USAWC STRATEGY RESEARCH PROJECT

The National Telecommunications Infrastructure: A 21st Century Organizational Paradox

by

Lieutenant Colonel Mark D. Baines
U.S. Army

Dr. Olenda Johnson
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
07-04-2003		xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE
The National Telecommunications Infrastructure: A 21st Century Organizational Paradox
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Baines, Mark ; Author

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Army War College
Carlisle Barracks
Carlisle, PA17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Same as Report (SAR)	36	Rife, Dave RifeD@awc.carlisle.army.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number DSN

ABSTRACT

AUTHOR: Lieutenant Colonel Mark D. Baines

TITLE: The National Telecommunications Infrastructure: A 21st Century Organizational Paradox

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 40 CLASSIFICATION: Unclassified

The telecommunications infrastructure of the United States is large, organizationally bureaucratic, and vulnerable. Yet, it is the means by which the U.S. facilitates its dominant forms of strategic power, specifically a thriving economy and an unparalleled military. It is literally the backbone of the Information Age. Is this critical infrastructure capable of meeting the demand being placed upon it? What organizations are responsible for it? What are the vulnerabilities? And do the answers to these questions have national security implications?

This paper examines the national telecommunications infrastructure of the United States and argues that the size and bureaucratic nature of this infrastructure exposes the United States to vulnerabilities and inefficiencies that may impact national security. It evaluates efforts to establish an infrastructure capable of meeting the intent of Presidential Directives and legislation regarding a secure, robust, and interoperable national communications infrastructure. It looks specifically at Department of Defense organizations involved with this effort and examines recent shifts in oversight of the National Communications System (NCS) from the Department of Defense (DOD) to the newly established Office of Homeland Security.

TABLE OF CONTENTS

ACKNOWLEDGEMENT

To Angela and O.J.

LIST OF TABLES

THE NATIONAL TELECOMMUNICATIONS INFRASTRUCTURE: A 21ST CENTURY ORGANIZATIONAL PARADOX.

The national telecommunications infrastructure, historically recognized as essential to our national security, has been formally identified as a Critical Infrastructure by Executive Order 13010 and more recently, the Office of Homeland Security. All of the other 12 Critical Infrastructures identified by the Office of Homeland Security are dependent upon the national telecommunications infrastructure for their daily operations – it is the backbone through which we engage in diplomacy, facilitate our economy, command and control our military, and process information – all primary sources of our national power.

A great paradox of the information age is that the very technology that makes us stronger makes us increasingly vulnerable. Widespread telecommunications interconnectivity poses enormous risks to our information systems, essential computer operations, and critical infrastructures such as power distribution, national defense, law enforcement, and government services. Potential adversaries, whether terrorist groups, criminal organizations, nation-states, or malicious insiders can develop relatively inexpensive cyber attack capabilities and attempt to exploit these risks.[1] Therefore, it is essential that the telecommunications infrastructure of the United States be adequately organized, effectively managed, appropriately resourced and securely protected.

This paper examines the national telecommunications infrastructure of the United States and argues that the size and bureaucratic nature of this infrastructure exposes the United States to vulnerabilities and inefficiencies that may impact national security. It evaluates efforts to establish an infrastructure capable of meeting the intent of Presidential Directives and legislation regarding a secure, robust, and interoperable national communications infrastructure. It looks specifically at Department of Defense organizations involved with this effort and examines recent shifts in oversight of the National Communications System (NCS) from the Department of Defense (DOD) to the newly established Office of Homeland Security.

BRIEF HISTORY OF TELECOMMUNICATIONS TECHNOLOGY

Much of what makes this subject both challenging and interesting is the tremendous speed of technological breakthroughs in the area of telecommunications and the apparently slow legal, organizational and management responses to these changes. To emphasize this point, a brief observation of significant technological advances in telecommunications over the last 150 years is helpful (see Table 1). The rapid pace of these innovations, coupled with the naturally cumbersome operating nature of large, bureaucratic governmental organizations,

leads logically to a source of concern as stated by former President Clinton, particularly when applied in the context of our national security. …"In less than one generation, the information revolution and the introduction of the computer into virtually every dimension of our society has changed how our economy works, how we provide for our national security, and how we structure our everyday lives."[2]

1844	The first public message over a telegraph line.
1876	The telephone was patented.
1896	The invention of wireless and radio Communications.
1920	The Marconi Company begins sound broadcasting.
1939	The advent of the first modern day computer.
1963	The first Communications satellite put into orbit.
1969	The Internet.
1988	The first fiber optic cable across the Atlantic Ocean.

TABLE 1. BRIEF HISTORY OF TELECOMMUNICATIONS TECHNOLOGY

As depicted in this table, advances in information and telecommunications technologies are proceeding at an increasingly rapid rate and there is no foreseeable slowdown. Throughout history, these technologies have impacted our approach to national security and significantly altered the strategic environment. To further illustrate this point, while many of the military communications systems used during the Gulf War in 1990 transmitted messages at a rate of roughly 2,400 bits per second, today the rate has increased to well over 23 million bits per second. A message that took an hour to send in 1990 can now be transmitted in less than a second.[3]

THE CURRENT ENVIRONMENT

Our society is increasingly relying on new information technologies and the Internet to conduct business, manage industrial activities, engage in personal communications, and perform scientific research.[4] These technologies allow for enormous gains in efficiency, productivity, and communications. Yet the same interconnectivity that allows us to transmit information around the globe at the click of a mouse or push of a button also creates unprecedented opportunities for criminals, terrorists, and hostile foreign nation-states who might seek to steal money or proprietary data, invade private records, conduct operations, or engage

in Information Warfare – specifically, cyber attacks.[5] As a result, the national telecommunications infrastructure is exposed to a host of threats and vulnerabilities.

THREATS

The President's Commission on Critical Infrastructure Protection defines "Threat" as "Anyone with the capability, technology, opportunity, and intent to do harm. Potential threats can be foreign or domestic, internal or external, state-sponsored or a single rogue element."[6] Of particular concern for the critical infrastructures are the threats derived from an external entity with malicious intent. The concept of Information Warfare is now common terminology within the Department of Defense and is becoming increasingly important to national security. An enemy can now attack from a distance, without detection, and without confronting our military force on force. One need only to review the daily logs at any of the numerous federal or industry sponsored Computer Emergency Response Team (CERT) facilities for proof.

Computer Intrusions

Clearly, the explosion in computer interconnectivity, while providing great benefits, also poses enormous risks. Terrorists or hostile foreign states could launch computer-based attacks on critical systems to severely damage or disrupt national defense or other critical operations. In 1999, 22,144 attacks against Department of Defense (DOD) computers were detected, a threefold increase over the previous year.[7] DOD computer intrusions, which are increasingly complex and destructive, reached over 40,000 in 2001. Even more alarming is that the CERT estimates that only 10 percent of such attacks are detected, and far fewer are reported. If this estimate is accurate, over 220,000 attempted intrusions into DOD computers took place in 1999, and over 400,000 in 2001.[8]

Everyday in the United States, thousands of unauthorized attempts are made to intrude into the computer systems that control key government and industry networks: defense facilities, power grids, banks, government agencies, telephone systems, and transportation systems. Some of these attempts fail. Some succeed. Some gain systems administrator status, download passwords, implant so called sniffers to copy transactions, or insert trap doors to permit an easy return. Some attackers are the equivalent of car thief joy riders, who commit a felony as a thrill. Others are commit attacks for industrial espionage, theft, revenge-seeking vandalism, or extortion. Some attacks may be committed for intelligence collections, reconnaissance, or creation of a future attack capability. The perpetrators range from juveniles to potentially hostile

militaries. What has emerged in the last several years is an increase in the seriousness of the threat.[9]

The United States is exposed to such attacks because it has become dependent upon computer networks for many essential services, while paying insufficient attention to protecting those networks. Water, electricity, gas, rail, aviation, and other critical functions are directed by computer controls over vast telecommunications networks and expansive information systems. The possibility exists that adversaries could exploit these networked infrastructures, not necessarily for destruction, but for large-scale disruption prior to a more kinetic form of attack.

Information Warfare

One of the great asymmetric threats identified by American defense planners, Information Warfare (IW), would be an effective tool for use against both civil society and against the military.[10] Although military information systems are increasingly well protected against IW intrusion, they are still susceptible to attacks. Additionally, the civilian telecommunications infrastructure, further behind in protection efforts, is very susceptible. IW attacks against financial systems, such as online banking networks and investment systems, for example, would cause significant discomfort in the American populace, acting directly against the political will. Several countries have or are developing robust IW capabilities. Indeed, developing this attack capability is relatively inexpensive, deniable and easily concealable due to the dual-use nature of the expertise and hardware.[11]

VULNERABILITIES

Similar to threat possibilities, of equal concern are the vulnerabilities that are internal to some organizations. As stated previously, these telecommunications infrastructures are large, expensive, subject to technical and operator-induced failures, and vulnerable. There are multiple potential points of failure that range from the management of networks to the more physical characteristics of telecommunications such as transmission and switching. The issues are numerous, as the following examples reveal.

Legacy systems and aging equipment

Significant portions of the United States' national telecommunications infrastructure regularly fail during normal operations. After a three day outage in January of 2000, costing thousands of person-hours and over $1.5 million in repairs, Stephen B.Tate, the chief of the National Security Agency's (NSA) Strategic Directions Team, was quoted as saying "our information technology infrastructure is a critical part of our mission and it needs some repair…

It is a burning platform and we've got to fix it."[12] The NSA failure was, unfortunately, not unique. Similar outages have occurred in critical infrastructures across the defense intelligence community; at the National Imagery and Mapping Agency, and at the Defense Intelligence Agency for example.[13] All of these outages were not the result of a high-tech cyber attack, but rather were traced to defects in the wires, switches and nodes that make up the physical electronic nervous system of these agencies and their individual telecommunications infrastructure.

Reliance on industry

Another notable vulnerability is the reliance of the infrastructure on commercial services. This reliance and mutual dependence presents a mix of governmental and industry based motivations. Currently, approximately 95% of telecommunications vital for our national security travel over commercial telecommunications networks.[14] We are presented with the traditional conflicting interests of politics, national defense and the financial bottom line. One might suggest that these conflicting interests and motivations raise significant concerns ranging from bureaucratic organizational structures and inefficient management to wasted resources and ultimately, national security issues.

Large networks

Beyond the purely physical dimensions of vulnerability associated with the national telecommunications infrastructure are the more intangible vulnerabilities of large networks themselves. In an article entitled *Confronting the limits of Networks,* Andrew McAfee and Francois-Xavier Oliveau describe five phenomena that can affect large networks negatively. They are: Saturation (the point where the number of different resources is maximized), Cacophony (when too many users of a network make interaction difficult… a crowded chat room for example), Contamination (spam or offensive content), Clustering (when users consistently use only one portion of a network), and Search Costs (as a network becomes larger, it simply takes more time to navigate). Their basic argument is that large and expanding networks are good up to a certain point. Beyond that point, however, leaders and managers must understand that there are significant risks involved.[15] They argue that Metcalfe's Law, which states that the "value of a network increases in proportion to the square of the number of people using it", does not always hold true.[16] Similarly, the NSA example referred to above appears to have been more managerial than physical in nature according to NSA director Lieutenant General Michael

V. Hayden. He pointed out that NSA at that time had five largely autonomous directorates and 68 e-mail systems at Fort Mead alone.[17]

In the current environment, these are only a few examples of the threats and vulnerabilities facing the national telecommunications infrastructure of the United States. Concern over these threats and vulnerabilities permeate society as evidenced in the media with such front-page headlines as this one, in *The Washington Post* last June: "Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say." Unfortunately, the vulnerabilities could become more acute and the threat could mature faster than adequate defenses could thwart them.

DEFENSE ATTEMPTS

Attempts to identify and protect against these threats and vulnerabilities are increasing in society, within the political realm, and in the defense department. Ironically however, the best defenses against massive attacks and failures against the national telecommunications and other critical infrastructures may be happening entirely by accident. Many organizations have developed proprietary or stove-pipe systems, unique to their branch of government. While these systems produce tremendous inefficiencies, information sharing roadblocks and overwhelming interoperability issues, they do provide a form of protection.[18] That is, if only a few number of employees are familiar with a certain software package, or how to operate certain hardware – intrusions become difficult.

SOURCES OF AUTHORITY IN TELECOMMUNICAITONS

The idea of a fully integrated, interoperable, functional, and secure national telecommunications infrastructure is indeed a challenge. Federal organizations involved with this complex effort derive their authority and responsibilities from a variety of laws, regulations and federal policy documents. Therefore, to understand the organizations themselves it is necessary to examine executive orders, legislation, and directives which provide the sources of authority for organizations responsible for the national telecommunications infrastructure of the United States. A brief summary of the more relevant sources of authority for telecommunications organizations is shown in Table 2.

Source of Authority	Description
Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions"	Signed in 1984, this order established the National Communications System and assigns national security emergency preparedness responsibilities for telecommunications
Executive Order 13228, "Establishing the Office of the Homeland Security Council"	Signed in October 2001, this order establishes the Office of Homeland Security, whose mission is to develop and coordinate the implementation of a comprehensive national strategy to secure the U.S. from terrorist threats or attacks. Specifically related to telecommunications: "the Department of Homeland Security will work to develop comprehensive emergency communications systems. The National Communications System would be incorporated into the Department of Homeland Security to facilitate the effort."[19]
The Information Technology Management Reform Act "The Clinger-Cohen Act"	Signed in 1996, this act grants authority to the head of each agency to acquire information technology (IT) resources and makes them responsible for effectively managing IT investments. It established best practices, Chief Information Officer (CIO) positions, and evaluation measurements for IT.[20]
National Security Directive 42, "National Policy for the Security of National Security Systems"	Signed in 1990, this directive designates the Director, National Security Agency (NSA) the national manager of national security telecommunications and information systems security and calls upon him or her to promote and coordinated defense efforts against threats to national security systems.[21]

TABLE 2 SOURCES OF AUTHORITY

ORGANIZATIONS RESPONSIBLE FOR THE NATIONAL COMMUNICATIONS INFRASTRUCTURE

In support, and as a direct result of this legislation, there is a myriad of organizations involved either directly or indirectly with the administration of the national communications infrastructure of the United States. A recent Government Accounting Office (GAO) report on Critical Infrastructure Protection (CIP) found that 52 organizations were all involved with CIP: 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations.[22]

Although some of the organizations described in the GAO report have little to do directly with the national telecommunications infrastructure, many of them are central. These organizations are primarily located within 13 major departments and agencies. Several departments including Department of Defense (DOD), Treasury, and Commerce have multiple

subordinate organizations involved. For example, 7 organizations within DOD alone are involved in national or multi-agency CIP efforts. Table 3 highlights these organizations and their respective roles regarding the national telecommunications infrastructure.

ORGANIZATION	Policy Development	Research and Development	Emergency Preparedness	Network Management	Interagency/Industry Coordination
Federal Advisory Committees					
President's National Security Telecommunications Advisory Committee	v		v		
President's Information Technology Advisory Committee	v	v			v
Executive Office of the President					
Office of Homeland Security	v		v		v
Office of Science and Technology Policy	v	v	v		
Office of Management and Budget					v
President's Critical Infrastructure Protection Board			v		v
Chief Information Officers Council	v				v
National Communications System		v	v	v	v
Federal Communications Commission			v		v
U.S. Department of Commerce					
Critical Infrastructure Assurance Office	v		v		
National Institute of Standards and Technology		v	v		v
National Telecommunications and Information Administration		v	v	v	v
U.S. Department of					

Defense					
Joint Staff				v	v
Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence	v		v	v	v
Defense Advanced Research Projects Agency		v	v		
National Security Agency		v	v		v
Joint Task Force – Computer Network Operations			v		v
U.S. Department of Justice					
National Infrastructure Protection Center			v	v	v
Federal Emergency Management Agency					
Office of National Preparedness			v		v
Office of the Chief Information Officer and Information Technology Services Directorate			v		
U.S. General Services Administration					
Federal Computer Incident Response Center		v		v	v

TABLE 3 ORGANIZATIONS INVOLVED WITH THE NATIONAL TELECOMMUNICATIONS INFRASTRUCTURE

As depicted in Table 3 there are numerous organizations involved with the national telecommunications infrastructure. There is also extensive evidence of duplication of effort and overlapping responsibilities associated with this critical infrastructure. This pattern undermines effective performance and potentially threatens our national security. Of particular interest to the U.S. military are telecommunications organizations within DOD. The number of these organizations is a reflection of and is indicative of the broader, more comprehensive and unwieldy, national telecommunications infrastructure, and warrants closer examination.

DOD ORGANIZATIONS AND THE NATIONAL COMMUNICATIONS SYSTEM

Under the provisions of Executive Order 12472, *Assignment of the national security and emergency preparedness telecommunications* functions, the Department of Defense was given the broad responsibility to provide, operate, and maintain the telecommunications services and facilities in support of the National Command Authorities.[23] To accomplish this task, internal DOD telecommunications staffing and organizations were established. They include:

- The Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (OSDC3I). This office is at the pinnacle of the DOD regarding telecommunications issues, programs and resources. According to its mission statement OSDC3I "builds the foundations for network-centric operations through policies, program oversight, resource allocation, and the provision of value-added support."[24]
- The Joint Chiefs of Staff (JCS). The JCS serve as the primary military advisors to the President on all military and national defense related issues. Regarding telecommunications, the JCS maintains operational oversight of the Defense Information Systems Agency (DISA) which responds directly to the Chairman, Joint Chiefs of Staff on all operational matters and communications requirements.
- The Defense Information Systems Agency (DISA) is a separate agency under the direction, authority, and control of ASDC3I although DISA reports to the JCS on operational matters. Additionally, DISA is responsible for management and implementation of the National Communications System (NCS). The NCS will be discussed in more detail later in this paper.
- The National Security Agency (NSA). The primary mission of the NSA is protecting national security telecommunications and information systems. Additionally, NSA produces vulnerability assessments which are used to develop hardware and software computer network defenses. NSA is required, at the direction of the ASDC3I, to "work with" – "assist" – and "coordinate" with a host of other federal and non-federal organizations.
- The Joint Task Force for Computer Network Operations (JTFCNO). The JTFCNO, like the NSA, is focused on coordinating and directing activities related to computer based attacks, contains damage, and restores functionality when disruptions occur.
- The Defense Advance Research Projects Agency (DARPA) assists with federal government research and development for protecting critical infrastructure information

systems, including emergency preparedness communications.[25] Additionally DARPA is required to "coordinate" with a host of internal and external agencies including the National Science Foundation for research and development.

Specifically, within DOD, duplication of effort and overlapping responsibilities associated with this critical infrastructure lead to inefficient performance and potentially threaten our national security.

> … today there is an adversary that poses a threat, a serious threat, to the security of the United States of America. This adversary is one of the world's last bastions of central planning. It governs by dictating five-year plans. From a single capital, it attempts to impose its demands across time zones, continents, oceans and beyond. With brutal consistency, it stifles free thought and crushes new ideas. It disrupts the defense of the Untied States and places the lives of men and women in uniform at risk. This adversary's closer to home. It's the Pentagon bureaucracy. Not the people, but the process. Not the civilians, but the systems. Not the men and women in uniform, but the uniformity of thought and action that we too often impose on them. Seventeen layers of bureaucracy within DOD are too many. Some of these levels of management are not contributing a lot of value added. One of the benefits of decentralizing decision making is to flatten organizations and eliminate less productive layers.[26] – Secretary of Defense, Rumsfeld.

The National Communications System

Overall, DOD facilitates its role in the national telecommunications infrastructure through the National Communications System or NCS. The NCS is arguably the central nervous system of the national telecommunications infrastructure, particularly in the area of emergency preparedness and emergency response. In 1963, under the direction of John F. Kennedy, the NCS's charter was to "link together, improve, and extend, on an evolutionary basis, the communications facilities and components of the various Federal agencies… to provide necessary communications for the Federal Government under all conditions ranging from a normal situation to national emergencies and international crisis, including nuclear attack."[27]

However, in 1984 with Executive Order 12472, the focus of the NCS was changed. The order generated the new mission of assisting 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 exercising wartime and non-wartime emergency communications responsibilities while coordinating emergency telecommunications planning for the federal government.[28] Thus the responsibility of the NCS evolved from its centralized, focused role of

implementing a single Federal telecommunications system, to a rather decentralized, unfocused role of advising and coordinating among several entities.

The numerous concerns raised by the shifting focus of the NCS clearly relate directly to the threats and vulnerabilities outlined previously. Furthermore, at issue are concerns regarding the benefits and shortfalls of centralized versus decentralized organizations. Centralized organizations possess the advantages of decision making and focused planning for activities needed to pursue the organization's strategy. Decentralized organizations are generally characterized by organizational flexibility and more motivated and involved employees. However, the NCS is not an organization in and of itself, but rather a system which is managed by the DOD. Therefore, the application of the NCS, as a system, could be centralized, while management of the NCS could, in theory, be more decentralized.

Change in oversight of the NCS

Apparently, the current administration is again looking at influencing the mission of the NCS. The Office of Homeland Security and the Homeland Security Council was established by Executive Order 13228 in order to develop and coordinate the implementation of a comprehensive national strategy to secure the U.S. from terrorist threats or attacks. Included in the National Strategy for Homeland Security document published in July of 2002 is incorporation of the NCS: "The Department of Homeland Security will work to develop comprehensive emergency communications systems. The National Communications System (NCS) would be incorporated into the Department of Homeland Security to facilitate the effort".[29] The shift of the NCS from DOD to the DHS is a recognition by the current administration that the organizations currently responsible for the implementation of the NCS and the national telecommunications infrastructure, are inefficient at best, or at worst, not succeeding in their mission. Simply shifting oversight of the NCS from the DOD to the OHS does not address the issues of overlapping responsibilities within organizations, and perhaps may even exacerbate organizational concerns. In 1999, the commission for National Security in the 21st Century highlighted organizational and other issues within DOD.

> The DOD needs to be overhauled. The growth in staff and staff activities has created mounting confusion and delay. The failure to outsource or privatize many defense support activities wastes huge sums of money. The programming and budgeting process is not guided by effective strategic planning. The weapons acquisition process is so hobbled by excessive laws, regulation, and oversight strictures that it can neither recognize nor seize opportunities for major innovation, and its procurement bureaucracy weakens a defense industry that is already in a state of financial crisis. [30]

The move of the NCS from DOD to OHS is not the solution to achieving the goals of a comprehensive, robust, and interoperable national telecommunications infrastructure, as outlined in Executive Orders and legislation, because it does not address the root issue of having too many organizations with overlapping and sometimes conflicting responsibilities. It is, unfortunately, indicative of sweeping governmental reaction to very complex organizational issues. The creation of the OHD may improve other functions of the government, but in the area of our national telecommunications infrastructure, its chances of success are marginal unless it aggressively restructures the organizations involved based on identifying organizational capabilities and core competencies.

The evidence of overlap and duplication of effort within the federal government is unfortunately not unique to the DOD or the telecommunications sector. Some of the more dramatic examples include:[31]

- Seven different federal agencies administer 40 different programs aimed primarily at job training.
- Eight different federal agencies operate 50 different programs to aid the homeless.
- Nine agencies operated 27 teen pregnancy programs.
- Ninety early childhood programs are scattered among 11 federal agencies.

The move of the NCS from the DOD to OHS is recognition of the issue – but the wrong approach to addressing it. The application of the national telecommunications infrastructure requires organizations that are *flexible* enough to adjust to the constantly changing strategic environment described by many as volatile, uncertain, complex and ambiguous; *adaptive* enough to react to a fluid political situations which directly impact resourcing (manpower, programs, personnel etc…); and *integrated* with commercial industry because of the pace with which innovative technology products are introduced. Simply changing oversight of the NCS from the DOD to the OHS only further complicates the organizational dilemmas.

RECOMMENDATIONS

In an address to the National Press Club on January 13th, Paul A. Volcker, former chairman of the Federal Reserve Board, stated "the executive branch has inadvertently grown into an archipelago of agencies and departments… without logical structure. Reacting to particular perceived needs and pressures, they have been put together piecemeal with overlapping and conflicting responsibilities that deter intelligent policy-making."[32]

Volcker's comments were based on a report by the National Commission on the Public Service, which he chaired. The report called for sweeping reorganization of the federal government, as did a report by the U.S. Commission on National Security/21st Century three years earlier.[33] That commission found that "there is a critical need to reshape the DOD to meet the challenges of the 21st Century security environment." And the Commission warned that the U.S. intelligence capabilities were hindered by "organizational constraints that limit the Intelligence Community's ability to optimally address emerging security threats." All of these recommendations were made prior to the attacks on September 11th.

As we delve further into the more recent Volcker report, it provides some concrete and supportable recommendations that should be applied to the organizations responsible for the national telecommunications infrastructure. It recommends that "The federal government should be reorganized into a limited number of mission-related executive departments." As shown in Table 2, too many agencies share responsibilities that could be combined or eliminated, and the implied requirement to be in constant coordination, both internally and externally, delays substantive and timely decisions. Again, using the DOD as indicative of the larger federal structure, the following are examples of potential organizational changes.

A critical first step in undertaking any organizational restructuring is a valid assessment of organizational capabilities coupled with a solid definition of core organizational competencies. Currently, the OSD/C3I is DOD's equivalent of industry's Chief Executive Officer position regarding telecommunications within DOD. Using this office as a starting point, changes immediately present themselves and permeate through the remaining subordinate organizations.

First: Change the title of this position from the Office of the Secretary of Defense for Command, Control and Intelligence to simply the Office of the Secretary of Defense for Telecommunications. The Intelligence function clearly resides elsewhere and the terms Command and Control are broad, all encompassing, and embedded in DOD's "core identity".[34] Organizations are often handicapped from adapting because of their core identity. Decisions are made and strategy is developed based on the organization's history which is reinforced over time. When organizations form an identity, similar to an individual's life style, ethnic group or profession, this identity tends to influence how employees perceive the environment and address issues.[35] The change from OSD/C3I to OSD/T better defines the core mission of the office and provides focus on the DOD portion of the national telecommunications infrastructure. This office would provide leadership, set policy, articulate rules, and publish guidance.

Second: Remove the JCS from maintaining operational influence over DISA, thus focusing the JCS specifically on the strategic war fighting aspects of the DOD and enabling the JCS to fulfill its role as chief military advisors to the President. This step relieves DISA from the burden of having multiple reporting chains and allows them to focus on management of the NCS.

Third: Combine the functions of the NSA and JTF-CNO into one agency with the mandate to *secure* and *protect* the telecommunications infrastructure from cyber-related attacks. This move aligns missions, functions and core competencies currently shared by both organizations. It would provide significant resource efficiencies, particularly in the area of personnel and network monitoring. It would further facilitate unity of effort in the emerging concepts of computer network operations and information warfare.

Fourth: Allow DISA to *manage* the entire strategic telecommunications network for DOD. This provides DISA with mission focus, cultural identity, and sense of purpose. It would further eliminate redundancies currently resonant within multiple subordinate DOD telecommunications organizations.

Finally: Integrate DARPA with the multitude of other agencies and organizations involved with *research and development* within DOD and throughout the federal government – with a specific focus on telecommunications and information technologies. This would ensure interoperability of telecommunications related software and hardware within DOD, synchronize research efforts and provide tremendous resource efficiencies particularly when contracting with industry.

Although these changes may appear oversimplified, they present a visualization of the utility in defining and aligning core competencies during an organizational redesign. Once telecommunications organizations are aligned with core competencies, value can immediately be recognized in terms of efficiency, interoperability and resources. More importantly, organizations are then more effectively postured to address the national security issues posed by the numerous threats and vulnerabilities.

A BROADER PERSPECTIVE

The application of the national telecommunications infrastructure requires organizations that are ***flexible*** enough to adjust to the constantly changing strategic environment described by many as volatile, uncertain, complex and ambiguous;[36] ***adaptive*** enough to react to fluid political situations, which directly impact resourcing (manpower, programs, personnel etc…); and ***integrated*** with commercial industry because of the rapid pace with which innovative technology

products are introduced. The benefits of fixed hierarchical organizations, particularly those involved with complex telecommunications infrastructures, are few. Today's environment makes organizational flexibility an imperative. The organizations and individuals involved with the national telecommunications infrastructure must be capable of independent actions which are consistent with a synchronized strategic plan.

Apparently within the federal government, and within DOD specifically, this is not happening: "For all the rhetoric in documents like the report of the National Defense Panel and Joint Vision 2010 about better joint teamwork and more adaptive organizations, a basic fault line exists in the U.S. military establishment."[37] Both military and civilian leaders must revitalize a culture that in many ways is dysfunctional. This is a monumental challenge as recognized by Secretary of Defense Rumsfeld in his quest to review and change national defense priorities and integrate business practices into the DOD: For the military, "change is hard."[38]

Integration of commercial industry with federal agencies is clearly one of the most significant challenges facing the application of the national telecommunications infrastructure. As stated previously, roughly 95% of the national telecommunications infrastructure traverses through commercial networks. Furthermore, industry has the capability to develop and introduce new technology with much greater speed than is possible in the bureaucratic world of the federal government.[39] The Federal organizations responsible for the application of the national telecommunications infrastructure must embrace and integrate industry into their organization and business practices. As articulated previously in the vulnerabilities section, the reluctance to do this understandably revolves around security and national defense. By no means should security concerns be ignored, but by focusing on *only* security, efficiency and relevancy are quickly forfeited – which itself is a real security risk.

SUMMARY

The national telecommunications infrastructure, historically recognized as essential to our national security, has been identified as a Critical Infrastructure by the Office of Homeland Security. All of the other 12 Critical Infrastructures identified by the Office of Homeland Security are dependent upon the national telecommunications infrastructure – it is the backbone through which we exercise all four sources of our national power, Diplomatic, Military, Informational and Economic.

The national telecommunications infrastructure, while presenting tremendous opportunity, is increasingly vulnerable, both internally and externally, for a myriad of reasons. One of the most

complex of these vulnerabilities is the massive, bureaucratic nature of the organizations responsible for the national telecommunications infrastructure. The Department of Defense alone has 6 major subordinate organizations involved with the national telecommunications infrastructure and is indicative of the broader issue. The National Communications System (NCS), arguably the central nervous system of the national telecommunications infrastructure, is being moved from the DOD to the OHS.

The recommendations articulated in the Hart/Rudman commission and the Volcker commission should be acted upon. The bottom line is that because of the critical nature of the telecommunications infrastructure and the increasingly rapid change of technologies supporting it – the organizations responsible for the national telecommunications infrastructure must be redesigned to become adaptive, flexible, and integrated.

CONCLUSION

The nature of the world is changing. Alvin Toffler, in his book The Third Wave, published in 1980, described the transformation of societies in the context of an Agricultural age, an Industrial age and an Information age.[40] Much of what he described in his book has materialized, as advances in Information technology have enabled the virtual shrinking of vast geographical distances and facilitated the compression of time. Great wealth and tremendous power, traditionally held by the very few and achieved over a lengthy period of time, are now being achieved by the many and in a very short period of time. Amazon.com and eBay are modern examples of technology-based business adventures that made many individuals very rich, very fast. [41]

Ten years after Toffler's book, John Naisbitt and Patricia Aburdene published Megatrands 2000 (1990) in which they clearly articulated the importance of a vibrant telecommunications infrastructure.

> Telecommunications-and computers-will continue to drive change, just as manufacturing did during the industrial period. We are laying the foundations for an international information highway system. In telecommunications we are moving to a single worldwide information network, just as economically we are becoming one global marketplace. We are moving toward the capability to communicate anything to anyone, anywhere, by any form-voice, data, text, or image-at the speed of light. [42]

The opportunities presented by a robust, reliable, and secure national telecommunications infrastructure are numerous and cross virtually all aspects of day-to-day life, the economy and democracy. The opportunity presented by advanced telecommunications networks on the national and global economy (arguably the United States' Center of Gravity) is overwhelming.

Electronic currency transfer systems allow banks to move capital around at a moment's notice, avoiding interest rate differentials, taking advantage of favorable exchange rates, and avoiding political unrest.[43] For example, Citicorp's telecommunications Network allows it to trade $200 billion daily in foreign exchange markets around the world. Similar networks give the global banking community the ability to move money with light speed, at an estimated $1.5 trillion daily.[44]

Secondly, the opportunity presented by advanced telecommunications networks in a democratic society is already proven. If a person is literate and has access to a television or computer, he or she possesses the means to be well informed about political issues and candidates. Additionally, this technology has the potential to transcend all of the ethnic and race issues traditionally associated with politics. It simply gives people a voice in politics through myriad of means and enables more people to dialogue in the political realm. In 1995 the Benton Foundation presented a project briefing entitled "Telecommunications and Democracy," in which they highlight six areas that advancing telecommunications technology can influence and enhance the democratic process.[45] These areas include the ability to "deepen people's understanding of policy issues" and to "broaden participation in deliberations on political issues."

Again, the economy and the democratic process are just two areas of opportunity presented to a nation connected through a robust, secure, and reliable telecommunications infrastructure; there are countless more. "It is not by chance that communications and community come from the same Latin root. Any system that enhances or denies our ability to learn from and talk to one another necessarily affects our social fabric. "[46]

This paper discusses evidence that shows that as the rapid pace of IT continues to increase exponentially, so do the associated vulnerabilities, threats, and opportunities. One of the most significant vulnerabilities in this electronically interconnected environment, is the organizational construct of our national telecommunications infrastructure. This vulnerability has not gone unrecognized as evidenced by the recent shift of the NCS from DOD to the Office of Homeland Security. But, the dramatic changes in the world since the end of the cold war have not been accompanied by any other major institutional changes in the U.S. government – particularly in the area of telecommunications. Clearly change of this nature is a daunting, complex, and bureaucratic endeavor. It will take bold initiatives by our political institutions, integrated support and cooperation from industry, legislative reform, and time.

> Organizational reform is not a panacea. There is no perfect organizational design, no flawless managerial fix. The reason is that organizations are made out of people, and people invariably devise informal means of dealing with one another in accord with the accidents of personality and temperament. Even

> excellent organizational structure cannot make impetuous or mistaken leaders patient or wise, but poor organizational design can make good leaders less effective. …Sound organization is important. It can ensure that problems reach their proper level of decision quickly and efficiently and can balance the conflicting imperatives inherent in any national security decision-system.[47]

Between senior involvement and expert input, between speed and the need to consider a variety of views, between tactical flexibility and strategic consistency, there are many conflicting imperatives involved in related decision making. Talk is cheap. Let us take appropriate informed steps now to refine our national telecommunications infrastructure from the organizational paradox that it is, to the model 21st century organization it must be.

WORD COUNT = 6,398

ENDNOTES

[1] Tim Gibson, Colonel U.S. Army, "What You Should Know about attacking Computer Networks," Proceedings (January 2003): 48-51.

[2] William Jefferson Clinton, Presidential Decision Directive 63, White paper – President's Message. The White House. January 7 2000.

[3] Jim Katzaman, "Short Path to the Future," Air Force News Service, September 13, 1996.

[4] Joseph S. Nye and William A. Owens, "America's Information Edge," in Information Age Anthology: National Security Implications of the Information Age, ed. David S. Alberts and Daniel S. Papp (CCRP publications series, August 2000), 115.

[5] Ibid

[6] President's, commission, Critical infrastructure protection. Critical Infrastructure Assurance Office. Available from http://www.ciao.gov/resource/commission.html; Internet; accessed 10 December 2002.

[7] Arnaud de Borchgrave et al., Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington: Center for Strategic and International Studies, December 2000), p.9.

[8] Ibid., See also Carnegie Mellon University's website at http://www.cert.org/research/.

[9] Charles Schumer, We Are Far and Away the Most Technologically vulnerable, *Prepared Remarks to the Critical Infrastructure Assurance Summit,* New York, N.Y., September 22, 2000; available from http://www.ncs.gov/N5_HP/Customer_Service/Xaffairs/SpeechService/SS00-057.htm; Internet; accessed 11 December 2002.

[10] Joseph C. Cyrulik,, "Asymmetric Warfare and the Threat to the American Homeland" Landpower Essay Series (November 1999), No. 99-8

[11] George Tenet, director of Central Intelligence, Testimony before the Senate Armed Services Committee, 2 February 1999.

[12] James Bamford, Body of Secrets (New York: Doubleday, 2001) p. 574.

[13] Rudy de Leon, "DOD Perspectives on Critical Infrastructure Protection", *Prepared Remarks before the President's National Security Telecommunications Advisory Committee (NSTAC),* Colorado Springs, Colorado, May 16, 2000; available from http://www.ncs.gov/N5_HP/Customer_Service?Xaffairs/SpeechService/SS00-035.htm; Internet; accessed 11 December 2002.

[14] Donald H. Rumsfeld, chairman, "Report of the Commission to Assess United States National Security Space Management and Organization," 11 January 2001, available from http://www.defenselink.mil/pubs/space20010111.html; Internet; accessed 30 December 2002.

[15] Andrew McAfee and Francois-Xavier Oliveau, "Confronting the Limits of Networks", MIT Sloan Management Review, (Summer 2002) p. 85

[16] George Gilder, "Telecosm: Metcalfe's Law and Legacy," Forbes ASAP 152: Supplement (September 1993), 158-166. Metcalfe's Law of the telecosm states that the potential value of a network is "n" squared, with "n" being the number of nodes on the network.

[17] Vernon Loeb, "Test of Strength," The Washington Post Magazine, 29 July 2001, p.23

[18] Joshua Green, "The Myth of Cyberterrorism," The Washington Monthly *Online* (November 2002) available from <http://www.washingtonmonthly.com/features/2001/0211.green.html >; internet; Accessed 1 December 2002.

[19] Office of Homeland Security, National Strategy for Homeland Security, (July 2002): p. 58

[20] The Information Technology Reform Act, (the Clinger-Cohen Act), Statutes at Large 508 (1996): available from <http://irm.cit.nih.gov/policy/legislation.html>; Internet. Accessed 6 December 2002.

[21] National Policy for the Security of National Security Systems, National Security Directive 42. (1990).

[22] General Accounting Office, Critical Infrastructure Protection: Report to the committee on Governmental Affairs, U.S. Senate. (Washington, D.C.: U.S. General Accounting Office, July 2002), GAO-02-474.

[23] Executive Order 12472, Assignment of the national security and emergency preparedness telecommunications functions, Statutes at Large (April 1984) <http://www.fas.org/irp/offdocs/eo/eo-12472.html>; Internet. Accessed 28 November 2002.

[24] John P. Stenbit, Mission Statement, Office of the Assistant Secretary of Defense for Command, Control, Communications, & Intelligence. (21 November 2002) http://www.c3i.osd.mil./; Internet. Accessed 2 December 2002.

[25] General Accounting Office, Critical Infrastructure Protection: Report to the committee on Governmental Affairs, U.S. Senate. (Washington, D.C.: U.S. General Accounting Office, July 2002), GAO-02-474.

[26] Donald H. Rumsfeld, "DOD Acquisition and Logistics Excellence Week Kickoff-Bureaucracy to Battlefield," speech, Pentagon, Washington DC, 10 September 2001; <available from http://www.defenselink.mil/speeches/2001/s20010910-secdef.html; Internet; accessed 10 December 2002.>

[27] John f. Kennedy, "Establishment of the National Communications System". Presidential Memorandum (August 21 1963).

[28] Executive Order 12472, Assignment of the national security and emergency preparedness telecommunications functions, Statutes at Large (April 1984) <http://www.fas.org/irp/offdocs/eo/eo-12472.html>; Internet. Accessed 28 November 2002. See also, http://www.ncs.gov/NCS/HTML/NCSorgchart.html <accessed 8 November 2002>

[29] Office of Homeland Security, National Strategy for Homeland Security, (July 2002): 58.

[30] Gary Hart and Warren Rudman, U.S. Commission on National Security and the 21st Century, (February 2001), 10 http://www.nssg.gov/Reports/reports.htm; Internet. Accessed 2 February 2003.

[31] Paul A. Volcker, The National Commission on the Public Service, (January 2003), http://www.brookings.edu/dybdocroot/GS/CPS/Volcker/reportfinal.pdf. <accessed 10 February 2003.

[32] Paul A. Volcker, "Speech to the National Press Club" January 13 2003, Government Executive, (February 2003). 6.

[33] Gary Hart and Warren Rudman, U.S. Commission on National Security and the 21st Century, (February 2001), 10 http://www.nssg.gov/Reports/reports.htm; Internet. Accessed 2 February 2003.

[34] Lauren Keller Johnson, "The Organizational Identity Trap, The answer to the question, 'Who are we?' is complex, elusive and can confound strategic change". MIT Sloan Management Review. (Summer 2002): 11.

[35] Ibid.

[36] U.S. Army War College, Strategic Leader Primer

[37] Edwin Dorn and Howard D. Graves, "Shaping American Military Culture in the 21st Century", American Military Culture In The Twenty-First Century CSIS Report, (February 2000), p. 56.

[38] Thomas E. Ricks, "for Military, 'Change Is Hard,'" The Washington Post, (19 July 2001): A16.

[39] "A more Commercial Future" The Economist July 20th 2002. p15.

[40] Alvin Toffler, The Third Wave. Bantam Books published in association with William Morrow and Company, Inc. 1980.

[41] Peter Newcomb, "The First Billion Takes a Lifetime…Except in the Internet Age," Forbes 163:8 (April 19,1999): 26-247.

[42] John Naisbitt and Patricia Aburdene; Megatrands 2000, "ten New Directions For the 1990's", Avon books 1990. p.6.

[43] J. Langdale, "Electronic Funds Transfer and the Internationalization of the Banking And Finance Industry," Geoforum (16:1985), pp. 1-13, Langdale, "The Geography of International Business Telecommunications: The Role of Leased Networks," Annals of the Association of American Geographers (79: 1989), pp. 501-522; and B. Warf, "Telecommunications and the Globalization of Financial Services," Professional Geographer (41:1989), pp. 257-271.

[44] Barney Warf, Information Age Anthology "Telecommunications and the changing Geographics of Knowledge Transmission in the late 20th Century", (2002): Chapter 20.

[45] The Benton Foundation, Communications Policy Project Briefing #4, "Telecommunications and Democracy" Washington, D.C., (1995).

[46] Ibid.p.429

[47] Gary Hart and Warren Rudman, U.S. Commission on National Security and the 21st Century, (February 2001), 10 http://www.nssg.gov/Reports/reports.htm; Internet. Accessed 2 February 2003.

BIBLIOGRAPHY

Bamford, James, Body of Secrets (New York: Doubleday, 2001) p. 574

Borchgrave, Arnaud de et al., Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington: Center for Strategic and International Studies, December 2000), p.9.

Clinton, William Jefferson. Presidential Decision Directive 63, White paper – President's Message. The White House. January 7 2000.

Cyrulik, Joseph C.. "Asymmetric Warfare and the Threat to the American Homeland" Landpower Essay Series (November 1999), No. 99-8.

De Leon, Rudy, "DOD Perspectives on Critical Infrastructure Protection", *Prepared Remarks before the President's National Security Telecommunications Advisory Committee (NSTAC),* Colorado Springs, Colorado, May 16, 2000

Dorn, Edwin and Graves, Howard D. "Shaping American Military Culture in the 21st Century", American Military Culture In The Twenty-First Century CSIS Report, (February 2000), p. 56.

Executive Order 12472, Assignment of the national security and emergency preparedness telecommunications functions, Statutes at Large (April 1984) <http://www.fas.org/irp/offdocs/eo/eo-12472.html>; Internet. Accessed 28 November 2002.

Executive Order 12472, Assignment of the national security and emergency preparedness telecommunications functions, Statutes at Large (April 1984) <http://www.fas.org/irp/offdocs/eo/eo-12472.html>; Internet. Accessed 28 November 2002.

Gibson, Timothy. Colonel U.S. Army, "What You Should Know about attacking Computer Networks," Proceedings (January 2003): 48-51.

Gilder, George. "Telecosm: Metcalfe's Law and Legacy," Forbes ASAP 152: Supplement (September 1993), 158-166.

Green, Joshua. "The Myth of Cyberterrorism," The Washington Monthly *Online* (November 2002) available from <http://www.washingtonmonthly.com/features/2001/0211.green.html >; internet; Accessed 1 December 2002.

Hart, Gary and Rudman, Warren. U.S. Commission on National Security and the 21st Century, (February 2001), 10 http://www.nssg.gov/Reports/reports.htm; Internet. Accessed 2 February 2003.

Johnson, Lauren Keller. "The Organizational Identity Trap, The answer to the question, 'Who are we?' is complex, elusive and can confound strategic change". MIT Sloan Management Review. (Summer 2002): 11.

Katzaman, James. "Short Path to the Future," Air Force News Service, September 13, 1996

Kennedy, John F. "Establishment of the National Communications System". Presidential Memorandum (August 21 1963).

Langdale, J. "Electronic Funds Transfer and the Internationalization of the Banking And Finance Industry," Geoforum (16:1985), pp. 1-13.

Loeb, Vernon. "Test of Strength," The Washington Post Magazine, 29 July 2001, p.23.

McAfee, Andrew and Oliveau, Francois-Xavier. "Confronting the Limits of Networks", MIT Sloan Management Review, (Summer 2002) p. 85

Naisbitt, John and Aburdene, Patricia. Megatrands 2000, "ten New Directions For the 1990's", Avon books 1990. p.6.

National Policy for the Security of National Security Systems, National Security Directive 42. (1990).

National Strategy for Homeland Security, Office of Homeland Security, (July 2002): p. 58.

Newcomb, Peter. "The First Billion Takes a Lifetime…Except in the Internet Age," Forbes 163:8 (April 19,1999): 26-247.

Nye, Joseph S. and Owens, William A.. "America's Information Edge," in Information Age Anthology: National Security Implications of the Information Age, ed. David S. Alberts and Daniel S. Papp (CCRP publications series, August 2000), 115.

Ricks, Thomas E. "for Military, 'Change Is Hard,'" The Washington Post, (19 July 2001): A16.

Rumsfeld, Donald H., "Report of the Commission to Assess United States National Security Space Management and Organization," 11 January 2001, available from http://www.defenselink.mil/pubs/space20010111.html; Internet; accessed 30 December 2002.

Rumsfeld, Donald H.. "DOD Acquisition and Logistics Excellence Week Kickoff-Bureaucracy to Battlefield," speech, Pentagon, Washington DC, 10 September 2001; <available from http://www.defenselink.mil/speeches/2001/s20010910-secdef.html; Internet; accessed 10 December 2002.>

Schumer, Charles. We Are Far and Away the Most Technologically vulnerable, Prepared Remarks to the Critical Infrastructure Assurance Summit, New York, N.Y., September 22, 2000

Stenbit, John P.. Mission Statement, Office of the Assistant Secretary of Defense for Command, Control, Communications, & Intelligence. (21 November 2002) http://www.c3i.osd.mil./; Internet. Accessed 2 December 2002.

Strategic Leader Primer. U.S. Army War College.

Tenet, George, Testimony before the Senate Armed Services Committee, 2 February 1999.

The Benton Foundation. Communications Policy Project Briefing #4, "Telecommunications and Democracy" Washington, D.C., (1995).

The Economist, "A more Commercial Future" July 20th 2002. p15.

The Information Technology Reform Act, (the Clinger-Cohen Act), Statutes at Large 508 (1996): available from <http://irm.cit.nih.gov/policy/legislation.html>; Internet. Accessed 6 December 2002.

Toffler, Alvin. The Third Wave. Bantam Books published in association with William Morrow and Company, Inc. 1980.

U.S. General Accounting Office, Critical Infrastructure Protection: Report to the committee on Governmental Affairs, U.S. Senate. (Washington, D.C.: U.S. General Accounting Office, July 2002), GAO-02-474.

Volcker, Paul A., The National Commission on the Public Service, (January 2003), http://www.brookings.edu/dybdocroot/GS/CPS/Volcker/reportfinal.pdf. <accessed 10 February 2003.

Volcker, Paul A., "Speech to the National Press Club" January 13 2003, Government Executive, (February 2003). 6.

Warf, Barney. Information Age Anthology "Telecommunications and the changing Geographics of Knowledge Transmission in the late 20th Century", (2002): Chapter 20.