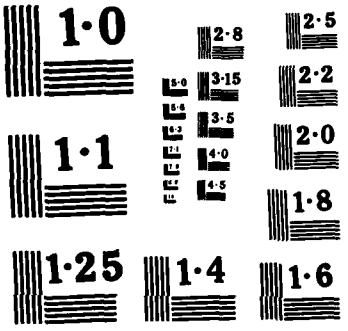
AD-A158 160 LEARNING TO LIVE WITH DIVESTITURE(U) ARMY WAR COLL CARLISLE BARRACKS PA J J RUDIGIER 30 APR 85 1/1

UNCLASSIFIED F/G 5/1 NL



NATIONAL BUREAU OF STANDARDS
MICROCOPY RESOLUTION TEST CHART

(2)

STUDENT ESSAY

LEARNING TO LIVE WITH DIVESTITURE

BY

JOSEPH J. RUDIGIER

30 APRIL 1985

US ARMY WAR COLLEGE, CARLISLE BARRACKS, PENNSYLVANIA

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A158160 / 3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Learning to Live With Divestiture	5. TYPE OF REPORT & PERIOD COVERED STUDENT ESSAY
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Mr. Joseph J. Rudigier	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS US Army War College Carlisle Barracks, PA 17013-5050	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Same	12. REPORT DATE 30 April 1985
	13. NUMBER OF PAGES 27
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)	15. SECURITY CLASS. (of this report) Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution is unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The divestiture of AT&T has created many problems for the federal government and, in particular, the Defense Department. Numerous articles have been written about the negative impact of the divestiture on national security and emergency preparedness (NSEP). However, action has been taken by the executive branch in the past year in an attempt to restore telecommunications management to pre-divestiture status. In the meanwhile, the increased competition and technological improvements underway by industry have served to increase the (Cont)

robustness of NSEP telecommunications which will eventually enhance national security and emergency preparedness. In order to take advantage of the added capability, the government must continue to implement policies and develop guidance to ensure that NSEP telecommunications systems have the necessary degree of interoperability and that actions by federal agencies to acquire new systems are coordinated.

USAWC MILITARY STUDIES PROGRAM PAPER

LEARNING TO LIVE WITH DIVESTITURE

AN INDIVIDUAL ESSAY

by

Joseph J. Rudigier

Lieutenant Colonel Robert A. Holden, FA
Project Adviser

US Army War College
Carlisle Barracks, Pennsylvania 17013
30 April 1985

ABSTRACT

AUTHOR: Joseph J. Rudigier, DAC

TITLE: Learning to Live With Divestiture

FORMAT: Individual Essay

DATE: 30 April 1985 PAGES: 21 CLASSIFICATION: Unclassified

The divestiture of AT&T has created many problems for the federal government and in particular, the Defense Department. Numerous articles have been written about the negative impact of the divestiture on national security and emergency preparedness (NSEP). However action has been taken by the executive branch in the past year in an attempt to restore telecommunications management to pre-divestiture status. In the meanwhile, the increased competition and technological improvements underway by industry have served to increase the robustness of NSEP telecommunications which will eventually enhance national security and emergency preparedness. In order to take advantage of the added capability, the government must continue to implement policies and develop guidance to insure that NSEP telecommunications systems have the necessary degree of interoperability and that actions by federal agencies to acquire new systems are coordinated.

LEARNING TO LIVE WITH DIVESTITURE

The Decision

On 24 August, 1982 an historic judicial order was issued which specified how and when the divestiture of AT&T would take place. The impact of that decision on the nation was enormous in terms of cost of service to telecommunications users as well as to the security of the United States. As described by Col. George Bolling in his book AT&T Aftermath of Antitrust,[1] and in numerous other publications, the AT&T network was the national telecommunications system since it comprised approximately 80% of all the telecommunications in the U.S. The Defense Department had opposed the divestiture on the grounds that AT&T was the end-to-end manager of national security and emergency preparedness (NSEP) telecommunications (see appendix for definition) and would be unable to serve as the nation's telecommunications manager under the terms of the divestiture.

Computer Inquiry II

Within five months of the divestiture order, another momentous decision rocked the government telecommunications agencies. The landmark Computer Inquiry II decision of the Federal Communications Commission, which was implemented in January, 1983, exacerbated the management problems of the

government. It allowed AT&T to market computers but prohibited AT&T Communications Corp. (the old AT&T Long Lines Division) from providing customer premise equipment and thereby further fragmenting management of the network.[2]

The Defense Department was neither staffed nor funded to deal with a multiplicity of industry communications managers in a national emergency. Neither were there operating procedures in the government to provide for the necessary coordination among the various companies involved after divestiture. Likewise the companies did not have sufficient personnel or procedures to take on the new management and billing responsibilities. After divestiture went into effect, the lead time for ordering long distance service for DoD increased from 30 days to 160 days because of the shift in responsibilities and fragmentation of effort. The backlog of orders is being reduced by the companies, but it is still a serious problem. The complexities of acquiring new service in an environment of dozens of vendors has caused difficulties for those federal agencies responsible for such acquisitions. Some of the new vendors complained that existing facilities owned by an incumbent contractor gives the incumbent an unfair advantage which caused DCA to obtain a legal ruling that the government has no responsibility to equalize bidders as long as information on those facilities is made available to all.

To compound the problem, there was no single manager of communications in the federal government. NSEP telecommunications consists of a conglomeration of networks paid for and controlled by DoD, FEMA, FAA, NASA, GSA, Department of State, and others. For the past twenty years the National Communications System (NCS) in the Defense Communications Agency (DCA) has been trying to coordinate efforts of the agencies involved and in the process develop technical standards to allow the systems to interoperate. Up until 1981 the NCS was woefully underfunded and inadequately staffed to accomplish that important mission.

In 1983, the first year of divestiture, the ability of the federal government to control NSEP telecommunications was very limited. As Col. Robert Reinman says in his monograph National Emergency Telecommunications Policy: Who's in Charge?

> No one is in charge; regulations and directives have grown to the point where no single person or group is making national emergency telecommunications policy with a clear Presidential or Congressional mandate. This has caused a dangerous lack of progress toward establishing readiness for national emergencies. Each organization involved is trying to carry out its assigned responsibilities, but the responsibilities are inadequately specified and overlap.[3]

TIGHTENING UP IN 84

Executive Order 12472

Although management responsibilities were unclear in 1983, the situation began to improve in 1984. On April third, President Reagan signed Executive Order 12472 which provides for the consolidation of assignment and responsibility for improved execution of national security and emergency preparedness telecommunications functions. Although the National Communications System was created on August 21, 1963 by a presidential memorandum, EO 12472 establishes it as a legitimate government agency (the presidential memorandum does not have that authority). It also confirms the positions of NCS Executive Agent and NCS Manager and establishes an NCS Committee of Principals.

The Committee of Principals consists of representatives from Federal departments, agencies and entities, as designated by the President. The designated activities are those that lease or own telecommunications facilities or services of significance to national security or emergency preparedness. Also assigned to the committee are representatives of appropriate policy, regulatory and enforcement entities of the executive branch. The primary purpose of the Committee of Principals is to provide a forum for coordination and oversight of the multitude of telecommunications programs of the Federal government. The Secretary of Defense is officially designated as Executive Agent and is once again charged with naming the manager of the NCS.

The executive order gives to the NCS the mission of ensuring that a national telecommunications infrastructure is developed which is responsive to the nation's security and emergency needs and can satisfy priority requirements under all circumstances. It also requires that the infrastructure incorporate the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and security to obtain survivability in all circumstances. That is a tall order! To accomplish that difficult task requires, among other things, a great deal of coordination and cooperation among companies who are now competitors and who must be sensitive to antitrust laws.

EO 12472 also clarifies roles and relationships among other government agencies that are involved in national telecommunications management. Specifically it defines the management and technical responsibilities of the departments of Commerce, State, Defense and Justice, FEMA, CIA, GSA and the FCC.

One of the most significant results of EO 12472 was the establishment of a National Security Telecommunications Advisory Council (NSTAC). Comprised of 30 high ranking representatives of the telecommunications industry, the NSTAC advises the President and the Executive Agent of the NCS on

planning and implementation options for national security telecommunications. The NSTAC meets several times each year and has succeeded in bringing to the President's attention some of the more serious NSEP telecommunications problems.

The National Coordinating Center

EO 12472 also addresses what George Bolling and others have identified as the most critical problem for national security as a result of divestiture - the loss of the single manager of the telecommunications network which the nation has enjoyed since the network was created. The executive order directs NCS to create a joint industry-government National Coordinating Center (NCC) to assist in the initiation, coordination, restoration and reconstitution of NSEP telecommunications under all conditions of crisis or emergency. The manager of the NCS immediately established a colocated NCC with a manager, a deputy manager and a small full time staff. These positions were created from assets of the NCS and FEMA.

In addition, the NCC includes representatives from government agencies who have responsibility for portions of NSEP telecommunications. Also included are representatives from twelve of the principal communications companies involved. The industry representatives are from American Satellite Corp., AT&T, Bell Communications Research, Inc., COMSAT, GTE,

ITT, MCI, Pacific Telecom, RCA, TRT Communications Corp., U.S. Telephone Association, and Western Union. The government agencies represented are GSA, Departments of Defense, Interior, Transportation, State, Commerce, Energy, Agriculture, Treasury and Justice, NASA, CIA, FEMA, U.S. Information Agency, National Telecommunications and Information Administration, OJCS, NSA, and the VA. The government representation reflects the membership of the NCS. Some of the agency representatives actively assigned to the NCS also represent their agencies in the NCC.

The industry representatives have computer terminals in the NCC connected to their company's operating centers. Unless the responsible government activity is having difficulty meeting its NSEP communications requirements, the NCC doesn't get involved. If high level attention is required, the NCC manager will work with the members of the center to solve the problem. In its first year of operation the NCC provided assistance in forty plus cases.[4] NCC representatives are jointly developing service restoration and network configuration contingency plans for specific natural disasters such as a California earthquake. Exercises are also being conducted to test and improve the plans.

Accomplishments of the NCC thus far include the completion of a definitional framework for identifying NSEP telecom-

mix of media is possible. However in order to take advantage of the inherent redundancy, the various networks must be interoperable. Before divestiture the Bell System Practices were the de facto technical standards for the industry. If a non-AT&T company wanted to interconnect with the Bell system, it had to comply with those practices. What will happen in the future? Will the government establish standards for the industry? I doubt it. As long as AT&T dominates the business, other companies will follow suit technically much as the computer industry has done in following the lead of IBM. But there are no guarantees. As telecommunications networks become more and more computer oriented as they have for the past twenty years, software compatibility becomes increasingly important. AT&T does not hold the same dominant position in establishing software protocols as it holds in engineering parameters.

CONCLUSIONS

As George Bolling and Robert Reinman described in their papers, the management of the national telecommunications network was significantly degraded by the divestiture decision. It now appears that the government is taking steps to correct some of the more serious problems, particularly in the policymaking and crisis management arenas. Certainly the active participation of the telecommunications industry in that effort is vital to success. As Dr. John L. Boyes said

place, the degradation should be minimized, although that remains to be seen because DNHR offers fewer routing possibilities from any one node.

AT&T was also awarded contracts to analyze and test the vulnerability of major equipments develop hardening techniques against electromagnetic pulse (EMP) for selected equipments such as their T carrier and optical fiber systems.

In times of national crisis, it is essential to be able to control the network from a central point. AT&T has a network operations center (NOC) in Bedminster, N.J. from which the network is monitored and reconfiguration orders are issued during peacetime. The company has also constructed an alternate NOC in a hardened facility in New Jersey to survive a nuclear attack. In addition, the company maintains an emergency status center in Washington, D.C. and a hardened alternate facility in suburban Maryland. As a result, when the management problems facing the federal government are finally solved, there are already in place many of the necessary tools to manage the bulk of the network in times of national emergency.

Interoperability

Competition does enhance the robustness of the network in that more paths are available for transmission and a greater

losing business to "no frills" competitors.

If defense communications are to survive attack, either by terrorists or by more "conventional" (including nuclear) forces, the network must either be hardened or redundant or both. As stated in a 1984 report by the Center for Strategic and International Studies of Georgetown University

> Communications networks, an essential tool for the management of national crisis, of other types of networks, and of commerce, are particularly susceptible to human interference.[7]

and also

> The continued functioning of essential networks - or their rapid restoration to proper functioning after failure - can be facilitated by a variety of measures. Physical protection can avert problems. Network redundancy can permit bypassing a failed link. Stockpiles of spare parts can speed up repairs. Insurance can help compensate for abnormal costs. Risk analysis can be used to evaluate the perils faced and the countermeasures thus justified. Contingency planning and simulation can prepare managers to cope efficiently with emergencies. But all countermeasures require some investment of time and money, and thus the pressure of market competition militates strongly against them.[8]

In other words, if the government insists on competition in telecommunications, it must be prepared to pay the price to increase survivability.

How survivable is the network? An examination of the network hierarchy shows that due to the locations of the higher level switching centers, they are the least likely to survive a nuclear attack. The majority of the lower level nodes should survive however. With dynamic non-hierarchical routing in

terrestrial radio links including cellular radio are steadily increasing in number. If the DoD and industry can solve the management problem, there is a rich mixture of capabilities available which provides for a robust telecommunications network in times of national emergency. Another important technology being introduced into the network is common channel signalling (CCS) which increases the control of the manager and the flexibility of the network. CCS is made possible by the evolution of the network from analog to digital.

Survivability of the network

When AT&T was our "telephone company", the facilities used in the network were designed to last a long time and were, in many instances, overdesigned to allow for expansion and to withstand extreme environmental conditions. Also many key microwave and switching centers incorporated a nominal amount of "hardness" to survive in times of emergency. Concrete and steel were not spared! The costs for these facilities were included in the rate base. Now that AT&T is competing against an ever-increasing number of common carriers that are offering a wide variety of services over various types of transmission systems, the company is under pressure to get "lean and mean." What this portends for future facility design remains to be seen, but certainly the company cannot continue to overdesign plants if they are going to avoid

AT&T and other major companies are also looking at the future integration of voice and data into one network. AT&T's plan is to evolve their system into the Integrated Services Digital Network (ISDN) over a period of years. When other vendors are involved, careful coordination of upgrades will be required.

AT&T is in the process of converting their hierarchical network to a non hierarchical network by the addition of new routing algorithms to their #4ESS offices. This new capability is called dynamic non hierarchical routing (DNHR) and makes it possible for calls to be routed automatically much more efficiently without switching the call upward through the hierarchy under call blocking conditions. DNHR will change route tables ten times a day to accommodate changing traffic patterns.

Other improvements in telecommunications technology have augmented NSEP telecommunications. For example, it is now possible to space repeaters on optical fiber cables up to 100 miles which increases reliability and maintainability of the system. AT&T is preparing to lay a transoceanic optical fiber cable to the U.K. with service beginning in 1988. A much greater variety of transmission media is now commercially available to telecommunications users. Satellite, optical fiber, wire and coaxial cable and

multiple billings and determining which vendor is responsible when service is degraded or lost. The DoD has not yet learned how to deal efficiently in the multivendor environment. Undoubtedly the government pays a significant management fee in order to lease service from a single vendor. Whether it is cost-effective for the government to do that job in-house remains to be seen. In the meanwhile, DECCO invited industry to offer end-to-end (circuit and terminal equipment) service. So far only three companies responded positively to that invitation - AT&T Information Systems, GTE Service Corporation and Western Union.

Improvements in the commercial network

As the DoD is developing the final architecture of the DSN in the western hemisphere, the telecommunications industry is reconfiguring the national network and maneuvering to gain competitive advantages. AT&T has filed for a tariff for a software defined network which may be implemented in the DCTN Level II. AT&T has also proposed it to the DoD for the DSN. The software defined network would take advantage of the capabilities of the large number of computers that AT&T now has in their network for switching circuits. By properly programming network switching centers, network reconfigurations can be done automatically to meet the needs of a variety of high priorty customers.

equipment suppliers at the same time as it is trying to transition to new state-of-the-art voice and data networks. While the system design is being finalized, the government is studying acquisition alternatives in order to come up with the most cost effective and manageable strategy for acquiring the new system. Undoubtedly it will be the most complicated acquisition of telecommunications ever undertaken by the federal government.

Defense communications in the U.S. consists mostly of circuits and equipment leased from the telecommunications industry by the Defense Commercial Communications Office (DECCO). Because of the large number of companies now offering telecommunications and long distance service (400 at last count[6]), DECCO was authorized in November, 1984 to purchase as well as lease equipment. DECCO provides four basic lease or buy services to DoD telecommunications users - equipment only, circuits only, networks and systems (e.g. DDN), and circuits with terminal equipment.

There is some unhappiness in the industry with the way the DoD acquires long distance communications. Most of the DoD customers who need circuits and terminal equipment would prefer to deal with one company for end-to-end service rather than a number of separate companies. When more than one company is involved, the government has the problem of

March, 1984 for the Defense Commercial Telecommunications Network (DCTN). When complete, the DCTN will mix voice, data, and video service into one integrated network. Level I of DCTN includes fifteen nodal voice switches (ESS#5) and nine colocated satellite ground stations and will enable DCA to off-load onto DCTN up to 50% of its AUTOVON routine traffic. The video service will be digital and near full motion color at 1.544 Megabits per second. Level I includes two video networks, one for the Chief of Staff, Army and one for the commander, Army Materiel Command using satellite links and a low level of encryption via the Digital Encryption Standard (DES). Also included in Level I are wideband and narrowband data (4.8 kilobits per second) circuits, some dedicated and some switched. The DDN will also use the DCTN digital data switches.

Level II of the DCTN may be ordered by the government after Level I has been implemented. It will add five more ESS#5 multifunction switches and will off-load more of the routine AUTOVON traffic. AT&T will manage and maintain the DCTN from their facility in Dranesville, Va.

Divestiture and the DSN

The divestiture of AT&T couldn't have come at a worst time for DoD. As a result of divestiture, the government is required to deal with a large number of common carriers and

the U.S. will use a larger number of smaller switches than AUTOVON which will reduce the distance from the user to the nearest switch. As a result, the cost to the user should be less for the DSN. Unlike AUTOVON which uses large switches dedicated to AUTOVON, the DSN will use mostly multifunction switches located on military installations. These multifunction switches will provide day-to-day telephone service to personnel on the installation as well as provide the DSN long distance switching functions. This should save personnel and money. Users of AUTOVON pay fixed access line charges whereas charges for DSN will vary according to usage (a much more equitable billing arrangement).

Data communications

Eventually the DSN will be integrated with the packet switched network that is being used for data communications in the Defense Digital Network (DDN). The DDN is the successor to AUTODIN which will be phased out. In other words the future defense communications system will be a fully integrated voice and data network but will still rely heavily on commercial telecommunications in the U.S.

A step towards integrated service

While planning for the DSN in the continental U.S. continues, the DoD has taken a first major step toward implementation in the U.S. A contract was competitively awarded to AT&T in

switches is twenty years old.

Future defense communications

Although DCA had a long range plan for replacing AUTOVON, it wasn't until the costs escalated sharply that the agency shifted into high gear. In 1981 the Assistant Chief of Staff for Command, Control, Communications and Intelligence in OSD tasked DCA to begin planning to replace AUTOVON with a new system to be called the Defense Switched Network (DSN). The DSN is now in the final stages of design and the early stages of implementation. Unlike the original AUTOVON, it will include a significant amount of command and control telecommunications. The design of the system in the Pacific and in Europe is complete and implementation has started.

The first phase of the DSN began with the European Telephone System (ETS), an Army program to replace 120 antiquated telephone switches in Germany. Five of the 120 switches will be DSN nodal switches. The Air Force will expand ETS to other countries and will incorporate more DSN switches. The Army also has a major telephone switch replacement program underway in South Korea. There will be four DSN nodal switches in that country.

The final western hemisphere network architecture will be completed this summer and will incorporate some satellite communications links for increased survivability. The DSN in

CHANGES IN THE NETWORK

Defense communications

Altogether there are in excess of fifty telecommunications systems that are considered by DCA to affect national security and emergency preparedness. Three of these are major networks of the Defense Communications System - the Automatic Voice Network (AUTOVON), the Automatic Digital Network (AUTODIN) and the Automatic Secure Voice Network (AUTOSEVOCOM). All three use the commercial telecommunications network in the continental U.S. and are managed by DCA. Each of the three networks uses a unique electronic switching system especially designed to meet the needs of the DoD.

AUTOVON is the primary administrative telephone system for the Defense Department. It also provides some command and contol communications. Because of the elimination of the TELPAK rates (special discounted rates for the DoD) by the FCC several years ago, the cost of AUTOVON skyrocketed. One reason for the high cost is that there are only 53 AUTOVON switches in the continental U.S. Because of the limited number of switches, the access lines from the users to the switches are quite long in many cases. Since the access line charge is based on distance, the cost to the user is very high. In addition the technology used in the AUTOVON

2. Joint Chiefs of Staff Alerting Network (JCSAN)
3. Minuteman
4. SAC Primary Alerting System (PAS)
5. SAC Command Post C2 Consoles (Turret)
6. SAC Operations Conference System (SOCS)
7. NORAD Alerting System (NAS)
8. TAC C2 Alerting System (TACCALS)
9. TAC Force Control Management System (TACNET)
10. MAC Operational Phone System (MACOPS)
11. Air Force Digital Graphics System (AFDIGS)
12. Air Force Command Post Alerting Network (COPAN)
13. Air Force Command Post Record Capability (COPREC)
14. White House Communications Agency Transportable Electric Consoles (TEC)
15. White House Communications Agency Echo Fox Radio System
16. U.S. National Airspace System
17. FEMA (classified system)
18. Emergency Broadcast System
19. FEMA National Voice System (FNAVS)
20. FEMA National Warning System
21. Nuclear Regulatory Commission Emergency Notification System (ENS)

At least for these 21 systems, DoD has a single commercial manager to deal with for end-to-end control of the networks.

failed to get White House support and died after hearings were held by the Communications Subcommittee of the Senate Commerce Committee.

FCC Docket 94-652

As stated earlier, under the Computer Inquiry II decision, AT&T-C was prohibited from providing and maintaining customer premise equipment (CPE). This meant that AT&T could not provide end-to-end service. Since the government was not prepared to take on that job in-house, NSEP telecommunications were adversely impacted. At the request of DoD and other federal agencies responsible for NSEP telecommunications, AT&T petitioned FCC for a waiver of Computer Inquiry II to allow the company to be responsible for end-to-end service including providing any new CPE for 21 specific NSEP systems. The FCC held hearings, considered options and approved the request in 1984. As a result, FCC Docket 94-652 went into effect 1 January, 1985 granting AT&T the requested waiver and also permitting the Bell Operating Companies (BOC's) to provide and service CPE for the systems.[5] This was another step in increasing national security, at least to the level that existed before divestiture for the 21 systems. The systems covered, which include some command and control circuits, are:

1. Automatic Secure Voice Communications Network (AUTOSEVOCOM)

munications requirements as shown in the appendix and a draft NSEP telecommunications procedures manual.

Telecommunications policymaking

The executive order also tasks the National Security Council with providing policy direction for the exercise of the war power function of the President under Section 606(a),(c)-(e), of the Communications Act of 1934. In addition, it tasks the Director, Office of Science and Technology Policy (OSTP) with directing the exercise of the war power functions of the President under the same section of the Act of 1934. Thus, telecommunications policy will be made in the executive office of the President.

In 1984 a position was established in the executive office of the President to provide telecommunications advice to the National Security Council. In November, 1984 Mr. John Grimes was placed in that position. Mr. Grimes was formerly the Deputy Manager of the NCS. In his new job, Mr. Grimes wears three hats - Director, National Security Telecommunications; Director, Defense Programs - National Telecommunications; and Director, National Crisis Management Center.

A similar effort by the Senate in 1983 (Senate bill S.999) to establish a high level policymaking position in the executive office of the President with rank equivalent to ambassador

in July 1984:

> The threat to national security can be very real in that a very few telecommunications vendors now have become many, with many offerings and services, and with, perhaps, a lesser degree of long-term responsibility than before.
>
> The opportinity lies in the potentials of gaining additional telecommunications systems robustness and enhanced overall survivability of the national telecommuniction infrastructure through the skills and energies and the new technologies of the many working together.[9]

The network modernization efforts of the government and industry taking advantage of new technology can enhance the ability of the responsible managers to provide the necessary service in times of national crisis. A great deal depends on the acquisition strategy that is finally selected for the Defense Switched Network. It is critical to national security that the future defense communications system be rapidly reconfigurable in times of stress and under the control of a single industry manager who is responsive to the needs of the government. Although management problems, both in government and in industry remain, the recognition of those problems has reached the highest levels of government and improvements are being made.

Recommendations

In a paper published in 1978, Forrest P. Chisman, Director of Plans and Policy Coordination at the National Telecommunications and Information Administration of the Department of Commerce, wrote

> There is therefore a need for some form of integration and forward-looking leadership; by default if not by immutable constitutional plan, that requirement falls on the executive.[10]

Although written before the divestiture decision, those words are even more appropriate today. The first steps have been taken toward the establishment of a management structure within the executive branch of the federal government to insure that NSEP telecommunications are operational in times of crisis. However, as described in this paper, there are problems remaining.

The new office of the National Security Telecommunications Director in the White House; the NSTAC; the NCS Committee of Principals and the NCC provide the necessary structure. What remains to be done is to see that the following tasks, as a minimum, are accomplished:

-Coordinate the efforts of the telecommunications industry in areas that affect NSEP.

-Review and approve the major telecommunications plans of all federal agencies involved in NSEP telecommunications.

-Develop policies that will insure the necessary amount of interoperability among competing networks.

-Pay for hardening and alternate routes where necessary.

-Monitor new technology developments and disseminate information to all NSEP telecommunications federal agencies.

-Develop and promulgate guidance on telecommunications network planning including inter operability standards.

-Develop and maintain a data base of NSEP telecommunications resources.

-Oversee the integration of industry network controls to achieve the required degree of survivability.

Most of the above tasks are within the charter of the NCS. The funds allotted to the NCS have increased significantly since 1981 and must be maintained at the required level if progress in this critical area is to continue.

ENDNOTES

1. George H. Bolling, AT&T Aftermath of Antitrust, National Defense University, Washington, D.C., 1983, p.22

2. Robert A. Reinman, National Emergency Telecommunications Policy: Who's in Charge?, National Defense University, Washington, D.C., 1984

3. Ibid, p.33

4. William B. Belford, speech at the Armed Forces Communications Electronics Association West Conference, Los Angeles, January, 1985

5. Federal Register, January 11, 1985, pp.1526-1534

6. Wall Street Journal, July 31, 1984, p.37

7. The Center for Strategic and InternationalStudies, Science and Technology Committee, panel on Crisis Management, America's Hidden Vulnerabilities: Crisis Management in a Society of Networks, 1984, p. 7.

8. Ibid., P. 9.

9. Dr. John L. Boyes, Signal, July, 1984, p. 11.

10. Forrest Chisman, "The Executive Branch", Communications For Tomorrow, 1978, p. 403.

COMMERCIAL TELECOMMUNICATIONS SERVICES OR CIRCUITS WHICH MAY BE DESIGNATED NSEP*

The following four categories of commercial telecommunications services or circuits may be designated National Security or Emergency Preparedness (NSEP) Telecommunications.

1. Restoration Priority Services/Circuits

a. Any existing service or circuit which has been assigned an NCS/FCC approved restoration priority (RP) 1-4.

b. Any new service or circuit which is eligible for assignment of an NCS/FCC restoration priority (RP) 1-4.

2. Emergency Services/Circuits

Any service or circuit required in support of a presidentially declared disaster or emergency as defined in the Disaster Relief Act (42 U.S. Code § 5122), or other emergency as defined in DCA Circular 310-130-1. The latter are:

a. State of crisis declared by the National Command authorities.

b. Efforts to protect endangered U.S. personnel or property.

c. Enemy action, civil disturbance, natural disaster, or any other unpredictable occurrence that has damaged facilities whose uninterrupted operation is essential to national security or other ongoing crisis.

d. Certification by the director of a Federal agency, commander of a unified/specified command, head of a military department, or commander of a major military command, that a communications requirement is so critical to protection of life and property or to the national defense that it must be processed immediately.

3. Exercise Services/Circuits

In addition to those exercise services or circuits which qualify under the Restoration Priority or Emergency categories, the following may be designated NSEP.

a. The minimum quantity of services or circuits essential to permit safe conduct of an exercise and/or achievement of primary exercise objectives. This would include any exercise services or circuits extending and/or directly supporting any of the 21 C^3 Systems covered by the Computer II waiver. Those exercise services or circuits in support of exercises which do not involve the movement of personnel, arms, munitions or other critical materials, or the control of aircraft are not included.

b. Short-notice exercise services or circuits resulting from changes in exercise locations or scenarios which could not reasonably have been foreseen, and without which the exercise cannot be conducted safely or effectively.

4. Special Purpose Services/Circuits

In addition to those services and circuits which qualify under categories 1-3 above, the following may be designated NSEP:

a. Services or circuits in support of activities conducted pursuant to the Foreign Intelligence Surveillance Act;

b. Services or circuits in support of the President or Vice-President; and

c. Services or circuits in direct support of the conduct of foreign affairs (i.e., visiting foreign heads of state or similar dignitaries, permanent diplomatic and consular missions in the U.S., and significant international conferences, meetings, or events held in the U.S.) as certified by the Secretary of State.

*This is not intended to be a comprehensive definition of NSEP telecommunications for purposes of Executive Order No. 12472.

END

FILMED

9-85

DTIC