oversee implementation of the NII, Vice-President Gore formed the Information Infrastructure Task Force (IITF), to look into technical, legal, security, and policy areas pertinent to the NII.

Through Executive Order 12864, President Clinton created the United States Advisory Council on the NII. Within the Department of Commerce, this panel of twenty-five members, drawn from industry, state and local governments, and public interest groups, reports through the Secretary of Commerce and is responsible for providing advice "on a national strategy for promoting the development of a National Information Infrastructure which includes issues regarding national security, emergency preparedness, system security and network protection implications."[12]

As a result of the Joint Security Commission Report *Redefining Security* (Feb. 28, 1994), President Clinton directed the establishment of a new security policy structure, under the NSC, for the coordination, formulation, evaluation, and oversight of security policy.

> The Commission unanimously believes that the fragmentation of the security policy structure is the prime cause of the problems associated with security policies, practices, and procedures and that no substantive and long-term improvements can be achieved without a unifying structure to provide leadership, focus, and direction to the government security communities.... US Government security policies and practices have evolved in an ad hoc manner over the last four decades.... This piecemeal approach to security policy has led to a decentralized policy structure in which multiple groups with different interests and authorities work independently of one another.... The process is slow and some people never seem to get the word...there is no effective mechanism to look across government to ensure that security policy is being implemented properly, if at all.[13]

Presidential Decision Directive (PDD) 29 created the Security Policy Board, which consists of the Director of Central Intelligence, the Deputy Secretary of Defense, the Vice-Chairman of the Joint Chiefs of Staff, the Deputy Secretary of State, the Under Secretary of Energy, the Deputy Secretary of Commerce, the Deputy Attorney General, one Deputy Secretary from another non-defense related agency, one member from the OMB and the NSC

---

[11]*The National Information Infrastructure: Agenda for Action*, Report published by Executive Office of the President (Washington, D.C., 1993).

[12]Exec. Order. No. 12864, 3 C.F.R. (1993), 635.

[13]Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence* (Washington, D.C.: Joint Security Commission, Feb. 28, 1994), 127, 128.

staff. Reporting to the president through the Assistant to the President for National Security Affairs, this board is to oversee the development of national security policy.

The Security Policy Forum was established under the Security Policy Board to consider, develop, evaluate, monitor, implement, and guide security policy issues. In existence for one year as of February 1996, this forum consists of six working groups: Personnel Security, Facilities Protection, Policy Integration, Training and Professional Development, Classification Management, and Information Systems Security. All the groups were active as of February 1996, except the Information Systems Security group, which had not been activated owing to differences between the government and private sectors regarding the role of government in this area.

Sensible discussion about the complexity involved in protecting U.S. telecommunications infrastructure is beginning to take shape in Congress; the NII Protection Act of 1995, sponsored by Senators Leahy (Vt., Dem.) and Kyl (Az., Rep.), is intended "to protect the NII against any criminal element."[14] Senator Kyl offered an amendment to S.1026, the Defense Authorization Bill, which would "require the President to analyze all issues in developing a progressive, cohesive national policy toward protecting our ability to communicate, our defense structure, and our information,"[15] and with Senator Charles Robb (Va., Dem.) he requested "the Armed Services Committee to hold a hearing on policy to strengthen our national defense by protecting our information infrastructure."[16]

In July 1996 the Clinton administration took an important step by issuing Executive Order 13010, Critical Infrastructure Protection, to assess the needs of the public and private sectors to protect against the threat of information warfare; to determine what legal and policy issues are raised by efforts to protect critical infrastructures; and to recommend a comprehensive national policy and implementation strategy for protecting these assets.

The race to ensure that information is available to support the security of the United States and to protect its people, its values, and its social, economic, and political structures continues. Passage of the Telecommunications Act of 1996, which emphasizes deregulation and increased competition, underscores the need to develop a cohesive policy to protect vital U.S. telecommunication infrastructure. The complexities of this development are just beginning to be understood.

---

[14]Letter from Jon Kyl, U.S. Senator, July 28, 1995.

[15]Ibid.

[16]Letter from Jon Kyl, U.S. Senator, and Charles Robb, U.S. Senator, to the Honorable Strom Thurmond, Chairman, Senate Armed Services Committee, Nov. 9, 1995.

Chapter Four

Where Perspectives Start: From the Heartland

Wisdom consists of the anticipation of consequences.
— Norman Cousins[1]

The history of emergency telecommunications policy in the United States has followed many paths. Sometimes it has followed the path least traveled, but most of the time it has followed the path of a centralized authority, and in some cases it has had to blaze a new path. The development of telecommunications policy is a complex undertaking, one "described by its acolytes 'as an often paralyzing task,' 'an endless policy loop,' a 'tangled web,' and a 'regulatory round robin.'"[2] A retrospective glance reveals that "history is a vast early warning system"[3] and offers important insights into how emergency telecommunications policy is shaped and how a policy that could serve the United States's information warfare needs might be developed.

4.1 Cultural Values

The values a country holds dear are the essence of a nation and determine the character of its society. Only by understanding the American way of life and the American value system can one begin to understand how to build a consensus in order to develop an information assurance telecommunications policy to meet the country's needs. "When the American public is confronted with change that is little understood, it is likely to react on core values and fundamental national interests. Ignoring the American ethos could result in a misguided policy that fails to garner long term domestic support."[4] The controversy in the early 1990s over the Clipper Chip encryption program, which was sanctioned by the federal government but caught the public sector by surprise, offers a lesson in domestic politics useful for developing an information assurance telecommunications policy. The challenges of information warfare, however, are liable to be more complex and controversial than those surrounding the Clipper Chip. As Samuel Huntington stated in *The Common Defense*, "policy is not the result of deductions from a clear statement of national objective. It is a product of the competition of

---

[1]*Simpson's Contemporary Quotations*, compiled by James B. Simpson (Boston: Houghton Mifflin Co., 1988), 224.

[2]Fred H. Cate, "The National Information Infrastructure: Policymaking and Policymakers," in *The Information Revolution*, edited by Donald Altschiller (N.Y.: H.W. Wilson, The Reference Shelf, Vol. 67, No. 5, 1995), 144.

[3]*Simpson's Contemporary Quotations*, 224.

[4]Jay W. Van Pelt, "Five Deficits and a Physics Problem: Restructuring the Military Services," in *Essays on Strategy XII*, edited by John N. Petrie (Washington, D.C.: National Defense University Press, 1994), 172.

purposes within individuals and groups and among individuals and groups. It is a result of politics not logic, more an area than a unity."[5] According to Newton N. Minow, former Chairman of the FCC:

> the history of telecommunications public policy in America teaches lessons we must not ignore. 'Public interest' has been used by all sides of public policy debates to mean contradictory things; promises made in 'public interest' are often ignored at no cost by those who make them. Many 'public interest' arguments cloak private interest combat between huge industries; and even the most compelling notion of 'public interest' may be useless if unenforceable, unconstitutional, or at war with market forces.[6]

History teaches that an emergency telecommunications policy cannot be a purely political-military based scheme. The makeup of American society derives from historical roots, "the English dominance of colonial affairs [that] led to the American Revolution and provided Americans with a deep and lasting mistrust of strong central governments."[7] Huntington described the problem: "the crux of military policy, to be sure, is the relation of force to national purposes. But it is always national purposes in the plural, national purposes which are continually conflicting, and often being compromised, and seldom realized."[8]

An American public informed about the multidimensional aspects of information assurance might feel confident that its interests would be protected, whereas an uninformed public might complicate government's ability to resolve complicated issues and hinder its necessary flexibility.

> Although protection of national values is the goal of national security policy, these values must be translated into something less abstract and related to specific situations if they are to serve as the basis of policy. By relating values to the domestic environment, policymakers can identify specific interests to serve as concrete objectives toward which the policy can be aimed.[9]

Concurrence and change will come only from a combined effort.

---

[5]Samuel P. Huntington, *The Common Defense: Strategic Programs in National Politics* (N.Y.: Columbia Univ. Press, 1961), 2.

[6]"Commemorative Message," in *A Legislative History of the Communications Act of 1934*, edited by Max D. Paglin (N.Y.: Oxford Univ. Press, 1989), xv.

[7]Van Pelt, 172.

[8]Huntington, 2.

[9]"A Conceptual Framework," *U.S. National Security: A Framework for Analysis*, edited by Daniel J. Kaufman, Jeffrey S. McKitrick, Thomas J. Leney (Lexington, Mass.: D.C. Heath and Co., 1985), 7.

4.2 Legal Issues

The range of legal issues involved in developing an emergency telecommunications policy encompasses all avenues of the U.S. domestic and international legal systems. From individual rights to privacy, to organizational authority, to commercial intellectual property rights, to the jurisdictional boundaries of cyberspace, to fair and equitable judicial due process, to international agreements, this policy challenges U.S. law and the federal system of government.

Perhaps the most important determinant of a national policy is the Constitution. "It was written over two hundred years ago in an effort to strike a balance between the need for greater governmental authority in the 13 newly independent colonies and the fears that government represented the greatest threat to individual liberty."[10] The Constitution outlines the principal powers of the government and defines the authorities and responsibilities of the executive, legislative, and judicial branches in determining policy matters through a unique system of checks and balances. "The Framers of the Constitution, believing that it was wiser not to take chances, devised a remarkably complex system of dividing power and responsibility."[11] Under the Constitution, the national government has only those powers assigned by it, while the states posses the remaining powers of government, thus striking a balance of power between the authority of the government and the freedom of its citizens.

Article I gives all legislative powers to Congress, namely, to the Senate and House of Representatives. Among these are the right to levy taxes, borrow money, regulate interstate commerce, provide for military forces, and to declare war. Article II provides executive power to the president, whose responsibilities include those of chief executive and commander in chief of the armed forces. Article III places the judicial power of the government in the hands of the courts. Through the Bill of Rights, the Constitution provides for the basic rights of its citizens. Within these three articles lie three fundamental issues that affect development of an emergency telecommunications policy.

The first issue for the development of an information assurance policy involves the traditional struggle of the three branches of government for control of domestic and foreign policymaking. According to John H. Lehman, "There are...no frameworks, no cookbooks, no valid models, and no 'golden ages' of administrations past to which we might refer in judging a 'proper' distribution of powers or even 'constitutional' relationship between branches."[12]

---

[10]Frank M. Tuerkheimer, "The Underpinnings of Privacy Protection," in Altschiller, ed., *The Information Revolution*, 164.

[11]Huntington, 168.

[12]Quoted in Richard Haass, "Congressional Power: Implications for American Security Policy," in *U.S. National Security: A Framework for Analysis*, 298.

This power struggle has often led to problems. "By congressional fiat, both the USSS [U.S. Secret Service] and the FBI [Federal Bureau of Investigation] formally share jurisdiction over federal computer-crime busting activities. Neither of these groups has ever been remotely happy with this muddled situation."[13]

The second legal issue is between the government's power and states' rights in determining policy issues. Jurisdictional boundaries become open to question as are penalties for breaking the law. As Winn Schwartau pointed out, "all fifty states have their own computer crime laws—fifty different sets of rules applied to American Cyberspace."[14] Further, "crossing international borders introduces several elements that make identification and prosecution of an intruder more difficult.... Weaving[15] increases the difficulty for law enforcement to trace an intruder, but the problem is compounded when political and diplomatic issues need to be resolved. In addition, the different legal systems, laws, and law enforcement agencies in each country raise issues regarding jurisdiction."[16]

The last issue, a murky one, is the conflict between the rights of the individual and the responsibility of the government to provide for the welfare and common defense. "In 1990, the civil libertarians of cyberspace assembled out of nowhere in particular, at warp speed."[17] Today, organizations such as Computer Professionals for Social Responsibility, the American Civil Liberties Union, and the Electronic Frontier Foundation keep cyberspace issues on the front page and in the public eye. According to Huntington, "the competition of purposes is not just among the broad goals of policy but also among the specific goals of these particular groups and between specific goals and broad goals."[18] The realization of any one goal normally limits realization of the others. Because they are all legitimate they are all articulated, but also because they are legitimate the tendency of democratic politics is to obscure and to moderate the conflict among them."[19] "Telecommunication policy affects the survivability of the Nation, the general welfare of the people, the profitability, and sometimes the existence of powerful corporate entities of the civil sector. Therefore, what may seem

---

[13]Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (N.Y.: Bantam Bks., 1992), 165

[14]Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (N.Y.: Thunder Mouth Press, 1994), 331.

[15]Weaving is "The act of dialing to one computer and then using the outdial from that computer to dial elsewhere...to make free long distance calls from a local or toll-free outdial and to make a trace difficult." National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document*, 2nd ed. (Arlington, Va.), Dec. 5, 1994, B-8.

[16]Ibid., 3-8.

[17]Sterling, 232.

[18]Huntington, 3.

[19]Ibid.

delay is in reality a highly institutionalized regulatory and judicial process."[20] Oliver Wendell Holmes, Jr., explained this process best as far back as 1913:

> It cannot be helped, it is as it should be, that the law is behind the times...it means that the law is growing. As law embodies beliefs that have triumphed in the battle of ideas and then have translated themselves into action, while there is still doubt, while opposite convictions still keep a battle front against each other, the time for law has not come; the notion destined to prevail is not yet entitled to the field.... We too need education in the obvious—to learn to transcend our own convictions and to leave room for much that we held dear to be done away with short of revolution by the orderly change of law.[21]

The role of the federal government in the development of an information assurance telecommunications policy is clear: the federal government will be involved. As reported during the conference on Cyberspace and the American Dream,

> the libertarian-leaning panelists were admonished that if the government does not play a substantial role to ensure the safety of cyberspace and mediate among competing interests...then the new frontier will remain a wilderness.... Only a federal government could protect national security in the Industrial Age.... When the devastating attack comes [on the Internet], then we'll want every resource of the government brought to bear.[22]

4.3 Reactive Policy

The precept of crisis management has guided the development of U.S. emergency telecommunications policy (see **Chapter Two**). "Since the enactment of the Wireless Ship Act of 1910, American telecommunications law...has reflected the need to solve problems or prohibit lawful acts that the industry itself wouldn't solve or prevent."[23] Or, as Robert McNamara said in 1962, "There is no longer any such thing as strategy, only crisis management."[24] "The sinking of the passenger ship Titanic in 1912, prompted Congress to

---

[20]Thomas E. Will, *Telecommunications Structure and Management in the Executive Branch of Government, 1900-1970* (Boulder: Westview Press, 1978), 144-145.

[21]Oliver Wendell Holmes, "Law and the Court" [Speech at a Dinner of the Harvard Law School Association of New York on Feb. 15, 1913), *Collected Legal Papers* (N.Y.: Harcourt, Brace, and Co., 1921; from *Speeches*; Little, Brown, 1913), 294-295.

[22]Alan D. Campen, "Vulnerability of Info Systems Demands Immediate Action," *National Defense* (November 1995), 27.

[23]John M. Kittross, ed., *Administration of American Telecommunications Policy*, Vol. 1 (N.Y.: Arno Press, Collection of Historical Studies in Telecommunications, 1980), 1-2.

[24]Quoted in James L. Richardson, "Crisis Management: A Critical Appraisal," in *New Issues in International Crisis Management*, edited by Gilbert R. Winham (Boulder: Westview Press, 1988), 13.

strengthen the safety provisions of the 1910 radio Act."[25] World War I led to the signing of Public Resolution No. 38, in 1918, which gave the president formal authority over emergency radio. The communications industry's need to solve frequency allocation problems gave birth to the Radio Act of 1927. The Communications Act of 1934 came on the heels of the Great Depression in the United States, when "the mood of the land was for management of a high caliber and an accountability for executive expenditures."[26] "Although some parts of the 1934 Act reflect fears of 'what might happen in the future,' most of this law...was written to prohibit specific evils that were apparent to the lawmakers."[27]

The Board of War Communications came into being as a result of World War II, and the development of the National Communications System was born of the failure of communications during the Cuban Missile Crisis. Presidents Eisenhower and Kennedy placed the telecommunications function outside the executive branch. The OTP, which came into being during Nixon administration, may have been developed to control telecommunications policy because "Nixon, suffering from what he believed to be a liberal network bias in the news, might have seen in the escalation of executive branch telecommunication jurisdiction a potential solution."[28] The increased emphasis on survivable, interoperable communications to support the Carter and Reagan administrations was rooted in the threat of nuclear exchange with the Soviet Union and its aftermath. Thus, every president since Truman changed the organizational structure of the telecommunications policy function of the government, some more than once during a presidency.

In organizational theory, organizations dislike uncertainty and favor slow change, and when they respond to radical changes in the external environment, usually most organizations fail to identify or manage reform successfully.[29] Although changes in the organizational structure occurred with each presidency, according to Thomas Will, "until the Nixon administration no President had been willing to apply a reasonable level of resources to the task of managing, guiding and regulating the telecommunication activities of the Nation."[30] Even though President Nixon focused additional manpower against the problem, the OTP "operated under severe constraints from 1970 until 1977. Manning was never high enough to perform broad functions effectively—authorizations ranged from a high of 65 in 1972 to a low of 41 in 1977...because [the OTP] did not focus needed attention on emergency

---

[25]Will, 4.

[26]Ibid., 14.

[27]Kittross, 2.

[28]Will, 129.

[29]See Ronald D. Asmus, Robert D. Blackwill, F. Stephen Larrabee, "Can NATO Survive?" *Washington Quarterly* **19**, 2 (Spring 1996), 85.

[30]Ibid., 144.

telecommunications, agency-oriented systems continued to develop as they had since the beginnings of the NCS."[31]

Organizational theory also points to the persistence of outdated standard operating procedures in dominating organizational behavior and resistance to change in part because often change upsets the balance of power within an organization.[32] "During the Kennedy Administration the Central Intelligence Agency and the DOD had more influence on the President in regard to emergency preparedness. Both the Director of the CIA and the Secretary of Defense saw the President; the Director of Telecommunications Management never did."[33]

4.4 Cold War Mentality

U.S. emergency telecommunications policy reflected the Cold War mentality. During the Cold War, the balance of power between the two superpowers centered on nuclear weapons and on the continuity of government in the event of nuclear war. President Kennedy, in his message to Congress on the Defense Budget in March 1961, promised to "lay new emphasis on improved command and control—more flexible, more selective, more deliberate, better protected and under civilian authority at all times...to achieve a truly unified, nationwide, indestructible system to insure high-level command, communication and control and a properly authorized response under any conditions."[34] The Cuban Missile Crisis brought the United States to the brink of nuclear war and gave rise to the development of the NCS and the "Molink," a direct communications link to Moscow, "to help reduce the risk of war occurring by accident or miscalculation."[35]

The need for survivable communications was again emphasized by President Carter, with the signing of Presidential Directives 53, National Security Telecommunications Policy, and 59, Flexible Response and Nuclear Targeting, both of which called for "increased survivability and endurance in the command-and-control communications used by the nation's

---

[31]Robert A. Reinman, *National Emergency Telecommunications Policy: Who's In Charge?* National Security Monograph Series 84-2 (Washington, D.C.: National Defense University Press, 1984), 14.

[32]"Can NATO Survive?" 85.

[33]Will, 75.

[34]*Public Papers of the Presidents of the United States: John F. Kennedy, Containing the Public Messages, Speeches, and Statements of the President January 20 to December 31, 1961* (Washington, D.C.: U.S. Gov't Printing Office, 1962), Doc. 99, Special Message the Congress on the Defense Budget, March 28, 1961, 235-236.

[35]*Public Papers of the Presidents of the United States: John F. Kennedy, Containing the Public Messages, Speeches, and Statements of the President January 1 to November 22, 1963* (Washington, D.C.: U.S. Gov't Printing Office, 1964), Doc. 250, White House Announcement of Agreement to Link Washington and Moscow by Direct Telecommunications Facilities, June 20, 1963, 495.

leaders during a prolonged nuclear exchange."[36] The important role of command and control (C^2) communications in the nuclear age was again emphasized by President Reagan, when he included the upgrade of C^2 programs as a key part of the United States's Strategic Weapons Program when he directed the Secretary of Defense to

> strengthen and rebuild our communications and control system, a much neglected factor in our strategic deterrent. I consider this decision to improve our communications and control system as important as any of the other decisions announced today. This system must be foolproof.[37]

By the mid-1990s, the threat of nuclear conflict between two superpowers had diminished, and the end of the Cold War had brought, in President Bush's phrase, a "new world order" in which the United States is the only viable superpower. But the absence of a well-defined threat cannot be equated with the absence of danger to U.S. security. "The introduction of a widely interconnected and globally networked communications environment in which companies and national economies routinely control real-time processes and transfer vast sums of resources as well as sensitive information has redefined the traditional notions of a safe and secure strategic rear."[38] With antecedents in the divestiture of AT&T and with the impact of technology and the information revolution, communications networks have proliferated tremendously. "Former science advisor to the White House G. A. Keyworth II [noted] that the shift from highly centralized mainframe computing to 'distributed' computing by 'hordes of lowly PCs [personal computers]' is paralleled in the 'threat environment' facing the global community. Instead of a so-called 'Evil Empire,' the world now faces 'distributed threats.'"[39]

Distributed computing has expanded the use of information networks in the United States and nearly everywhere else. "The average number of electronic point-of-sale transactions in the United States went from 38 per day in 1985 to 1.2 million per day in 1993. An average of $800 billion is transferred among partners in international currency markets everyday; about $1 trillion is transferred daily among U.S. banks; and an average $2 trillion worth of securities is traded daily in New York markets."[40] New threats are on the horizon. "The

---

[36]George H. Bolling, *AT&T: Aftermath of Antitrust; Preserving Positive Command and Control* (Washington, D.C.: National Defense University, 1983), 4.

[37]Ibid., 4.

[38]Jeffrey R. Cooper, "Conflict in the Information Age: Information Warfare and the Implications of Intelligence," *Colloquy: A Publication of Security Affairs Support Association* **16**, 2 (December 1995), 20.

[39]Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 90.

[40]U.S. Congress, Office of Technology Assessment (OTA), *Information Security and Privacy in Network Environments* (Washington, D.C.: U.S. Gov't Printing Office, September 1994), 1-2.

enemy will be unseen and even unknown. Acts of aggression may be launched from disgruntled nations or rogue states, by religious fanatics, terrorists, criminals, or teenagers insolently and ignorantly flouting their intellectual muscles in cyberspace."[41] In November 1988, the "worm" virus shut down thousands of computers on the Internet. "Related dollar losses are estimated to be between $100,000 and $10 million."[42] "On January 15, 1990, AT&T's long distance telephone switching system crashed, disrupting 70 million telephone calls."[43] According to a threat analysis published in 1994, "a study of one government agency's network systems estimates that approximately 98 percent of all intrusion incidents have gone undetected. Compounding this problem, the study also discovered that only 5 percent of detected incidents were already reported to system or security administrators."[44] In November 1995, I watched while a young Lieutenant, using tools found on the Internet, breached a U.S. Navy vessel at sea. The information systems of the United States are indeed vulnerable. The war over cyberspace has just begun.

NSTAC, formed in 1982, remains in existence in 1996, and in those thirteen years its charter has not changed. Mandated as a presidential advisory council, it was established under the DOD and has often been plagued by bureaucratic red tape, as indicated in the Executive summary of January 12, 1995: "NSTAC representatives and members of the NCS Office of the Joint Secretariat have met with officials from the Executive Office of the President to expedite the President's response to NSTAC recommendations."[45] Even though as early as 1993 the committee had recognized the need to develop procedures to give priority access to cellular phone services for the purposes of national security and emergency preparedness, not until October 1995 did the Secretary of Defense ask the FCC to adopt rules to authorize this service. In commenting on the relationship of technological change and military affairs, Bernard Brodie wrote that "the speed and extent of technological changes have not usually been closely coupled with the strategic and political implications of the relevant changes."[46]

4.5 Technical Intricacies

The structure of telecommunications in the United States consists of a more or less interconnected family of networks serving both private and public sectors. The major network

---

[41]Campen, 26.

[42]OTA, *Information Security and Privacy in Network Environments*, 2.

[43]Sterling, 1.

[44]*The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document*, 3-2.

[45]Executive Report on the 17th Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC XVII), Jan. 12, 1995, 5.

[46]Kaufman, McKitrick, and Leney, 33.

serving the general public is the public switched network (PSN). As a direct consequence of the divestiture of AT&T, telecommunications service is no longer provided by a single supplier using a single network but by a more or less cohesive set of networks consisting of a combination of terrestrial, multipair, copper, coaxial, and fiber-optic cables, microwave and satellite communications with a variety of competing and cooperating owners and users. The ubiquity of the long-distance networks of the PSN, however, is highly dependent on the AT&T network. "The common thread uniting virtually all of these NS/EP systems and services is that an overwhelming majority either transit or reside on existing PSN facilities."[47] The key question becomes, how much real diversity exists within the U.S. information infrastructure as many different competitors share some of the underlying infrastructure in meeting the telecommunications needs of American society?

Both old and new telecommunications systems technologies appear fair game and open to attack, and attacks have occurred on data networks, international gateways, signaling networks, wireless systems, synchronous optical networks (SONET), asynchronous transfer mode (ATM) networks, and integrated services digital networks (ISDN). "Intruders have compromised nearly all categories or types of PSN elements, including switching systems; operations, administration, maintenance, and provisioning systems; and packet data networks. Research also shows that electronic intruders have regularly attacked all types of networks linked to the PSN."[48] According to a publication by the National Communications System, entitled *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications*:

> The emerging technologies have several things in common. Most notably, they offer the customer more management control by supporting intelligent network features. These new technologies also have in common similarities and reliances on older, existing technologies and systems. Electronic intruders have developed the skills to compromise many of these existing technologies and may be able to build on these skills to target the new technologies.[49]

The passage of the Telecommunications Act of 1996 only strengthens this reliance, because the Act provides for a "pro-competitive, de-regulatory national policy framework,"[50] which allows telecommunications service providers easier access to interconnect with the underlying infrastructure. Because of reliance on the PSN infrastructure, most NS/EP systems

---

[47]*The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document*, 4-4.

[48]Ibid., 3-3.

[49]Ibid., 3-14.

[50]Telecommunications Act of 1996, 104th Congress, 2d Sess., Report 104-458, 1.

and services will be more vulnerable to a variety of information warfare threats. "The possible effects of the threat to the PSN include denial or disruption of service, unauthorized monitoring or disclosure of sensitive information, unauthorized modification of network databases/services, and fraud/financial loss."[51] As NCS experts point out:

> An adversary determined to harm the United States through the use of information warfare techniques may choose to completely ignore military systems because of the higher likelihood of success with civilian systems. Major dislocations in American society could be caused by targeting sensitive, but unclassified data, such as power systems, electronic fund transfer systems, the PSN, and the national airspace management system. For a terrorist or hostile power, the virtue of targeting infrastructure industries could be significant. First, any attack on a major infrastructure industry would have an adverse effect on the ability of the U.S. Government to perform its national security and general governmental functions. The confusion resulting from the loss of major infrastructure segments and the loss of essential service capabilities could result in a paralysis of critical U.S. Government activities for a significant period of time. Second, such an attack would affect all of the normal user population, potentially causing widespread fear throughout the civilian population.[52]

It is no surprise that telecommunications resources in the private sector outweigh those of the federal government. The DOD follows the commercial field in information technology. The extent to which the DOD relies on the civilian industry to meet its telecommunications needs suggests why that industry must be a key player. Current numbers indicate that 90 to 95 percent of all unclassified military communications travel on commercial systems. "The long DOD development cycles virtually guarantee a follower status in all areas of technology that have commercial commonality."[53] Systems such as the Digital Switched Network (DSN), the Automatic Digital Network (AUTODIN), the Automatic Secure Voice Communications (AUTOSEVOCOM) network, the Primary Alerting System (PAS), and the North American Aerospace Defense Alerting System are but a few built and operated by the telecommunications industry. During the Gulf War, "extremely complex linkages were established to tie many different U.S.-based databases and networks to those in the war zone. In all, they handled up to 700,000 telephone calls and 152,000 messages per day, and used 30,000 radio

---

[51]*The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document*, ES-1.

[52]Ibid., 2-24.

[53]Ashton B. Carter, "Telecommunications Policy and U.S. National Security," in *Changing the Rules: Technological Change, International Competition, and Regulation in Communications*, edited by Robert W. Crandall and Kenneth Flamm (Washington, D.C.: The Brookings Institution, 1989), 249.

frequencies. The air war alone involved nearly 30 million telephone calls."[54] Until divestiture, the DOD relied on AT&T to provide one-stop shopping for its telecommunications needs—from engineering support, to network management, to handling survivability requirements. But after divestiture, the advent of the *Computer Inquiry II* legislation,[55] and budget reductions, new companies, products, and services came into being that increased the DOD's reliance on industry to satisfy its requirements.

With the United States's increasing reliance on the global information infrastructure (GII) to meet the demands of national security and welfare, actions are needed to develop a workable information assurance policy that can satisfy as far as possible the concerns of all involved stakeholders. The country needs to discover how to avoid fulfilling Winn Schwartau's prediction that "With over 100 million computers inextricably tying us all together through the most complex array of land and satellite based communications systems...government and commercial systems are so poorly protected today that they can be essentially considered defenseless. An electronic Pearl Harbor is waiting to happen."[56]

---

[54]Toffler and Toffler, 79.

[55]This legislation which deregulated the customer premises equipment market and opened it further to competition. See Carol L. Weinhaus and Anthony G. Oettinger, *Behind the Telephone Debates* (Norwood, N.J.: Ablex Pub. Corp., 1988), 16.

[56]Quoted in Toffler and Toffler, 149.

Chapter Five

Beginning Again: Toward a Process

We must be clear sighted in beginnings, for, as in their budding we discern not the danger, so in their full growth we perceive not the remedy.
— Montaigne, *Essays*[1]

A process for the development of an information assurance telecommunications policy awaits definition, to be derived from political debate, public consensus, and events, and with implications yet unknown. The key to developing a national level policy for dealing with an attack on the United States's information infrastructure is understanding that the vast majority of Americans grasp only the emotional level of this subject and that as a subject it not fully understood even by those intimately involved. In 1995 Winn Schwartau noted that "while discussing the lethality of the high energy radio frequency (HERF) gun on information systems during congressional testimony, one congressman asked if the HERF gun should be included as part of the Brady Bill."[2]

Much of this complexity derives from the many dimensions of the issue of providing information assurance and involves a variety of perspectives—technical, legal, domestic, military, and political. In a very real sense, information assurance is an interdisciplinary subject, combining many considerations in various mixes, depending on the particular issue at hand, and most stakeholders understand the nature of the subject only from their own viewpoint and care little about other stakeholders' interests. The elements in the threat picture, for instance, can mean different things to different organizations. The DOD, for example, is mainly concerned with threats from other nation states and nonstate actors. The Department of Justice deals with domestic threats, such as terrorism, threats to citizens, and organized crime. Corporations are concerned with industrial espionage, malicious intruders, and disgruntled employees. An appreciation of the complex array of considerations affecting information assurance is essential in order to discover the necessary tradeoffs for developing a policy that can take the conflicting perspectives into account.

An effective policy must not only protect national security interests but also inspire confidence in the American public and in the business community that their interests are being

---

[1]Quoted in Robert S. McNamara (with Brian VanDeMark), *In Retrospect: The Tragedy and Lessons of Vietnam* (N.Y.: Times Books, 1995), 29.

[2]In a paper presented at the Conference on War in the Information Age, sponsored by the International Security Studies Program at the Fletcher School of Law and Diplomacy, Tufts University, Medford, Mass., Nov. 15-16, 1995.

protected and that the arrangements are functioning both fairly and effectively. Equilibrium is the best defense:

> Policy reflects the power, interests, and attitudes of the public and private individuals and groups concerned with it and affected by it. A change in policy requires either a change in the attitudes of the groups which influence policy or a change in the groups themselves. A policy equilibrium, on the other hand, means that a stable and reasonably harmonious pattern of relationships exists among these groups. Needless to say, policies are never completely harmonious. Equilibrium simply means relative stability and harmony as contrasted with the change and conflict characteristic of disequilibrium.[3]

The best prospect for addressing the problems of "the new world order" is mutual cooperation—government and the people working together to develop a policymaking process that will provide for the common defense. The concept of devising an information assurance policy based upon mutual cooperation differs from the way similar policies were developed in the past. Henry E. Eccles wrote in 1979 that "the ultimate source of strategy lies in the values of the people of a nation."[4] To develop a process requires an approach that will consist of several small but incremental steps, to integrate the sum of the parts into a well-developed and comprehensible policy. "In the discovery and elaboration of new programs, the decision-making process will proceed in stages, and at no time will it be concerned with the 'whole' problem in all of its complexity, but always with parts of the problem. Innovation is more the result of accretion than of any single action."[5] Because development of a new policy will take time, there is no time like the present to get started, as Winn Schwartau stated in *Information Warfare: Chaos on the Electronic Superhighway*:

> ...to leave well enough alone and hope for the best; to hope that, over time, the needed policies, rules guidelines, and mores will somehow successfully assemble themselves into a workable solution, while we suffer minimal disruption or damage in the process. I think not—too much is at stake.[6]

The key to successful development of a coherent and effective process for an information assurance telecommunications policy is to navigate among all the domestic

---

[3]Samuel P. Huntington, *The Common Defense: Strategic Programs in National Politics* (N.Y. Columbia Univ. Press, 1961), 8.

[4]Quoted in Jay W. Van Pelt, "Five Deficits and a Physics Problem: Restructuring the Military Services," in *Essays on Strategy XII*, edited by John N. Petrie (Washington, D.C.: National Defense University Press, 1994), 172.

[5]Huntington, 287.

[6]Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* (N.Y.: Thunder's Mouth Press, 1994), 333.

political pressures and concerns about the information threat to the United States. Currently, there are four main domestic political pressures—from the areas of national security, commerce, law enforcement, and privacy—competing for a voice in the development of this structure and how it should work. A fair court is needed to balance these equities. The larger question becomes, is an information assurance policy to be the responsibility of a single official or agency or the product of negotiation and compromise among a number of officials and agencies?

As of the mid-1990s, no senior person in Washington had sole charge for ensuring information assurance within the United States. With the president, vice president, the secretaries of State, Commerce, and Defense, the National Security advisor, and their associates all having divided attention to a host of complex and demanding issues, information assurance became the responsibility of myriad government agencies, each taking control of its own piece of the puzzle. Failure to establish an organization capable of directing the task of ensuring information assurance in the United States could instead ensure that the fundamental issues involved might be either misaddressed or not recognized. Because so many interests are at stake, deep-seated disagreements among the president's advisors and in the industry about how to proceed could be pushed aside and therefore remain unresolved. As Huntington points out:

> Judgements of the effectiveness of a policy-making process, however, must be based upon at least two criteria. In strategy, as elsewhere, meaningful policy requires both content and consensus. Strategic policies, like statutes or treaties, are both prescriptions for future action and ratifications of existing power relationships. A strategy which is so vague or contradictory that it sets forth no prescriptions for action is no strategy. So also, a strategy whose prescriptions are so unacceptable that they are ignored is no strategy. Consensus is a cost to each participant in the policy-making process, but it is a prerequisite to any policy.[7]

5.1 Analogy to the International Financial Market

This dilemma is not unlike the potential regulatory problems perceived in the international financial markets during the 1970s and 1980s, when the failure of major banking institutions created havoc across national borders: "These policy makers faced a problem that was straightforward yet complex: while money and banks might cross borders, they could not."[8]

---

[7]Huntington, 167.

[8]Ethan B. Kapstein, "Shockproof: The End of the Financial Crisis," *Foreign Affairs* **75**, 1 (January-February 1996), 3.

> In June 1974, when the small German Bankhaus Herstatt floundered, the contagious effect was immediate: interest rates rose, the Eurobanks (the London-based markets for dollars and hard currencies) shriveled, and the integrity of the American payments system was threatened. The 1982 debt crisis led to even greater anxiety about a possible catastrophe, and the payments system was kept in motion only by the injection of huge amounts of cash by the industrial countries and the International Monetary Fund.[9]

Although it took more than twenty years to improve the system in the financial world, "the leading economic powers have created a regulatory structure that has permitted the financial markets to continue towards globalization without the threat of systemic collapse."[10] The potential financial crises, which could have occurred with the "meltdown of the Mexican peso in December 1994, the failure of the 233-year-old Barings Bank last February [1995], and the Daiwa Bank's $1 billion loss in November,"[11] were met "with little more than a 'ho hum.' In fact, the U.S. stock market boomed, and interest rates around the world declined."[12] The financial markets survived those difficulties because the Basle Concordat of 1975 and the Basle Accord were in place, and "the new regulations and standards developed during the 1980s reflected a shift in the focus of banking regulators from crisis management to crisis prevention."[13] Banking regulators

> aimed to share information about banks and regulatory systems and to identify which national regulator had primary responsibility for overseeing the activities of the increasingly international financial institutions. The Basle Concordat laid down the general principles that no international bank would be permitted to escape supervision. It further stated that "parent" or "home" country authorities would be responsible for the oversight of bank solvency. Finally, it urged home and host countries to share information about the activities of multinational banks.[14]

The twin concepts of "home country control" and international cooperation helped financial institutions withstand financial crises. According to Ethan B. Kapstein:

---

[9]Ibid., 2.

[10]Ibid.

[11]Ibid.

[12]Ibid.

[13]Ethan B. Kapstein, *Governing the Global Economy: International Finance and the State* (Cambridge, Mass.: Harvard Univ. Press, 1994), 104.

[14]Kapstein, "Shockproof," 3-4.

> "Home country control" refers to a model of governance in which the responsibility for defining national financial institutions (that is, for determining "who is us?") and regulating them is placed on the [nation] state. Under home country supervision, states look to one another, as opposed to some supranational or multilateral entity, to legislate and enforce any agreements that have been collectively reached.[15]

5.2 Toward a National Information Assurance Policymaking Process

The approaches to these difficulties in the international financial arena offer one model that might be considered for developing and adopting a process for a national information assurance policy. Several principles found in Kapstein's discussion of the Basle Concordat and Accord (see section **5.1**) might usefully be adapted for consideration in the development of a U.S. national telecommunications policy on information assurance:

- that information and telecommunications services can transcend state and national borders and that regulatory problems exist from border to border

- that in the telecommunications arena, responsibility for oversight of an information assurance policy might fall on the individual state, rather than the federal government

- that applying "home country control" (see section **5.1**) to the telecommunications arena at the state level might allow state government and private and public interests to work together more effectively than at the national level to develop a process for an information assurance policy to meet the needs of society

- that a telecommunications policy role based on crisis prevention might be adopted

- that states might share information about the activities of their information assurance efforts in order to standardize and promote intrastate-interstate cooperation by promoting policy convergence and uniform standards

In the words of Christopher Tugendhat, "it is much better to adopt a system of close cooperation between national supervisory authorities imposing a minimum number of legal requirements...than the lengthy and complex route of institutional harmonization."[16]

In short, the states are at the center of this option. Agreements among states to regulate and supervise the activities of telecommunications service providers at the national level might be the product of intense state debates and negotiations. "Honest difference of views and

---

[15]Kapstein, *Governing the Global Economy: International Finance and the State*, 9.

[16]Quoted in Kapstein, *Governing the Global Economy*, 137.

honest debate are not disunity. They are the vital process of policy among free men."[17] Rather than simply reflect the national interest as perceived by the federal government, policies might actually reflect more of society. "[I]nstitutions can help states define the rules of the game for sectors...by providing a setting in which policy ideas can be exchanged and debated, and best supervisory practices developed."[18]

Implementing a new approach and overseeing the process might mean the creation of a full-time team within the executive branch. The key to the success of this committee is finding the right place to position it within the executive branch.[19] "The decisive factor in the innovation of a functional program," according to Huntington, "is the extent to which it is supported by executive groups and congressional or other groups closely associated with the executive branch. If the executive groups substantially favor innovation, not much else is required to make it a reality."[20] Strong political leadership is needed to tackle the development of a U.S. information assurance telecommunications strategy. At the top, a president needs the confidence of Congress, industry, and the public.

> The policy decisions of the Executive Branch of the Government, like the decisions of the business executive or any decision an individual must make in his private affairs, are fundamentally different from the legislative decision. The latter is supposed to represent divergent interests brought to a common denominator or one interest which has won out over the others. The executive decision is supposed to be, first of all, the correct decision, the decision which is more likely than any other to bring forth the desired result. The committee system is appropriate for the legislative process, and it is not by accident that it originated and was institutionalized there. The executive decision requires the mind and will of one man who, after hearing the evidence and taking counsel, takes it upon himself to decide what is the right action under the circumstances.[21]

Implementation might also mean moving the NSTAC, the U.S.'s best expertise in the area of emergency telecommunications, out of the DOD into a home where it can become part of the core team concept. As a result of the move, the committee's charter might be reviewed,

---

[17]Herbert C. Hoover, in a speech in New York City, 20 Dec. 1950, quoted in *Political Quotations: A Collection of Notable Sayings on Politics from Antiquity Through 1989*, edited by Daniel B. Baker (Detroit : Gale Research, 1990), 167.

[18]Kapstein, *Governing the Global Economy*, 13.

[19]As shown in Chapter Two, the government's attempts to deal with its need to "assure" information, particularly during this century, has been haphazard at best.

[20]Huntington, 290.

[21]Huntington, 168-169.

to strengthen its leadership role, and its membership opened up to the departments of Justice, Commerce, and State and to key privacy advocates, as well as public and private industry, including major software companies. The committee's role might be similar to that of the Basle Committee[22] in overseeing the United States's efforts in developing an information assurance policy, with particular focus on regulation in both national and international arenas.

Policies resulting from implementing this approach might emphasize the role of crisis prevention, rather than the one used in the past, crisis management (see section **4.3**). To promote this role, one responsibility of the committee might be to provide a working definition of what information assurance means to various stakeholders, giving them details on services to expect during a crisis. This could be done by providing the states with a clear picture of the actual critical components of the NII, their value to the country, and the nature of threats that might affect the United States's ability to provide information assurance. Another, perhaps more important, responsibility might be to examine such questions as, "Do we *need* to take steps to protect information resources? How *effective* are the available options for protecting these resources? What will protection *cost*—financially and operationally?"[23] A third responsibility might be to act as a clearinghouse for information about the latest technological advances potentially useful for protecting the United States's information infrastructure.

Crisis prevention means states sharing information with one another on the "systemic risks [to] and recommendations for maintenance"[24] of the telecommunications infrastructure. As shown, problems that affect the telecommunications arena mirror those the financial markets confronted during the 1980s, when "public officials were [not only] concerned with maintaining the safety and soundness of the financial system, but they were concerned with the competitiveness of the American banks as well. The challenge was therefore to adopt policies that satisfied both sets of concerns."[25] Regulations, emergency response policies, as well as criminal sentences jointly developed might help to establish a level playing field for all involved. "If it is a good policy, it will also have direction and purpose. But the direction can only be a product of the consensus, not an alternative to it."[26]

---

[22]Established in December 1974, the committee's objective "should *not* [Kapstein's emphasis] be to make far-fetched attempts to harmonize the twelve countries' individual systems of supervision, but should be to enable its members to learn from each other and to apply the knowledge so acquired to improving their own systems of supervision, so indirectly enhancing the likelihood of overall stability in the international banking system" (quoted in *Governing the Global Economy*, 44, 45).

[23]Daniel J. Knauf, *The Family Jewels: Corporate Policy on the Protection of Information Resources* (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, P-91-5, June 1991), 2.

[24]Kapstein, *Governing the Global Economy*, 23.

[25]Ibid., 106.

[26]Huntington, 168.

> Mutual recognition, coupled with a minimal set of essential regulations, must ultimately lead to policy convergence across the member states; it was simply the "lowest common denominator" way of getting there. If detailed legislation could not be imposed upon member states from above, then the commission would adopt a 'bubble up' approach in which member states would ultimately move toward common standards and regulations in order to avoid chaos.[27]

As Dan Knauf points out, "a problem in identifying these factors is sorting the wheat from the chaff. Many things—different kinds of things—have a bearing on the matter. It can be difficult to relate them to each other in a way that allows them to be viewed as a unified whole."[28] Understanding that every piece of the playing field cannot be protected and that there is a difference between being susceptible and being vulnerable, the committee, through semiannual meetings with state representatives, would help to develop criteria for what needs to be protected and to what extent, at what cost, and with what advantage for whom. The committee would also be responsible for ensuring that agreed-upon minimum standards were met and for handling disputes among states. "In sum, while it is true the markets need structures of governance in order to function, they cannot operate efficiently when they are imprisoned by overregulation."[29]

Involving the states in decisionmaking might occur in several ways, including the following:

(1) The Communications Act of 1934, as amended in 1996, still allows the FCC to convene joint boards for the purpose of making "available, so far as possible, to all people of the United States, a rapid, efficient, nationwide, and worldwide wire and radio communications service...."[30] The use of joint boards promotes cooperation with each of the states through their respective commission structures.

> The Commission (FCC) may refer any matter arising in the administration of this Act (1934) to a joint board to be composed of a member, or of an equal number of members, as determined by the Commission, from each of the states in which the wire or radio communication affected by or involved in the proceeding takes place or is proposed, and any such board shall be vested with the same powers and be subject to the same duties and liabilities as in the case of a member

---

[27]Kapstein, *Governing the Global Economy*, 141.

[28]Knauf, *The Family Jewels*, 2.

[29]Kapstein, *Governing the Global Economy*, 184.

[30]Stat. 3285, §1 (1933-1934).

> of the Commission when designated by the Commission to hold a hearing as hereinbefore authorized.[31]

(2) Many mechanisms already exist at the state level to put a new process of this type into place; each state has an official or agency in charge of telecommunications. It is mainly a matter of organizing the effort into a cohesive one, allowing the states to come together and voice their opinions.

> State and local governments also regulate the telecommunications service providers, particularity local telephone and cable operators. Every state has a regulatory agency (i.e., Public Utility Commission or Public Service Commission) responsible for overseeing intrastate telecommunications. These state organizations not only exercise considerable power over telephone service within their respective states, they also act collectively through the National Association of Regulatory Utility Commissioners and with the FCC on Federal-State Joint Boards. In addition, many cities exercise some continuing control over cable television through local franchising authority. These cities may act collectively on issues of common concern through the National League of Cities.[32]

Joint boards and state mechanisms might be useful in promoting consensus among the various interests and stimulating active participation of the private sector. "Community building is an incremental process."[33] How can the state and federal agencies (such as the DOD, State, Commerce, etc.) and telecommunications service providers be persuaded to buy into this new approach? "Common purpose can only emerge out of broadly based policy discussion and widespread participation in the policy making process. It cannot be decreed from on high."[34] A sense of common purpose might be based on effective new uses of education, laws, funding, and taxation.

A major opportunity for an administration to present its case to Congress might be available in formal testimony, prepared statements, and other communications by executive branch officials at open and closed committee hearings. Public debates, similar to those recently held in Norway and Canada on the issue of television and violence, might be useful to reach the American people as a whole. Indeed, the lives of every American will be touched, and no one is invulnerable if the threats of information warfare to power grids, air

---

[31]Stat. 3285, §410a (1933-1934).

[32]Fred H. Cate, "The National Information Infrastructure: Policymaking and Policymakers," in *The Information Revolution*, edited by Donald Altschiller (N.Y.: H.W. Wilson, The Reference Shelf, Vol. 67, No. 5, 1995), 155.

[33]Kapstein, *Governing the Global Economy*, 149.

[34]Huntington, 196.

traffic control systems, telecommunications, and banking institutions are real. "Policy on a controversial issue can be free of tentativeness and certain of support only when it emerges from a process in which all the potentially interested groups have an opportunity to make a contribution."[35]

The American public's understanding of policy in the 1960s and 1970s, during the war in Vietnam, and, more recently, during the Clipper Chip debates, and the complicated effects of that understanding, stand in stark contrast to the success in gaining congressional and support through public awareness achieved by President Bush during the Gulf War. Extensive debate can clearly be beneficial:

> It would enable congressional and public groups to play a more effective and recognized role in the discussion of policy alternatives. It would broaden the consensus supporting the policy which is finally adopted. It would remove the need and the opportunity for dissident executive groups to appeal their cases to the public after the decision. It would minimize post-decision debate and lesson doubt about the finality of the presidential action. It would mitigate many of the defects of the policy-making process which disturb the critics.[36]

Education is a key component, but not the only component, of this approach. Given increasing reliance on information in a global economy, the federal government might provide tax incentives, funding, and grants to the states to encourage them to participate in this program. The federal government and the states, on the other hand, might turn around and offer the similar incentives to telecommunications service providers, through such means as tax breaks and alternative regulatory methods. According to Jeffrey A. Masoner, "regulators must seek to reach the decision that will maximize the public interest and most effectively balance ratepayer and shareholder interests."[37] Because their interests vary,

> the most critical questions stakeholders must address when evaluating regulatory alternatives focus on the issue of competition. Can regulators control competition? Is competition beneficial in all markets? Where is competition effective and where is it only emerging? At what point is competition sufficiently developed to better promote the public interest than regulation? And what form of regulation will best be able to promote traditional regulatory goals as well as facilitate the transition to

---

[35]Ibid., 195.

[36]Huntington, 196.

[37]*Alternatives to Rate Base/Rate of Return Regulation of Local Exchange Carriers: An Analysis of Stakeholder Positions* (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, May 1990, P-90-3 [Long Version]), 347.

> fully competitive markets? How will the success or failure of any regulatory alternative be judged?[38]

A concerted effort, bringing the states together, might provide a focal point for developing a comprehensible process for an information assurance policy, and, in the long run, foster a consistency in policymaking that might allow President Clinton's vision of the NII to mature in a sensible, cohesive fashion, both nationally and globally. "Broadening the scope of policy consensus may well go hand-in-hand with improving the quality of the policy content."[39] With such a partnership between government and the public, each might come to understand the other's needs, provide market opportunities for new products, and better the economic well-being of individual states and of the country as a whole. "Harmonization will develop from the 'bottom up' rather than the 'top down.'"[40]

---

[38]Ibid.

[39]Huntington, 196.

[40]Kapstein, *Governing the Global Economy*, 15.

Chapter Six

New Lessons from Old Stories

New opinions are always suspected, and usually opposed,
without any other reason but they are not already common.
— John Locke[1]

The following anecdote, based on the sinking of the *Titanic* in 1912, was related a few years ago by Vice-President Gore and can be said to assess the importance of the government's role in building an information assurance telecommunications policy:

> Why did the ship that couldn't be sunk steam full speed into an ice field? For in the last few hours before the Titanic collided, other ships were sending messages like this one from the Mesaba: "Lat 42N to 41.25 Long 49W to Long 50.30W. Saw much heavy pack ice and great number large icebergs also field ice." And why, when Titanic operators sent distress signal after distress signal, did so few ships respond? The answer is that—as the investigations proved—the wireless business was just that, a business. Operators had no obligation to remain on duty. They were to do what was profitable. When the day's work was done—often the lucrative transmissions from wealthy passengers—operators shut off their sets and went to sleep.... Ironically, that tragedy resulted in the first efforts to regulate the airwaves. Why did government get involved? Because there are certain public needs that outweigh private interests.[2]

The information revolution, which encompasses vast technological changes as well as the reactions to them, has brought new conditions into being that require new thinking. Rather than make rash decisions based solely on the end of the Cold War, the United States needs to discover how to think through and prepare helpful measures before a crisis occurs in order to assess how best to respond to a crisis and to put in place a process for adapting these measures to conditions that most likely will continue to change at a rapid pace.

In this country, the ultimate information assurance policy decisionmaker is "we, the people," and in its effort to balance the forces involved in this contentious issue, government involvement might work best by focussing on the states and their interests. By adopting a "states first" approach to resolving issues of information assurance, government may come up with policies and practices that could provide a necessary framework for devising a GII

---

[1]*The Wit and Wisdom of Politics*, compiled by Chuck Henning (Golden, Colo.: Fulcrum Press, 1992), 102.

[2]On Dec. 21, 1993, at the National Press Club; cited in Donald Altschiller, ed., *The Information Revolution* (N.Y.: H.W. Wilson, The Reference Shelf, 1995), 161.

strategy useful in a world developing since the end of the Cold War. Because of the apparent vulnerabilities of the U.S. information infrastructure, the United States can ignore the realities of the need for such a policy only at peril to itself, as Achilles, the greatest warrior among the Greeks, in a crisis of battle ignored his own vulnerability and safety:

> With Hector [the chief warrior among the Trojans] dead, Achilles knew, as his mother had told him, that his own death was near. One more great feat of arms he did before his fighting ended forever... [which was to kill] Memnon in a glorious combat.... Then he himself fell beside the Scaean gates. He had driven the Trojans before him up to the wall of Troy. There Paris shot an arrow at him and Apollo guided it so that it struck his foot in the one spot where he could be wounded, his heel.[3]

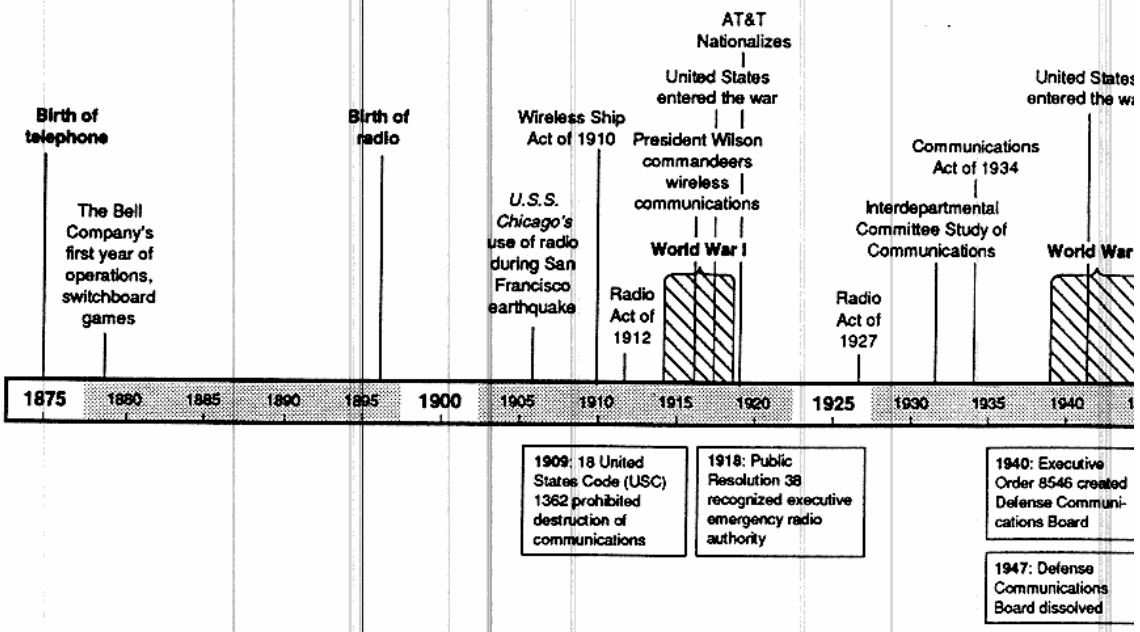
The challenge for the United States is to balance equities at play in the marketplace without enervating the dynamism it seeks to promote, and to begin with an acknowledgement that seeking to maintain the status quo cannot be an answer in a time of change.

---

[3]Edith Hamilton, *Mythology* (N.Y.: New American Library, 1969, rpt.; Little, Brown, 1940), 193-4.

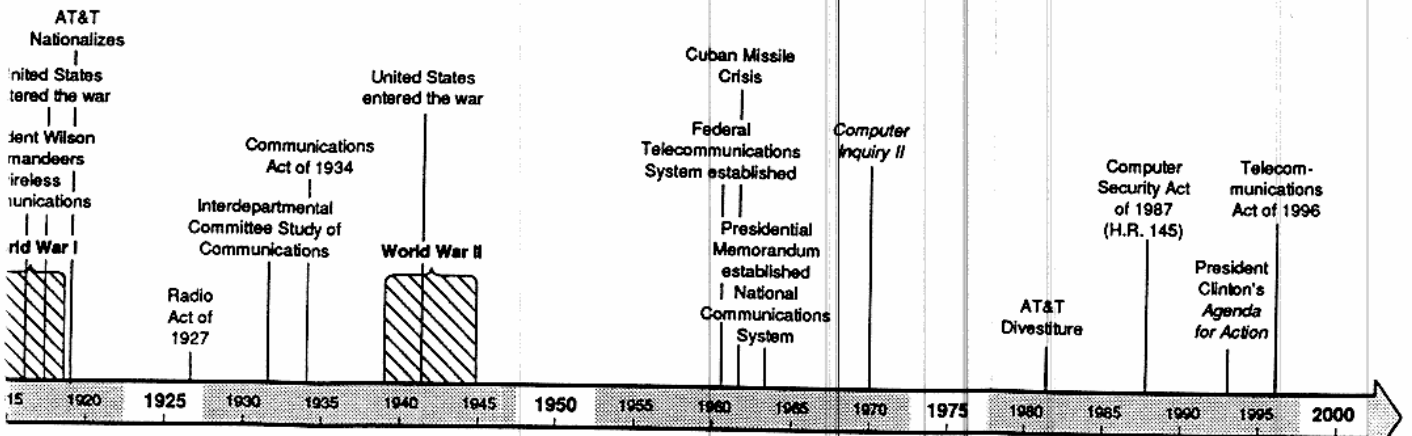
Appendix

Development of United States Informati



Appendix

Development of United States Information Systems Policy



1918: Public Resolution 38 recognized executive emergency radio authority

1940: Executive Order 8546 created Defense Communications Board

1947: Defense Communications Board dissolved

1950: Executive Order 10110 created President's Communications Policy Board

1951: Executive Order 10297 created position of Telecommunications Advisor to the President

Executive Order 10312: CONELRAD

1953: Executive Order 10460 abolished position of Telecommunications Advisor to the President and transferred its duties to the Director of the Office of Defense Mobilization

1961: 18 USC Section 1362 amended, provided penalties for malicious damage to telecommunications

1962: Executive Order 10995 established position of Director of the Office of Telecommunications Management

1963: Executive Orders 11092 and 11093 assigned emergency telecommunications responsibilities to the FCC and GSA

1968: Executive Order 11490 transferred emergency preparedness functions to federal agencies

1970: Executive Order 11556 created Office of Telecommunications Policy and abolished position of Director of the Office Telecommunications Management

1975: Executive Order 12046 abolished Office of Telecommunications Policy, appointed Secretary of Commerce as Principal Advisor on Telecommunications Policy, and created Office of the Assistant Secretary of Communications and Information

1979: Executive Order 12148 created Federal Emergency Management Agency

Presidential Directive 53 on National Security Telecommunications Policy

1982: National Security Decision Directive 47 on Emergency Mobilization Preparedness

Executive Order 12382 established National Security Telecommunications Advisory Committee

1983: National Security Decision Directive 97 rescinded Presidential Directive 53

1984: Executive Order 12472 reestablished the National Communications System

National Security Decision Directive 145 on National Policy on Telecommunications and Automated Information System Security

1988: National Security Decision Directive 188 on Government Coordination for National Security Emergency Preparedness

1989: National Security Directive 1 redefined the role of the National Security Council

National Security Directive 10 established National Security Policy Coordinating Committees

1993: Executive Order 12864 established U.S. Advisory Council on the National Information Infrastructure

1994: Joint Security Commission Report Redefining Security

Presidential Directive 29 created Security Policy Board

Title 47 Code of Federal Regulations

1996: Executive Order 13010 for Critical Infrastructure Protection

: Policy.

Acronyms

ATM	asynchronous transfer mode
AT&T	formerly American Telephone & Telegraph Co., Inc.
AUTODIN	Automatic Digital Network
AUTOSEVOCOM	Automatic Secure Voice Network
C^2	command and control
CIA	Central Intelligence Agency
CONELRAD	Control of Electromagnetic Radiation
DSN	Digital Switched Network
DTM	Director of Telecommunications Management
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GAO	General Accounting Office
GII	global information infrastructure
GSA	General Services Administration
HERF	high-energy radio frequency
ICC	Interstate Commerce Commission
IITF	Information Infrastructure Task Force
ISDN	integrated services digital network
IRAC	Interdepartmental Radio Advisory Committee
LATA	local access and transport area
MFJ	Modification of Final Judgement
NCS	National Communications System
NII	National Information Infrastructure
NSA	National Security Agency
NSC	National Security Council
NSDD	National Security Decision Directive
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
OEP	Office of Emergency Planning
OMB	Office of Management and Budget
OTA	Office of Technology Assessment
OTM	Office of Telecommunications Management
OTP	Office of Telecommunications Policy
PAS	Primary Alerting System

PC	personal computer
PC	Policy-Coordinating [Committee]
PCPB	President's Communications Policy Board
PD	Presidential Directive
PDD	Presidential Decision Directive
PSN	public switched network
SONET	synchronous optical network
USSS	United States Secret Service

PPPFC

ISBN 1-879716-40-2