Incidental Paper

THE U.S. DIPLOMATIC TELECOMMUNICATIONS SYSTEM: ITS ROLE IN U.S. NATIONAL SECURITY, WAR PREVENTION, AND WAR TERMINATION

Robert P. Richardson

Program on Information Resources Policy

Harvard University

Center for Information Policy Research

Cambridge, Massachusetts

An incidental paper of the Program on Information Resources Policy.

THE U.S. DIPLOMATIC TELECOMMUNICATIONS SYSTEM: ITS ROLE IN U.S. NATIONAL SECURITY, WAR PREVENTION, AND WAR TERMINATION
Robert P. Richardson
November 1984, I-84-4

Project Director: Oswald H. Ganley

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

Robert Richardson is Director of Communications for East Asian and Pacific Affairs, Department of State.

Printing 5 4 3 2 1

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University | **Center for Information Policy Research**

Contributors

Action for Children's Television
American Broadcasting Companies, Inc.
American District Telegraph Co.
American Management Systems, Inc.
American Telephone & Telegraph Co.
Arthur D. Little, Inc.
Auerbach Publishers Inc.
Automated Marketing Systems
BellSouth Corporation
Bell Atlantic
Booz-Allen Hamilton
Canada Post
Codex Corp.
Communications Workers of America
Computer & Communications Industry Assoc.
COMSAT
Continental Cablevision, Inc.
Continental Telecom, Inc.
Coopers & Lybrand
Copley Newspapers
Cowles Media Co.
Dialog Information Services, Inc.
Digital Equipment Corp.
Direction Generale
des Telecommunications (France)
Doubleday, Inc.
Dow Jones & Co., Inc.
Dun & Bradstreet
Economics and Technology, Inc.
EIC/Intelligence Inc.
Federal Reserve Bank of Boston
France Telecom (France)
Gannett Co., Inc.
General Motors Corp.
General Telephone & Electronics
GTE Sprint Communications Corp.
Harte-Hanks Communications, Inc.
Hazel Associates
Hitachi Research Institute (Japan)
Honeywell, Inc.
Hughes Communication Services, Inc.
E.F. Hutton and Co., Inc.
Illinois Bell
IBM Corp.
Information Gatekeepers, Inc.
International Data Corp.
International Resource Development, Inc.
Invoco AB Gunnar Bergvall (Sweden)
Knowledge Industry Publications, Inc.
Kokusai Denshin Denwa Co., Ltd. (Japan)
Lee Enterprises, Inc.
John and Mary R. Markle Foundation
MCI Telecommunications, Inc.
McKinsey & Co., Inc.
Mead Data Central
MITRE Corp.
Motorola, Inc.
National Association of Letter Carriers
NCR Corp.
National Telephone Cooperative Assoc.
New England Telephone
The New York Times Co.
NEC Corp. (Japan)
Nippon Telegraph & Telephone Public
Corp. (Japan)
Northern Telecom Ltd. (Canada)
Northrop Corp.
NYNEX
Ohio Bell
The Overseas Telecommunications
Commission (Australia)
Pitney Bowes, Inc.
Public Agenda Foundation
RCA Corporation
Reader's Digest Association, Inc.
Research Institute of Telecommunications
and Economics (Japan)
Royal Bank of Canada (Canada)
Salomon Brothers
Satellite Business Systems
Scaife Family Charitable Trusts
Seiden & de Cuevas, Inc.
Southwestern Bell Corp.
Telecom Futures, Inc.
Telecommunications Research
Action Center (TRAC)
Time Inc.
Times Mirror Co.
Times Publishing Co.
TRW Inc.
United States Government:
Central Intelligence Agency
Department of Commerce:
National Oceanographic and
Atmospheric Administration
National Telecommunications and
Information Administration
Department of Energy
Department of State
Office of Communications
Federal Communications Commission
Federal Emergency Management Agency
Internal Revenue Service
National Aeronautics and Space Admin.
National Security Agency
United States Information Agency
United States Postal Rate Commission
United States Postal Service
US - Japan Foundation
US West
United Telecommunications, Inc.
The Washington Post Co.
Western Union
Wolters Samsom Group (Holland)

ACKNOWLEDGMENTS

Special thanks are due to the following persons who were particularly helpful with background information, comments, counsel, and encouragement during the preparation of this paper.

Stuart E. Branch

Joe H. Chaddic

Hermann F. Eilts

Sabine Quitslund

Thomas J. Ramsey

Robert C. Ribera

The above persons and the Program's affiliates are not, however, responsible for, nor do they necessarily agree with, the views expressed herein. Any errors of fact or interpretation are mine.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

To review the status of the Diplomatic Telecommunications System (DTS) in the context of U.S. national security, this paper examines the purpose of DTS, its strengths, its weaknesses, and its capability to remain operational under stress conditions.

ISSUES

- Why is the DTS essential to policymakers at the highest level of the U.S. government in the formulation and implementation of foreign policy?

- What is Executive Branch policy concerning a secure and reliable telecommunications capability overseas?

- How can the DTS be enhanced and hardened to ensure its survivability, particularly in times of stress?

- What is the status of enhancement and modernization programs?

FINDINGS

The present Administration's policy and concern regarding National Security and Emergency Preparedness of Telecommunications follows a long tradition going back to the First Continental Congress. NSDD-97 and E.O.# 12472 have affirmed the goals of the Administration's national security telecommunications policy which are to establish a survivable telecommunications infrastructure able to support the national security of the country, utilizing the nation's domestic and international telecommunications resources. Thus, the purpose of a Telecommunications System in support of diplomacy has been mandated.

Today's needs are infinitely more complex and critical than in the past. Richard Beal, Senior Director for Crisis Management Systems and Planning at the White House, said in an interview with Science:

"...on such tasks as the notification of allies before a major new military or political initiative 'In a crisis, two hours is the difference between notification and a failure to notify....'" Hence, the capability to exchange information in a secure and real time basis with any government on the globe and/or U.S. representative abroad is a crucial factor in the decision-making process.

The DTS is a viable, sophisticated, modern organization. However, it is lean and potentially vulnerable to disruptions under various stress conditions, such as fire, earthquakes, civil disorders, industrial strikes, or terrorist acts. The principal weaknesses continue to be a lack of circuit redundancy, physical security, and restorability.

The Department of State (DOS) is aware of the vulnerability of its communications system. In accordance with the policy of NSDD-97, it is seeking to improve the reliability and survivability of the system. In 1983, DOS asked the National Communications System (NCS) to obtain the assistance of the National Security Telecommunications Advisory Committee (NSTAC). The NSTAC Industry Executive Subcommittee subsequently established an International Diplomatic Telecommunications (IDT) Task Force and directed the Task Force to address the issues of U.S. leased telecommunications service overseas and diplomatic telecommunications service in the U.S. Other DOS initiatives have been the introduction of automated software terminals, electronic storage, centralized data bases, higher speed and wider bandwidth, negotiations with foreign governments regarding

the security posture of leased telecommunications facilities, and restoration priorities for U.S. and foreign diplomatic missions.

The infrastructure necessary to carry out the Executive Branch policy is in place. The implementation of the enhancement and modernization programs is progressing within the usual bureaucratic budgetary constraints. However, a successful outcome will depend very much upon the level of national support.

1. INTRODUCTION

This paper identifies national policies relating to telecommunications facilities that support the conduct of foreign affairs and discusses policy implementation to date. A primary focus is the Diplomatic Telecommunications System (DTS), the only U.S. government telecommunications system operational on a worldwide basis, reaching such cities as Bejing, Moscow, Paris, and Pretoria. We will examine the DTS in the following contexts:

- o Its responsibilities to Executive branch policy regarding national security and emergency preparedness of U.S. telecommunications functions.
- o Its global role in the conduct of foreign relations, Presidential initiatives, exchange of information, and war-preventing, war-terminating functions.
- o Its strengths, weaknesses, and sustainability under stress conditions.
- o Its ability to provide Command and Control authorities with fast, secure, and reliable telecommunications facilities worldwide.
- o Its capabilities today and the needs of tomorrow.

It is critical that the survivability of the DTS be ensured, particularly in times of stress. For example, the Secretary of State, in his capacity as senior advisor to the President on foreign affairs, must use it to communicate with allies, neutrals, and enemies. Moreover, the DTS not only services the State Department but shares its facilities with over 50 federal departments and agencies. Thus, it affects the

entire spectrum of the U.S. government operations abroad and decision making at home.

The conduct of foreign affairs in our time requires a constant flow of information. Distance and time no longer limit the propagation of world events. Worldwide media services transmit policy announcements, public statements, and news almost instantaneously to millions around the globe.

Crises arise with unpredictable and alarming frequency, and in most instances the U.S. government becomes involved, whatever the issue may be. The continental United States itself is potentially threatened by foreign adversaries or terrorists. In the event of a crisis, policymakers have only a very short reaction time.

Over the years the federal government has acted to establish and improve national emergency preparedness capabilities, including those of emergency communications. A paper prepared by the MITRE Corporation, entitled "Evolution of Emergency Communications Roles and Responsibilities" states that heightened concern about our nation's overall state of emergency preparedness has coincided with an increased awareness of its critical reliance on advanced telecommunications and teleprocessing systems, the potential vulnerability of these systems, and the vital nature of telecommunications support in emergency situations. This concern has arisen during a period of great instability in the telecommunications industry brought about by increased foreign and domestic competition, the restructuring of organizations and markets, changing regulatory policies, and continuing technological development. Thus, federal efforts to enhance emergency communications capabilities are unfolding in an environment characterized both by urgent national

security emergency preparedness needs and by considerable industry uncertainty.[1]

However, the thrust of the federal programs designed to improve emergency communications capabilities has been primarily directed toward the domestic and military scenes. The need to enhance U.S. government emergency communications abroad has been recognized; its significance is only beginning to emerge.

2. MISSION

The Secretary of State is the senior advisor to the President of the United States on foreign affairs. In addition, many other policymakers including the President, the National Security advisor, the Secretary of Defense, a host of other Cabinet officers, heads of agencies, and Congress participate in formulating foreign policy.

The complexity of policymaking and the diversity of interests and opinions among key players require extensive research and consultation not only within the U.S. government but also with allied and neutral nations. Almost every issue affects domestic and international politics, public relations, and military, economic, and social subjects.

The role of the American Ambassador, as the personal representative of the President, is to inform foreign governments of proposed U.S. initiatives; explain, negotiate, and win support for the U.S. proposals; advise Washington decision makers of any pitfalls, and anticipate official and public reactions of the host country to the proposed course of action, as well as its impact on our relations elsewhere in the region. The Ambassador and his staff must report the conditions and analyze the developments of political, economic, social, military, and diplomatic activities in the host country.

The State Department is responsible for planning, implementing, operating, and maintaining a worldwide telecommunications system capable of supporting U.S. diplomacy and about 50 federal departments and agencies located at 253 U.S. diplomatic and consular posts overseas. In this connection, it is noteworthy that about 18% of the entire State

Department staff (including support personnel providing administrative, communications, and security services) is located at overseas missions.

Executive Order No. 12472, dated April 3, 1984, defines and clarifies the State Department's mission and responsibilities regarding national security and emergency preparedness of telecommunications functions to provide for the needs of U.S. diplomacy and foreign affairs community, under all conditions of stress and emergency. This Order consolidates a number of previously issued Presidential Directives and National Security Decision Directives and mandates certain federal departments and agencies to establish a survivable domestic and international telecommunications infrastructure that will have the capability to support U.S. national security needs.

3. BACKGROUND

The Diplomatic Telecommunications System (DTS) was created in 1963 as a direct result of the failure of the Department of State (DOS) communications system during the Cuban Missile Crisis.

The events surrounding the Cuban Missile Crisis and the political impact of the communications failure during critical negotiations have been the subject of numerous comments and publications. During a 1980 seminar on Command, Control, Communications and Intelligence (C^3I) Raymond Tate said:

> ...[events that occurred] when John Kennedy was President during the Cuban Missile Crisis [have] led to many of the activities we will discuss today. Kennedy's ability to negotiate and carry out a big portion of the President's responsibilities failed during the Cuban Crisis because of communications. He was, for example, totally unable, in the time period available at that time, to advise every South American Ambassador through the State Department that he was going to invoke the Monroe Doctrine - that he was going to take positive action against Krushchev's introduction of missiles that he thought were offensive into the island of Cuba. That system literally fell on its face, not only to his chagrin, but to his outright rage....[2]

Francis W. A'Hearn reported in The Information Arsenal: C^3I Profile "Kennedy is said to have experienced difficulty in communicating through military and diplomatic channels with several Latin American countries."[3]

In a Harvard University seminar held by the Program on Information Resources Policy, Lee Paschall termed communication problems with various Ambassadors "absolutely appalling."[4]

Robert F. Kennedy said in Thirteen Days: Cuban Missile Crisis:

> Diplomatic effort was of great significance. We were able to establish a firm legal foundation for our action under the OAS charter, and our position around the world

> was greatly strengthened when the Organization of American States unanimously supported the recommendation for a quarantine. France, England and Germany also supported this decision.[3]

Several investigations and a complete reorganization of the State Department's communications facilities followed the Cuban Missile Crisis. Even prior to 1963, these facilities were in a deplorable state. Although there were a few leased circuits and Defense Communications System (DCS) circuit allocations, most posts communicated to and from Washington through the local telegraph office. In many instances, messages were hand-carried to a post office which then conveyed the message when and how it saw fit. Twenty-four hour transmission time was considered excellent! And many post offices completely closed for weekends and holidays.

The situation in Moscow at the time of the Cuban Crisis illustrates a typical communications problem. The U.S. Embassy's communications were strictly limited to commercial facilities that transmitted messages via a low-speed leased teletype circuit between the Embassy and the Soviet Post Telephone and Telegraph (PTT). However, the Soviets were able to hold messages indefinitely before transmitting them, which they did. Traffic to and from Moscow was routinely encrypted, whether classified or not, but occasionally a note from the Foreign Ministry would be sent in plain text as well as in encrypted form. Invariably, the plain text message reached Washington hours <u>after</u> the encrypted one! Apparently, clear messages were held until Soviet authorities had reviewed their content. To avoid such problems, the State Department had actively sought to obtain a full-time, full-duplex, low-speed commercial teletype circuit between Washington and Moscow. The Soviets denied the request until 1964 when Ambassador Kohler raised the question once again and Foreign Minister Gromyko informed him that the matter

had received favorable consideration and that the U.S. Embassy should contact the Ministry of Communictions for implementation. The Embassy immediately dispatched its Communications Officer [this author] and a senior officer (a Soviet expert who spoke flawless Russian) to the Ministry of Communications where they were received by a large, solemn group of Soviet communications personnel. As the discussion progressed it became increasingly clear that the Soviets were offering a telex terminal rather than a dedicated leased circuit so the Communications Officer asked if the telex would pass "scrambled tapes" intact. The senior officer, who was translating, shook his head and warned the Communications Officer in English: "Shh... how can I translate this? I don't even know what it means in English." A few smiles appeared, then the discussion continued partly in English. It was finally established that only a telex terminal would be made available to the U.S. Embassy. The terminal was a small improvement since it assured the Embassy and the DOS that messages had been received without Soviet-imposed delays, but it sometimes took hours to obtain a telex connection.

Another example of DOS communications problems abroad occurred at the U.S. Embassy in New Delhi, India during the Chinese invasion in November 1962. At that time the Embassy had a 50 Baud leased teletype circuit to the U.S. Embassy in London. The U.S. government provided massive military assistance to India and, despite the fact that the U.S. Air Force flew in a mobile communications van (HF) communications team of some 20 men, the Embassy's communications capability was limited. Its low speed leased teletype circuit was manifestly insufficient to handle, on a real time basis, the extraordinary amount of high-precedence telegraphic traffic flowing into and out of DOS, the

Department of Defense, the U.S. Air Force, the U.S. Army, and the U.S. Embassy in New Delhi. The matter was further aggravated by the limited effectiveness of the U.S. Air Force's mobile communications station; propagation conditions allowed clear transmission only a few hours a day. Therefore, most military traffic was passed through DOS channels that were reliable, if slow. But, Command and Control functions lacked the timely communications support they require in times of crisis.

Since 1963 the DTS has undertaken a course of incremental modernization. A summary of its most significant accomplishments to date follows:

- Manual and electro-mechanical off-line systems have been largely eliminated, except at consular posts, and replaced with on-line, high speed automated software terminal systems.
- The Terminal Equipment Replacement Program (TERP) played a major role in automating the DTS. TERP I became operational in 1977 and provided an automated software terminal and limited cassette drive storage, eliminated labor intensive functions, and replaced obsolete limited application electro-mechanical equipment.

  TERP II was introduced in 1979 and added computer time memory access, unattended operation, increased software functions, and increased storage capacity introduction of floppy disks instead of cassette drives.

  In 1981 TERP III provided further enhancements such as file management, added security features, reduction of paper holdings, large storage capability, higher speed, and the capability for future end user automation.

TERP III B was introduced in 1983. When associated with the WANG 7550T system it becomes the Classified Information Handling System (CIHS). Both systems are interfaced with fiber optics and capable of supporting 32 input/output ports for end user work stations. Standard software for the TERP III B system includes classified word processing, glossary, word searches, spelling verification, supervisory functions, visual memory, notebook, telecommunications, and time management. TERP III B has an electronic mailbox that handles interoffice mail; an electronic file cabinet for on-line text and information retrieval, word processing capability that allows speedy text creation and/or corrections; computational, data processing, and desktop message transmission/-retrieval capabilities; and a centralized data base for all users. It is a complete distribution information system.

- In the early 1970s the DOS established a government owned communications network in Africa that utilizes HF and satellite systems.
- The High Speed Program began in 1977 and continues to date. It connects major U.S. Embassies with Washington via leased commercial circuitry operating at a minimum speed of 9.6 KBPS, which allocates channels to various foreign affairs users for data transmission.
- The Security Enhancement Program, created in 1980, now operates on a limited basis subject to budgetary constraints. Its purpose is to reduce or eliminate vulnerability at high risk posts by tightening physical security, specifically by replacing paper records holdings with electronic storage.

o Negotiations with a number of foreign ministries in Europe provide the framework for Embassy/PTT discussions aimed at improving the security posture of leased telecommunications facilities.

Today the DTS is a viable, sophisticated, and modern entity that continues to implement state-of-the-art technologies. It is a global system that provides high speed and data facilities to the foreign affairs community. Much remains to be done to ensure its survivability under conditions of stress and emergency.

4. HOT LINE HISTORY

The Cuban Missile crisis demonstrated the critical need for a direct line of communications between the White House and the Kremlin. A Memorandum of Understanding between the U.S. and the Soviet Union, signed at Geneva on June 20, 1963, established this link. The Hot Line consisted of two low-speed teletype circuits. One circuit ran via cable from Washington to London, Copenhagen, Stockholm, Helsinki, and Moscow. The other, a high-frequency radio circuit, connected Moscow and Washington via Tangier. Both circuits became operational on August 30, 1963.

In September 1971, as part of the initial Strategic Arms Limitations Talks (SALT), the United States and the Soviet Union agreed to upgrade the Hot Line configuration linking Washington and Moscow by using modern satellite communications techniques. The new Hot Line, officially named the Direct Communications Link (DCL), became operational in January 1978. It operates through the Soviet MOLNIYA satellite system and also through the INTELSAT system. The MOLNIYA and INTELSAT DCL systems operate simultaneouslly so that if one system fails, the other continues to provide communications. The DCL is less vulnerable than the older system as it does not depend on extensive terrestial microwave and cable relays subject to natural disaster or sabotage.

The most recent initiative for improving the capability of the present Washington-Moscow DCL (Hot Line) introduced by Senators Jackson, Nunn, and Warner. Their efforts resulted in the U.S. Department of Defense Authorization Act 1983, which directed the Secretary of Defense to study possible initiatives for "improving the containment and control of the use of nuclear weapons, particularly during crisis."[6] The

Department of Defense responded by proposing the following enhancements of the Hot Line:

- Addition of high-speed facsimile transmission capability.
- Addition of high-speed data links between the Department of State and U.S. Embassy in Moscow, and between the Soviet Foreign Ministry and the Soviet Embassy in Washington.
- Creation of a Joint Military Communications Link between the Pentagon and the Soviet Defense Ministry. This link would facilitate the exchange of urgent technical military information.
- Negotiate a multilateral agreement to consult with other nations in the event of a nuclear incident involving a terrorist group.[7]

These proposals were endorsed by President Reagan in May 1983, and are currently the subject of U.S.-Soviet discussions.

The New York Times on July 18, 1984 reported the following:

> ... Soviet and American officials initialed a diplomatic note today upgrading the 21-year-old hot-line link between Moscow and Washington for crisis communications.
>
> The new version to be installed within two years, will speed up word transmissions threefold from the present 64 words a minute. It could also transmit graphics, such as maps showing the disposition of forces, according to a senior Administration official who briefed reporters at the White House today.
>
> President Reagan issued a statement describing the agreement as a "modest but positive step" toward reducing the risks of nuclear war by "accident, miscalculation or misinterpretation."[8]

5. EXECUTIVE BRANCH POLICY RE NATIONAL SECURITY AND EMERGENCY PREPAREDNESS OF TELECOMMUNICATIONS

NATIONAL SECURITY DECISION DIRECTIVE NUMBER 97

National Security Decision Directive 97 (NSDD-97) mandated telecommunications policy to support the government's national security and emergency preparedness objectives. The agenda included the maintenance of communications with all governments, especially in crisis situations. In support of this and other objectives, NSDD-97 established as a policy principle the requirement of a survivable and enduring national telecommunications capability composed of government, commercial, and private facilities, systems and networks.

To oversee NSDD-97 and ensure its implementation, the directive created a Steering Group comprised of the Director of the Office of Science and Technology Policy (OSTP), the Executive Agent of the National Communications System (NCS), and the Associate Director of the Office of Management and Budget (OMB) for National Security and International Affairs, chaired by the Assistant to the President for National Security Affairs or his representative.

NSDD-97 directed the NCS to:

- consult with and take direction from the Steering Group regarding the implementation of this directive;
- ensure the development, in conjunction with NCS operating agencies, of plans to fulfill the principles and objectives stated in this directive, including an overall telecommunications architecture and timetable;
- function as the overall coordinator, in consultation with the designated implementing agency, for each initiative approved by the Steering Group pursuant to this directive;

- o ensure that all relevant activities in support of this policy directive are fully coordinated with the Executive Agent and all NCS principals;

- o develop, for review by the Steering Group, overall budget profiles regarding approved initiatives and related activities;

- o develop plans, in consultation with the National Security Telecommunications Advisory Committee (NSTAC), for an effective mechanism to manage and control the initiation, coordination, restoration, and reconstitution of existing commercial telecommunications services and facilities to support national security telecommunications leadership requirements;

- o consult with the Federal Communications Commission (FCC), as appropriate, concerning this directive; and

- o prepare annually, or as otherwise directed, a written report to the Steering Group on the progress of approved initiatives, including an assessment of the resources that will be required to attain the objectives of this directive.

NSTAC was given the following responsibilities under NSDD-97:

- o provide to the President and the Executive Agent of NCS information and advice from the perspective of the telecommunications industry with respect to the implementation of this policy directive, and periodically report to the President, through the Assistant to the President for National Security Affairs, and to the Secretary of Defense in his capacity as Executive Agent of the NCS, and;

- o serve as a forum, when appropriate, for joint industry and government planning to support this directive.

Finally, NSDD-97 mandates that all departments and agencies incorporate the provisions of this policy directive when modifying their current telecommunications facilities, systems, or networks or when planning new ones; and as deemed necessary or as required, provide information and assistance to, and consult with, the Steering Group in support of this directive which supersedes PD-53.

The Department of State (DOS) is aware of the vulnerability of its communications systems. In accordance with the policy of NSDD-97, it is improving the reliability and survivability of its worldwide telecommunications networks. In 1983, DOS asked NCS to employ the assistance of NSTAC. The NSTAC Industry Executive Subcommittee subsequently established an International Diplomatic Telecommunications (IDT) Task Force and directed the Task Force to address the issues of U.S. leased telecommunications service overseas and diplomatic telecommunications service in the United States.

EXECUTIVE ORDER No. 12472, April 3, 1984

E.O. 12472 consolidates several previously issued Presidential Directives and National Security Decision Directives. It authorizes certain federal departments and agencies to establish collectively a survivable domestic and international telecommunications infrastructure that will have the capability to support the national security needs of the U.S. government.

U.S. domestic and international telecommunications resources, including commercial, government, and privately owned services and facilities, are essential elements in support of national security policy and are vital to emergency preparedness. A survivable domestic and international telecommunications infrastructure with the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security is essential to national security and emergency preparedness requirements in all circumstances, including those of crisis or emergency.

The Executive Order establishes a framework for (1) the planning, development, and exercise of the capability to satisfy the national security and emergency preparedness telecommunications needs of the federal government; and (2) providing advice and assistance to state and local governments, private industry, and volunteer organizations, upon request, regarding their national security and emergency preparedness telecommunications requirements. The order establishes a planning and management framework for all conditions of crisis or emergency, including international crises, attack, recovery, and reconstitution, and the entire range of civil preparedness emergencies such as earthquakes and hurricanes. It also specifies the national security and emergency preparedness telecommunications roles to be played by the Executive Office and various federal departments and agencies.

E.O. 12472 consolidates the missions of the NCS, the National Security Council (NSC), the Director of the OSTP, and the Director of the OMB in the discharge of their national security and emergency preparedness telecommunications functions. The NCS consists of both the telecommunications assets of the entities represented on the NCS Committee of Principals, and of an administrative structure comprised of the Executive Agent, the NCS Committee of Principals, and the Manager. The NCS Committee of Principals includes representatives from those federal departments, agencies, and entities with significant national security or emergency preparedness telecommunications responsibilities. A primary function of the NCS is to help coordinate planning for and provision of national security and emergency preparedness communications to the federal government under all circumstances.

The Executive Order assigns specific planning, management, and oversight responsibilities to the NSC, the Director of the OSTP, and certain key federal agencies, including the Departments of State, Defense, and Commerce, and the Federal Emergency Management Agency.

E.O. 12472 defines and clarifies the mission and responsibilities of DOS regarding the telecommunications needs of the U.S. diplomatic corps and foreign affairs community, under all emergency conditions. Section 3(C) of the Order states that the Secretary of State, in accordance with assigned reponsibilities within the Diplomatic Telecommunications system, shall plan for and provide, operate and maintain, rapid, reliable, and secure telecommunications services to those federal entities represented at U.S. diplomatic missions and consular offices overseas. This responsibility shall include the provision and operation of domestic telecommunications in support of assigned national security or emergency preparedness responsibilities.

The magnitude of the Command, Control, Communications, and Intelligence (C^3I) programs indicates the significance the Executive Branch places upon the reliability and survivability of the Department of Defense's (DOD's) communication systems. For example, the estimated expenditures for C^3I from FY-85 through FY-89 total $220 billion.

The Report of Secretary of Defense Caspar W. Weinberger to the Congress on the FY-85 Budget, FY-86 Authorization Request, and FY-85 through FY-89 Programs includes $36 billion for C^3I in FY-85. The scope of the DTS does not compare with that of DOD, but it plays a key role within the C^3I context. A small fraction of DOD's C^3I budget would provide sufficient funding to enhance it. Hopefully, the Executive and Legislative Branches will give equal consideration and recognition to the needs of the DTS.

6. OUTLINE OF PROBLEMS AND FACTORS

This chapter addresses the vulnerability of the Diplomatic Telecommunications System (DTS) and outlines its problems.

To expect the establishment of a totally fail-safe mechanism for a global network is unrealistic. Nevertheless there are several initiatives which, if implemented, would enhance and guarantee to a reasonable and acceptable degree the system's survivability.

How do we protect and ensure the survivability of a global telecommunications system whose main assets are commercial circuits leased and controlled by U.S. carriers and foreign Post Telephone and Telegraph (PTT) Administrations at all times, but especially during stress situations such as earthquakes, fires, civil disorders, industrial strikes, terrorism actions, and, to contemplate the worst possible situation, nuclear attacks? The principal factors are: speed, survivability, endurance, security, and terminal equipment.

Speed is relative but now that many foreign affairs agencies use data service and computer-to-computer interoperability technologies, there is need for high-speed wideband circuitry such as 9.6 KBPS or higher. In other words, real time speed is demanded.

Survivability is absolutely essential but how do we guarantee it?

- By redundancy of circuits?
- By leasing circuits via several means, e.g., cables and satellites and different gateways?
- By installing leased satellite terminals in Embassy buildings thereby eliminating several potential vulnerable points?

- o By installing and operating U.S. government owned and controlled satellite terminals?
- o By obtaining from PTTs high restoration priorities?
- o How do we cope with electromagnetic pulse (EMP) generated by a nuclear explosion? Should EMP influence the use of satellite systems?
- o Do we install limited back up communications equipment (HF or satellite) at alternate sites?
- o How do we deal with foreign PTTs' legal, regulatory restrictions?

Endurance includes all of the survivability factors but also requires a sustained source of reliable power.

- o What are some of the alternatives if the commercial power grid fails because of terrorist acts, EMP, or other reasons?
- o Will emergency back-up portable or fixed-station generators be available?
- o How long can such generators function without outside assistance?
- o What about the stamina of personnel?

Security, that is communications security (COMSEC), is inherent in cryptographic systems. In addition we must consider the physical security of the Post's Communication Center and of vulnerable points along the route of a leased circuit such as cable head or satellite earth station, trunks, PTT central offices, local loops, and micro-wave terminals.

- o How do we convince U.S. and foreign carriers and PTTs to enhance their physical security posture?

o And who pays for such improvements?

Terminal Equipment. Do Foreign Service Posts have sufficient spare equipment to remain operational for a reasonable duration without outside technical assistance? Are their personnel trained in first echelon maintenance?

Secondary factors in the protection and survivability of the DTS include redundancy, U.S. controlled facilities, negotiations with foreign PTTs, and negotiations with U.S. International Record Carriers (IRCs).

Redundancy. The redundancy needed to ensure the system's survivability may in fact serve a dual purpose. A growing number of foreign affairs agencies are demanding additional telecommunications services that could provide higher speed and wider bandwidth which allow computer-to-computer data transmissions, video, etc.

U.S. Controlled Facilities. It may be attractive to suggest that the installation and operation of a completely U.S.-owned, operated, and controlled telecommunications global system would resolve a number of security and reliability problems. However, as one considers costs, (e.g., DOD's MILSTAR Program), and possible difficulties regarding compliance with laws and regulatory policies governing telecommunications operations in foreign countries as well as in the United States, the attraction fades. Many countries would not sanction installation and operation of U.S. government owned and controlled telecommunications systems because of possible technical interference with their own communications networks, loss of revenue, or prohibitive national laws and regulations. Similar objections arise to proposals for installations in the United States itself. In the middle and late '70s, several U.S. IRCs questioned the legality of the State Department's plan to

replace leased circuit cancellations with U.S. government owned facilities. The matter was resolved amicably, but the IRCs had made their point. Legal and ethical questions concerning the use of U.S. government owned, controlled and operated telecommunications facilities will continue to arise. In cases where it is clear that IRCs and local PTTs cannot provide appropriate facilities, provisions should be made for the installation of U.S. government owned facilities.

Negotiations with Foreign PTTs. A key issue in hardening the diplomatic telecommunications overseas will be the amount of cooperation foreign PTTs will give regarding security improvements at terminals and interconnecting points along the circuitry route which are under their operational control. Traditionally the PTTs in major industrial countries have been powerful, proud entities well aware of their importance and of their national sovereignty. To obtain their agreement and convince them to take steps to improve the security posture will demand skillful, tactful negotiation. Our approaches will have to be varied and should be respectful of the host country. An offer of technical assistance and/or equipment to certain countries would be considered offensive and disparaging. Or it might be seen as a means of introducing American technology into their country for future marketing. A genuine need for security enhancements may be best demonstrated by establishing common interests such as protecting vital telecommunications centers and links from terrorist actions, setting restoration priorities with reciprocity in the United States, and reaffirming diplomatic benefits of maintaining secure communication channels between the two countries. U.S. carriers may be instrumental in securing PTTs'

approval as they usually have excellent professional relationships with their counterparts.

Negotiations with U.S. IRCs. The deregulation of the telecommunications industry, particularly in the United States, has affected/influenced the services it provides. Now customers deal with several entities rather than just one and they must closely examine the various options available. They also must realize that reporting and correcting technical problems may take longer than heretofore. Overseas the PTTs still enjoy an actual monopoly, but the deregulation trend is spreading, particularly in the United Kingdom and Japan.

Prior to deregulation in the United States, the telecommunications industry could and did perform certain security enhancements for the benefit of the U.S. government. Costs of these enhancements were not paid by the U.S. government but were passed on to users in the form of increased rates. But in the competitive arena of today's deregulated world it is unlikely that such free services will be extended to the U.S. government.

7. WEAKNESSES AND FAILURES

All systems have their shortcomings and occasionally they fail. The Diplomatic Telecommunications System (DTS) is not an exception. There have been a number of communications failures, some caused by malfunctions or human errors, others due to fundamental weaknesses in the system. A most distressing example of the latter occurred during the critical cease-fire negotiations conducted by former Secretary of State Henry Kissinger in Moscow during the 1973 Middle East Yom Kippur War. Although there was no breakdown in the Embassy's communications facilities, their inability to transmit large volumes of sensitive traffic in real time caused considerable anguish and could have had disastrous affects on the cease-fire negotiations. In his book Years of Upheaval, Kissinger describes some of the issues at stake:

> ...The letter [from President Nixon to Golda Meir] pointed out the vast difference between the cease-fire resolution now being proposed and Sadat's program publicly put forward five days earlier. A prompt reply was requested.
>
> Messages were also drafted for Hafiz Ismail, the Shah, King Hussein, and our UN Ambassador John Scali. This process was completed by about 5:30 p.m. Moscow, or 10:30 a.m. Washington, time.
>
> At 6:30 p.m., I met with the British, French, and Australian ambassadors to Moscow, the first two in their capacity as permanent members of the Security Council, the Australian because his country's representative in New York was president of the Security Council for October as the consequence of rotation. Diplomats are congenitally careful in expressing their opinions on issues with respect to which their governments have not yet taken a stand. In this case they were sufficiently confident of their governments' views to offer warm congratulations before rushing off to inform their capitals. Because of a horrendous communication mix-up, it is likely that their reports arrived before ours.
>
> I then lay down to rest for an hour. When I awoke around 8:00 p.m. (1:00 p.m. Washington time) I found out to my horror that none of my messages had been received in

Washington. My staff had first sought to send the messages through our Embassy in downtown Moscow, forty-five minutes away. The Embassy had great difficulty, however, because its procedures for sensitive messages were cumbersome and time-consuming. We then resorted to transmitting via our Presidential aircraft, parked at Moscow's Vnukovo II Airport, for a satellite hookup to the White House Situation Room. But the messages sent from the plane were arriving in practically unreadable form in Washington. My associate Larry Eagleburger was in touch with our Embassy and then with Brent Scowcroft in Washington on an open phone line. Scowcroft could make out that we had agreed to a cease-fire, but the letter to Golda Meir had come in too garbled to pass to Dinitz. We thereupon had no choice but to switch back to sending the messages through the Embassy.

My reaction to this was later described by Larry Eagleburger in a reminiscence he sent to me:

> As if it were yesterday, I recall sitting at a desk in a fairly large room in the villa, yelling over the phone at the communications people in the Embassy. (I was yelling because of the bad telephone connection, not because I thought it would help move the cables faster. Unlike certain Secretaries of State, I never believed that a loud voice had much impact on inanimate objects, no matter how badly they functioned.) There were some twenty to thirty people in the room, all talking, with Joe Sisco (never a quiet fellow) taking the lead. In short, the room was crowded and noisy, but I was more-or-less hidden from view (and hearing) by the crowd.
>
> ...Unbeknownst to me, you walked in at that moment and obviously heard what I was saying (I still haven't figured out how). There was a bellow along the lines of: "What, the cables aren't out yet!?!" I looked up, to find you standing in the middle of the room with smoke issuing from nose, eyes, and ears, and no one else (with an exception I'll mention in a minute) in sight. All twenty or thirty people--no doubt led by Sisco--had exited with a speed and facility that would have put Houdini to shame. The single exception was Winston Lord, who was sort of huddled in a corner, but--God bless him--prepared to hang around for the pyrotechnics and to clean up the blood (mine) when it was all over. Winston, ever since, has had a special place in my heart, as well as my great respect for his outstanding courage.

The situation was far from funny. Altogether, at least four hours were lost and much Israeli confidence in us. At first I thought it was an inexplicable technical malfunction; I was told that electrical storms in the atmosphere were

> disrupting all radio communications. The next day it struck me as weird that all transmission channels should break down simultaneously on a Presidential plane that was outfitted for instant communications and that over five years of diplomatic missions had never failed. Then I recalled the delays and garbling I had experienced when cabling Nixon from the parked aircraft during my secret visit in April before the 1972 Moscow summit. If the interference was indeed deliberate (which I cannot prove),[9] it served Soviet purposes only marginally; but this of itself does not exclude the possibility. What is so maddening about much of Soviet maneuvering is the loss of confidence that Soviet bureaucrats seem willing to accept for relatively slight benefits."[10]

In an interview with the author, Ambassador Hermann Frederick Eilts reported on some problems he experienced with diplomatic communications systems while serving as American Ambassador to Egypt:

> For an American ambassador to function effectively abroad, a reliable and fast communications system is essential. Without such a system there are delays in receiving instructions from Washington, he is not able to make maximum input into the formulation of his instructions, interested Washington agencies are only inadequately informed of political and economical developments in a foreign country and, in general, the pace of an American Embassy in a foreign capital is decelerated.
>
> In my 35 years of foreign service work I have seen an enormous improvement in the speed and reliability of our diplomatic communications system. When I first entered the foreign service in 1947, most of our posts abroad still used the One Time Pad (OTP) system. Only the larger embassies had received encryption machines. I recall spending laborious hours encrypting and decrypting outgoing and incoming messages on OTPs. As far as transmission was concerned, we were dependent upon indigenous telegraphic systems. These varied widely in quality. Thus, for example, in the early fifties the Aden Post Telephone and Telegraph system (PTT), operated by the British, was reasonably efficient; next door in the Imamate of Yemen, to which I was also accredited, the government operated PTT was a virtual disaster. It took days for incoming telegrams to be delivered and, equally so, days for outgoing telegrams to be sent.
>
> In the ensuing years, increasing efforts were made to obtain leased telegraph lines as a means of giving greater reliability to American diplomatic communications. Our encrypting and decrypting procedures and equipment improved markedly in terms of greater speed and dependability. Great emphasis was placed by successive American administrations on

improving communications between Washington and foreign posts, and much progress was made. In the early sixties, however, with the advent of the Kennedy Administration, we suffered a slight communications setback. It had little to do with the nature of the available communications equipment at the time; rather it was a function of increasing verbosity on the part of Washington and foreign post message drafters.

I recall having my knuckles rapped in the mid-fifties for sending a two-page telegram; six or seven years later, outgoing telegrams from Washington and incoming telegraphs from foreign posts were often eight to ten pages or more. Whereas previously, drafting officers had been enjoined to send telegraphically only the essential elements of a diplomatic conversation, the Kennedy functionaries detailed in their messages every bit of what had been said, not only by the foreign official, but even more so, what they had said! It was a new style in diplomatic reporting. For a period, it seemed that the increasing length of diplomatic messages outpaced even the higher speed ratios that had developed in communications equipment. It was not long, however, before American diplomatic communications equipment had improved still more and could handle greater verbosity.

And yet, constant problems developed, sometimes because of equipment and sometimes because of continued need at certain places to rely upon indigenous telephone or telegraph lines. While Ambassador to Egypt, for example, I brought in a United States Navy component, whose mission it was to clear the still blocked Suez Canal of mines and unexploded ordinance. Its headquarters were set up in what had by then again become the American Embassy in Cairo, utilizing embassy communications. To my annoyance I quickly found that naval messages for the Suez Canal clearance operation were "flooding" my own diplomatic communications. Because the military placed a high precedence indicator on almost every message, no matter how routine its substance might be, such naval messages regularly preempted my diplomatic telegraphic traffic from Washington. Persuading the Navy to lower its precedence indicators to something commensurate with the importance or otherwise of the subject of the messages proved to be almost impossible. The Navy, along with the other military services, I was told, always used such high precedence indicators. They simply did not know how to operate in any other way.

I finally had to ask the Department of State to raise the precedence indicators on diplomatic messages being sent to me in Cairo as the only way to ensure that I would receive such messages on a timely basis. The Department of State communications people growled at this abuse of precedence indicators, but had no better luck than I did in trying to persuade the United States Navy to show better judgment in designating precedence indicators for routine military messages.

My most difficult communications experience took place at Aswan, Egypt, in January 1974. We had no communications of our own in Aswan, but I had had to deploy a number of officers to that locale in connection with Secretary of State Henry Kissinger's shuttle effort. All outgoing telegraphic communications from Aswan had to go through the as yet small United States Interests Section of the Spanish Embassy in Cairo, which also had to relay to me in Aswan any incoming messages. We were in the final stages of concluding the Sinai I disengagement accord between Egypt and Israel. Kissinger had just been in Aswan and had worked out with President Anwar al-Sadat an agreed text for that accord. He had then flown to Jerusalem to obtain Israeli agreement. He anticipated the possibility of a few minor textual changes, which would have to be sent by "Flash" message to me in order to obtain Egyptian agreement. All pertinent messages from Kissinger had to be sent to the United States Interests Section of the Spanish Embassy in Cairo, which would then try to forward them to me in Aswan.

With much difficulty my small staff and I had managed to lease an Egyptian telephone line between Cairo and Aswan, but this went through an Egyptian telephone operator in Luxor. Nominally, that line was supposed to be open all the time, but we quickly found that the Egyptian operator in Luxor would for one reason or another leave for long periods of time. Without him to plug us into a Cairo connection, we had no communications. The only way to keep him at his post in Luxor was to make continual use of our leased telephone line. We soon learned that even a few minutes of pause in on-line conversation would cause the unseen Egyptian operator at Luxor to bolt. Hence, as we awaited the critical message from Kissinger in Jerusalem on whether Sinai I could be signed or had to be amended, we had somehow to keep the Cairo to Luxor to Aswan telephone line constantly open.

For several hours the three members of my staff in Aswan and I simply talked on the phone, reading the Bible, reciting any and every poem that we could remember, and talking banalities until each of us was hoarse. We would spell each other in conducting this discursive function without interruption. Happily, Kissinger's message from Jerusalem arrived while we still had the line open. Had the Egyptian operator at Luxor been able to get away from his post, neither we nor Sadat would have known for hours whether Sinai I could be signed. Today in that kind of situation, mobile telegraphic equipment tied into a satellite system could be arranged. Only a few years ago one made do with whatever was available.

One of my most embarrassing communications problems also arose in Cairo in early 1974. Kissinger had just passed through on his way to Riyadh in Saudi Arabia. He told me to await a Flash message from Riyadh, which I was to convey not only to

President Sadat but also to Soviet Ambassador Vladimir Vinogradov. I alerted each of the two men to the likelihood that I would be coming by with such a message sometime in the evening.

Instead of receiving it in the time frame that had been indicated to me, hours went by and there was still no Flash message. Vinogradov kept telephoning me to ask where the promised message was, and I kept telling him that it should be coming at any time. (Sadat showed much more patience.) Finally, at about midnight, several hours after the message should have arrived, I went to see Vinogradov to explain the state of play. He and his embassy counselor were playing chess, but were not at all pleased about the delay. They were convinced that Kissinger had done this deliberately. I assured them that, as soon as I received the message, I would again come by.

Back at what was then the American Embassy I managed with great difficulty to get a telephone call through to Kissinger's aide, Larry Eagleberger, who was with him Riyadh. After asking him about the promised message, Eagleberger said it had been sent five hours before that time with Flash precedence. He could not understand why it had not yet been received but, in guarded fashion, gave me the gist of the message over the phone so that I could inform Vinogradov and Sadat. I did so at 3:00 in the morning. A sleepy Vinogradov and his counselor were still playing chess. They had been doing so for six and a half hours. Vinogradov's chess must have improved greatly from the experience; his temper had not!

It subsequently developed that human error had caused the delay in transmitting the Flash mesage. In Washington, where the message had to be transferred from the Riyadh communications system to that being utilized by Cairo, a communications clerk had inadvertently failed to notice the Flash precedence on the incoming message and had simply allowed it to lie around for several hours. Not until Eagleberger, from Riyadh, had sent a followup query was the commmunicator's error discovered. The incident was another reminder that, even with the best communications systems, the human error factor can never entirely be removed.

As already indicated, diplomatic communications have improved enormously. But for users, both in Washington and in posts abroad, communications can seldom be instantaneous enough. More and more redundancy is needed in communications systems in order to manage breakdowns in individual systems. The cost of modern diplomatic communications systems is directly related to their increasing sophistication. An ever growing demand for services is being placed upon diplomatic communications, but Congressionally-approved financial resources for this purpose always seem to lag behind. Hopefully, executive and legislative understanding of the need for the most effective and foolproof communications will continue to grow.[11]

Other failures have occasionally denied Foreign Services adequate communications facilities with Washington for undue periods of time. Fortunately, they did not affect national security or attract national attention. But the situation could have been altogether different. For instance, a fire in the American Embassy in Moscow in 1977 disabled the Embassy's communications capabilities for over 24 hours. Had this happened during a period of intensive negotiations with the Soviets, the communications cut-off could have been disastrous. There have been other breakdowns, particularly in Africa, when the only remaining means of communications was plain language HF voice radio, which seriously compromised security. Strikes by PTT personnel have resulted in total loss of leased circuitry. In most cases, the loss of communications facilities (and with them the ability to command and control), could have been avoided had a redundancy of circuitry been available. This is one of the most vulnerable points of the system, and it exists not only internationally but domestically as well.

The necessity for a secure DTS is reinforced by instances of Command, Control, Communications, and Intelligence (C^3I) failures in times of crisis which have resulted in loss of life, loss of ships and aircraft, compromise of sensitive information, and embarrassment to the U.S. government.

Because published material concerning the DTS is scarce, we have had to look at the history of defense communications. Our intent is not to criticize or compare, but simply to demonstrate that without proper communications, Command and Control cannot perform their functions effectively.

Oswald and Gladys Ganley report in To Inform or To Control?:

... While C^3I is an integral part of nuclear crisis management it is, fortunately, used more frequently for various less dramatic present-day international crises. Such crises have historically had a way of getting out of hand, which can no longer be tolerated in a nuclear age. So, now that we have such sophisticated communications means in place, decisions are rarely left to the discretion of the regional or local commander. Shortly after an alert, the president or the Secretary of Defense, personally takes control of the situation. Whether this is either necessary or desirable can be debated, but it is a fact created by the nuclear and the information age.

... The necessity for a secure C^3I system that works under diverse conditions worldwide is illustrated by the following cases.

... The case of the USS Liberty, had it not been so serious, could be racked up as a comedy of communications errors. On June 8, 1967, during the Arab-Israeli war, that ship was cruising 12 miles off the Sinai peninsula. It was there for the specific purpose of eavesdropping on battlefield communications. During a period of thirteen hours, six urgent messages for the Liberty were sent out by the Pentagon, ordering that ship out of the area and to a point 100 miles offshore.

... None of the messages reached the ship in time. Two were misrouted to a U.S. communications station in the Philippines. One went to Greece. One message was never directed to the Liberty. One was lost in the electronic labyrinth at the Army Communications Station at Pirmasens, Germany. A final message marked URGENT and TOP SECRET by the Joint Chiefs of Staff, sent the morning of June 8th: "... being passed from ship to ship and from communication station to communication station in search of a circuit to Liberty that was cleared for TOP SECRET traffic. Finding no such circuit, the message was undelivered."

... The message contained was of a "run for your life" variety. The result of this series of human and computer errors was tragic. At two in the afternoon, Israeli planes and boats began a coordinated attack on the Liberty with gunfire, torpedoes, rockets and napalm which lasted for an hour and twenty minutes. At the end of the Attack, 34 U.S. sailors were dead and 171 wounded.

... The incident of the U.S. intelligence ship Pueblo, which was attacked by the North Koreans in 1967, is another instance of failed communications. The National Security Agency had notified the Pentagon more than two days beforehand that an attack on the Pueblo was likely. But

> again, due to a variety of command and administration snafus, the ship was not notified. The ship, its men, and highly classified information and information equipment were, as a result, captured by the North Koreans.
>
> ... Here, not only was a physical disaster and a tragedy for the ship's men witnessed, but this was also the first instance ever in the history of the United States, of a Navy ship being hijacked on the high seas.
>
> ... Sometimes the problem is too much information. During the evacuation of the American Embassy in Saigon in 1975, very good communications were maintained throughout. That is, the United States had very good unsecured voice communications with the Embassy and were apprised of every detail. And so were the North Vietnamese.
>
> ... Another instance of this sort was the Mayaguez incident of 1976. In this case, the ship had been hijacked by the Cambodians, and President Ford had decided to retake it by force. Communications worked perfectly, and the President himself had direct control. However, everything that was discussed was discussed in the open. There is good reason to believe that the Cambodians were listening and knew every detail of exactly what was going to occur. For example, when helicopters were sent in to take the island where the ship was anchored, the direct orders for doing so were passed from the U.S. Air force to the U.S. Navy -- over open circuits. Thus, how many helicopters and how many men would participate, where they were going, at what time, and the replenishment rate were all open secrets, and the United States did all the work for the Cambodian military intelligence.[12] Twenty U.S. marines were killed during this operation.
>
> ... In 1969, the North Koreans shot down an EC-121 aircraft, a converted propeller driven Constellation on an intelligence mission in South Korea. It is almost a carbon copy of the other incidents cited above. The North Koreans' intentions were known to the military system; yet the EC-121 was not notified, and was shot down with total loss of life.[13]

The advent of information age has seen a dramatic increase in the speed with which the media report and interpret news. Unfortunately, this is not always advantageous. In 1979 a quickly spread rumor that the U.S. government was responsible for the seizure of the Great Mosque in Mecca by Moslem extremists inflamed public opinion in the Moslem

world, and sparked an attack on the U.S. Embassy in Islamabad, during which two Americans died and the Embassy burned down.[14] Other U.S. offices in the region were also attacked but with less severity and without loss of life.

The speed with which the U.S. government can debunk such rumors by informing the foreign governments involved of the facts is dependent upon the effectiveness of its DTS. Timely requests for protection of U.S. citizens and interests as well as the use of the local media to defuse volatile situations are important factors in preventing or at least containing mob actions which all too often have had tragic consequences.

8. POSITIVE ASPECTS

The positive effects of communications were particularly apparent during Henry Kissinger's tenure as Secretary of State. Secretary Kissinger was an exacting taskmaster who recognized the vital importance of communications. To meet his objectives, he rightfully demanded rapid and secure communications facilities between Washington and other nations' capitals. With the advent of "shuttle diplomacy" in January 1974, tremendous demands were placed on the Diplomatic Telecommunications System (DTS). Temporary communications centers had to be established on very short notice at locations such as Aswan, Aqaba, Riyadh, and Taiz where no U.S. Missions existed, and additional facilities dedicated to the new diplomacy had to be provided at existing Embassies on the itinerary. Thus, the era of the "CAN-DO" packages began. "CAN-DO" packages consisted of all equipment necessary to operate a field communications center, including HF radio or satellite hook-up if commercial circuits were unavailable. These packages are still used, although the facilities they provide are much improved.

The 1975 Sinai II Agreement between Egypt and Israel, which led to the establishment of the Sinai Field Mission, contains provisions for using communications and information for peacekeeping purposes. (Incidentally, the DTS succeeded in installing communications facilities for the Sinai field mission in a very short time.) Oswald and Gladys Ganley's discussion of the Sinai II Agreement summarizes the role of communications:

> ... A further step in the uses of communications and information resources for monitoring arms buildups was taken when Secretary of State Kissinger, during his shuttle diplomacy worked out an arrangement for technical assistance

by the United States for peacekeeping in the Sinai. The U.S. proposal, attached to the agreement between Egypt and Israel, initialed on September 1, 1975, in Jerusalem and Alexandria and signed in Geneva on September 4, read partially as follows:

> The Early Warning system ... shall have the following elements:
>
> a. There shall be two surveillance stations to provide early warning, one operated by Egyptians and one operated by Israeli personnel. Their locations are shown on the map attached to the Basic Agreement. Each station shall be manned by not more than 250 technical and administrative personnel. They shall perform the functions of visual and electronic surveillance only within their stations.
>
> b. In support of these stations, to provide tactical early warning and to verify access to them, three watch stations shall be established by the United States in the Mitla and Giddi Passes ... These stations shall be operated by United States civilian personnel. In support of these stations, there shall be established three unmanned electronic sensor fields at both ends of each Pass and in the general vicinity of each station and the roads leading to and from those stations.

The duties of the United States civilian personnel, who were not to total more than 200, were to:

> ...verify the nature of the operations of the stations and all movement into and out of each station and... immediately report any detected divergency from its authorized role of visual and electronic surveillance to the Parties to the Basic Agreement (Egypt and Israel) and to the United Nations Emergency Force.

This, together with U.S. aerial reconnaissance already in operation over the area, bolstered confidence against surprise attack sufficiently to permit disengagement in the Sinai. This plan, which was put into operation immediately, has been extremely successful and is still contributing to stability in that area. Speaking to the United Nations in 1978, Vice President Mondale dubbed this use of electronics devices "the eyes and ears of peace." He expressed U.S. willingness to consider similar requests from other countries with like peacekeeping needs.[15]

Both Egypt and Israel have praised the American performance in the Sinai. Defense Minister Peres is quoted as saying that, in his view, "... no other single element of the Sinai II Agreement had done as much as the Sinai Field Mission to reduce tensions in the Sinai."[16]

Egyptian Deputy Minister General El-Gamasy also praised the high degree of impartiality and credibility achieved by the Field Mission, as well as the professionalism with which the operation had been conducted.17

9. SUPPORTING OPINIONS

The government, academia, and industry all recognize the importance of the use of communications and information systems, including the State Department global Telecommunications System, in both peacekeeping and war-terminating roles.

> ... Since so much depends on the acceptance by other countries of communications innovations with respect to restoration priorities, security, etc., that cannot be obtained without the cooperation of the host countries, it is important to make it clear to them that the proposed enhancements are in their own interest too.
>
> ... Telecommunications, in contrast to mass communications is a two-way point to point interaction. It can become a bridge between nations; it demeans no one; it helps achieve mutual effort where common interest exists. Insofar as that kind of tightened mutual bond between nations is in the interest of the United States, the U.S. government would be well advised to move forward swiftly in promoting global Telecommunications. [Emphasis added.][18]

And on C^3I within the Department of State:

> ... The United States government, to conduct its foreign affairs and provide for its national security maintains many of the most extensive and complex telecommunications and information systems in existence today. These global systems range from the more basic, e.g. stand-alone word processing equipment, to the most advanced, e.g. high-speed enhanced telecommunications networks forming part of our national security C^3I matrix.
>
> The Department of State utilization of such systems derives from its primary mission, i.e. advising the President in the formulation and execution of foreign policy. In this regard, the primary business of the Department of State is the exchange of information. Such exchange is the keystone of diplomacy. It is essential in peacetime, times of escalating crisis and during and after conflict. C^3I systems provide the mechanisms for this exchange. They are the means, according to one authority, which allow an organization to probe its environment, plan, act and react, in order to avoid threats and to exploit opportunities, as well as provide the means for it to mobilize, deploy and integrate its energies and resources. From this perspective, the Department of State sees the continued maintenance of its command, control and communications

systems as essential for achieving its global responsibility and as such constitutes the touchstone of the Office of Communications' primary mission, i.e. the provision of fast, secure and reliable telecommunications for the foreign affairs community.[19]

. . . .

... If there is anything that I have developed great sensitivity to in my years in the House, it's communications. Clearly it governs the way we think, act and deal with others. Any politician worth his salt maintains good communications with his district, lest he not be reelected every two years.[20]

. . . .

... While those within the Defense Department may seem to be most intimately concerned with C³I matters, it is well to recall that there are a number of others in the government with strong interest in this area as well. The State Department, for example, has a key role [emphasis added] in the business of diplomatic communications and intelligence matters which may affect foreign policy and international relations.[21]

. . . .

... Looking at information needs from yet another angle, to make information usable to support command and control, you have to go through a basic process: collection, processing, analysis and reporting. Currently the collection process is largely seen either from the human collection or technical collection standpoint. Human collection all too often is taken to mean simply spies. And I would stress for you again the impact of the draw-down all across the national security account for a decade, which has impacted very heavily on the Foreign Service [emphasis added], to the point where a great deal of information we normally should rely on from human reporting, from overt collection by Foreign Service personnel, simply is not forthcoming, because for much of that decade we have put a premium on reduction of American presence. And when you have gone through a long period when an Ambassador makes his points with the President by the number of people he has reduced from the American presence in a country, rather than on the depth of understanding of that country's internal currents, crosscurrents and events, it should not be a great surprise that you end up being caught unawares by new developments or new activities.[22]

. . . .

> A major trend characterizing U. S. discussions of strategic issues during the past decade was an increased willingness among strategic thinkers to consider "limited" nuclear war scenarios, doctrine and contingencies. The concept of "limited" nuclear war implies that it is possible to fight a war using nuclear weapons, limit destruction in some meaningful sense, and terminate the war without automatic escalation to "unlimited" nuclear exchange. How difficult it would be to terminate a "limited" nuclear war, and how termination might be accomplished, are questions which deserve more attention; attempts to provide answers must address command, control, communications and intelligence (C^3I) considerations.
>
> . . . .
>
> Control in a war-terminating scenario may involve more than the "means of destruction". To successfully terminate hostilities, the surviving national authority may want to use diplomatic personnel to communicate and negotiate [emphasis added] with the national authority in the Soviet Union. Depending on the level of destruction and the confusion surrounding events, national leaders may want to preempt diplomatic channels and communicate directly with their Soviet counterparts. Control of diplomatic assets and possible means of employing those assets are certainly considerations worth examining in pre-hostilities planning for war-termination.
>
> The national diplomatic apparatus may offer at least two advantages in war-terminating efforts. First, diplomatic channels permit negotiations to proceed on different levels with varying degrees of formality and secrecy. Second, diplomatic personnel located in Allied or Soviet territory, may provide useful background information in the period immediately prior to hostilities. [Emphasis added.] If these personnel survive the outbreak of hostilities and are still able to communicate with U.S. leaders [emphasis added], a distinct possibility in a limited nuclear war scenario, they may provide post-hostilities information essential for war-termination, including assessments of successor Soviet (or Allied) leaders.[23]

Secretary of State Shultz addressed the serious problem of crisis management at the Disarmament of Europe Conference on January 17, 1984 in Stockholm, Sweden. There, Shultz said: "We should look for ways to make surprise attack more difficult; to make miscalculation less likely; to inhibit the use of military might for intimidation or coercion ... and to enhance our ability to defuse incipient crises." One means

toward those objectives, he noted, was "to enhance the capacity for rapid communications among our governments in times of crisis."

> The Secretary's proposal to "enhance the capacity for rapid communications" highlights the need to get on with technical discussions for not only improving the direct communications link between the heads of state, but also between other important military and diplomatic activities [emphasis added]. In doing so, improvements to the one must be considered in light of improvements to the others. Study proposals included adding high speed facsimile to the Hotline; the creation of a bilateral US-USSR Joint Military Communications Link; the establishment of high rate data links between governments and their embassies in the other's capital; and an agreement to consult with other nations in the event of a nuclear incident involving a terrorist group. Endorsed by President Reagan in May 1983, these proposals, along with others, are now being discussed between the Soviets and the Americans.[24]
>
> . . . .
>
> ... The hotline is not a great idea, just a good one. In an engineering sense, starting a major war is about the most demanding enterprise that a planner can face. In broader strategic terms, terminating a major war could be incomparably more challenging... getting it stopped in a manner that is consistent with all that is at stake would be of an importance and a difficulty that eclipses any other problem that any modern country has ever faced... Some kind of communication would be at the center of the process. [Emphasis added.] Even deciding with whom one is willing to negotiate might be of critical importance. The hotline does not take care of this problem; it only dramatizes it.[25]

10. CONCLUSION

This paper has demonstrated the central role that the State Department's communication system plays in the conduct of foreign affairs and our national security activities. It has shown the essentiality of maintaining--at all times, and particularly during times of stress and escalating crisis--a global telecommunications network capable of supporting, on a real time basis, the U.S. government's diplomatic initiatives and negotiations. Its foremost important function as a war-preventing tool deserves national attention and suppport.

The concern of the current and previous Administrations for the survivability of U.S. telecommunications resources and continuity of government has resulted in the issuance of a number of presidential directives, the latest being Executive Order No. 12472 signed on April 3, 1984. The intent of this order is to consolidate the assignment of and responsibility for improved execution of telecommunications functions that support national security and emergency preparedness. But does the government have the wherewithal to implement it? Will the budget drive the policy or will the policy drive the budget?

The world of the 1980s and 1990s will continue to breed political, military, economic, and other crises, and the United States will be called upon to negotiate, arbitrate, prevent, or terminate them in order to protect its national interests. The issues at stake are of tremendous importance not only to the United States but to the entire world. We can no longer afford to rely on public broadcasts by the news services to conduct sensitive, vital negotiations during periods of

confrontation or international crises as Kennedy and Kruschev had to do during the 1962 Cuban Missile Crisis. Fundamental weaknesses such as the one Secretary Kissinger experienced in Moscow in 1973 (see Chapter 8), must not reoccur.

Today, the U.S. government must not allow a lack of communications capabilities to endanger effective command and control functions. We must ensure the responsiveness of the DTS system in real time during world crises. And to do this, we must not only harden the system but also keep up with the rapid technological developments in the communications and information field.

In one of the worst imaginable scenarios, a limited nuclear exchange, direct communications between the Soviet Union and the United States may be unavailable. However, communications through a third party such as Geneva, Peking, or Tokyo might be possible, which would allow the National Command Authorities of each country to negotiate a possible settlement and cessation of hostilities that would avoid an all-out nuclear war.

In a less dramatic, nonetheless dangerous, situation such as an imminent conflict between two countries, timely approaches, negotiations, consultations with the parties concerned, and coordination and establishment of common policy with other governments might pressure the conflicting parties sufficiently to avoid a conflagration.

Terrorism is a relatively new frightening element in today's world. It is conceivable that terrorists may someday gain access to nuclear weapons and detonate them at any given place. Amidst the confusion that would follow the destruction of any major city, it would be absolutely essential to be able to communicate in real time with a number of

foreign governments to inform and query them regarding circumstances under which the nuclear explosion occurred.

As a participant in the 1982 Harvard Seminar on Command, Control and Communications Intelligence (C^3I) said: "C^3I systems must be modernized because a weapon system without effective communications is impotent." Anthony G. Oettinger, Chairman of the Harvard Program on Information Resources Policy, expressed the same view in an address before the Business-Higher Education Forum in 1981: "... We have these mammoth nuclear arsenals, lots of muscle, but the nervous system is not fit for an amoeba. Ponder that!" Similarly, the State Department as a war-preventing entity cannot function without a real time and stress resistant telecommunications system.

Richard Martin writes in Stopping the Unthinkable: C^3I Dimensions of Terminating a Limited Nuclear War:

> In the 1980 world of relative nuclear parity and limited nuclear options, it seems prudent to devote more attention not only to where the war will start, and how it will be conducted, but also to how it can be terminated at the lowest possible level of damage. The obstacles to achieving a war-terminating C^3I capability are clearly formidable; they are not, however, necessarily insurmountable.[36]

Martin's point should be carried a step further: What is more important than the capability to prevent war? The State Department's mission is not one of war fighting, but it will have great responsibilities in war terminating. Foremost it has a crucial role in war-preventing functions; its worldwide telecommunications network allows rapid secure communications with allies, neutrals, and enemies through our ambassadors abroad. In times of stress, it allows the President of the United States and his senior advisors to inform, negotiate, influence, and resolve escalating crises.

The issuance of Executive Order No. 12472 on April 3, 1984, emphasizes the significance the Reagan Administration places on telecommunications functions that support national security and emergency preparedness. The order provides a new impetus for enhancing telecommunications capabilities and requires a renewed and vigorous effort to meet the objectives of hardness and redundancy. The Diplomatic Telecommunications System (DTS) has the necessary infrastructure in place, and the State Department is selectively focusing its efforts on reducing vulnerabilities. However, accomplishing these goals on a timely basis will be largely dependent on the availability of resources. All too often, orders have not been implemented for lack of adequate resources. This must not be allowed to happen to the DTS. We must continue to improve our most effective means of conveying U.S. initiatives so that we might prevent or terminate war.

NOTES:

1. Joan Dain Sulek, Evolution of Emergency Communications Roles and Responsibilities (McLean, Va.: MITRE Corporation, May 1984), p. 19.

2. Raymond Tate, "Worldwide C^3I and Telecommunications," Seminar on Command, Control, Communications, and Intelligence Guest Presentations - Spring 1980. (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1980) p. 26.

3. Francis W. A'Hearn, The Information Arsenal: A C^3I Profile (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1983) p. 100.

4. Lee Paschall, "C^3I and the National Military Command System," Seminar on Command, Control, Communications, and Intelligence. Guest Presentations - Spring 1980. (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1980) p. 71.

5. Robert F. Kennedy, Thirteen Days: Cuban Missile Crisis (New York: W.W. Norton and Co., 1969) p. 2.

6. Jon L. Boyes, "Crisis Stability and C^3I," Signal, Vol. 38, no. 7, March 1984, p. 11.

7. Ibid., p. 12.

8. "U.S.-Soviet Accord on New Hot Line," The New York Times, July 18, 1984.

9. The aircraft radio operator routinely reserved a wide range of frequencies across the radio spectrum as insurance in case atmospheric interference rendered some frequencies unusable. This time, frequencies all across the radio band were disrupted by interference -- an extraordinary occurrence. Transmissions from both the aircraft and the U.S. Embassy were garbled. The problem was unusual enough to prompt investigation. A majority of experts concluded that atmospheric interference and other technical difficulties were responsible, but the aircraft radio operator remained convinced that such prolonged and extensive interference could only have been man-made.

10. Henry A. Kissinger, Years of Upheaval (Boston: Little, Brown and Co., 1982) pp. 556, 557.

11. Interview by the author with Ambassador Hermann Eilts, 1984.

12. Oswald H. Ganley and Gladys D. Ganley, To Inform or to Control: The New Communications Networks (New York: McGraw-Hill Book Co., 1982) pp. 130-132.

13. Raymond Tate, "Worldwide C^3I and Telecommunications," p. 28.

14. John M. Goshko, "13 Freed Hostages Arrive Home," The Washington Post, November 23, 1979.

15. Oswald Ganley and Gladys D. Ganley, To Inform or to Control, pp. 138, 140, 141.

16. U.S. Department of State, Watch in the Sinai, p. 31.

17. Barry Cherniavsky, The Case of Sinai II Agreement Between Egypt and Israel (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1982) p. 24.

18. Ithiel de Sola Pool and Arthur B. Corte, The Implications for American Foreign Policy of Low-Cost Non-Voice Communications. A Report to the Department of State. (Cambridge, Mass.: Center for Policy Alternatives and Center for International Studies, Massachusetts Institute of Technology, 1975) pp. 149-150.

19. Stuart E. Branch, "C^3I Within the Department of State," Signal, Vol. 37, no. 9, May 1983, p. 17.

20. Charles Rose, "Congress and C^3I," Seminar on Command, Control Communications and Intelligence. Guest Presentations - Spring 1981. (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1981) p. 170.

21. Robert Rosenberg, "The Influence of Policy on C^3I," Seminar on Command, Control Communications and Intelligence. Guest Presentations - Spring 1981. (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1981) p. 53.

22. B.R. Inman, "Issues in Intelligence," Seminar on Command, Control Communications and Intelligence. Guest Presentations - Spring 1981. (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1981) p. 196.

23. Richard Martin, Stopping the Unthinkable: C^3I Dimensions of Terminating a "Limited" Nuclear War (Cambridge, Mass.: Program on Information Resources Policy, Harvard University, 1982) p. 1.

24. Jon L. Boyes, "Crisis Stability and the C^3I," p. 11.

25. Thomas C. Schelling, Arms and Influence. New Haven, Conn.: Yale University Press, 1966) pp. 262, 263.

26. Richard Martin, Stopping the Unthinkable: C^3I Dimensions of Terminating a "Limited" Nuclear War, p. 10.

APPENDIX A

National Directives That Provide Policy Guidance

NSDD-55
Continuity of Government

NSDD-47
Mobilization Planning

PD-53
National Security Telecommunications Policy

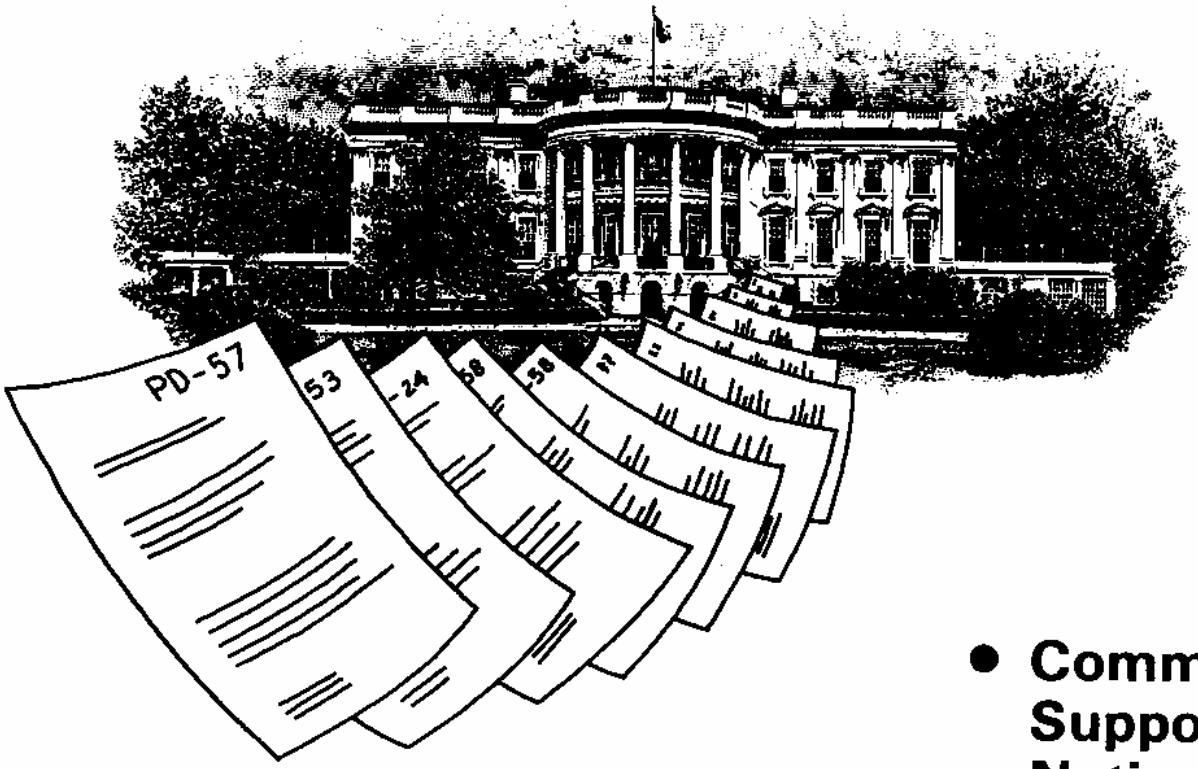
NSDD-42
National Space Policy

NSDD-13
Revised Nuclear Targeting Strategy

PD-24
Telecommunications Protection Policy

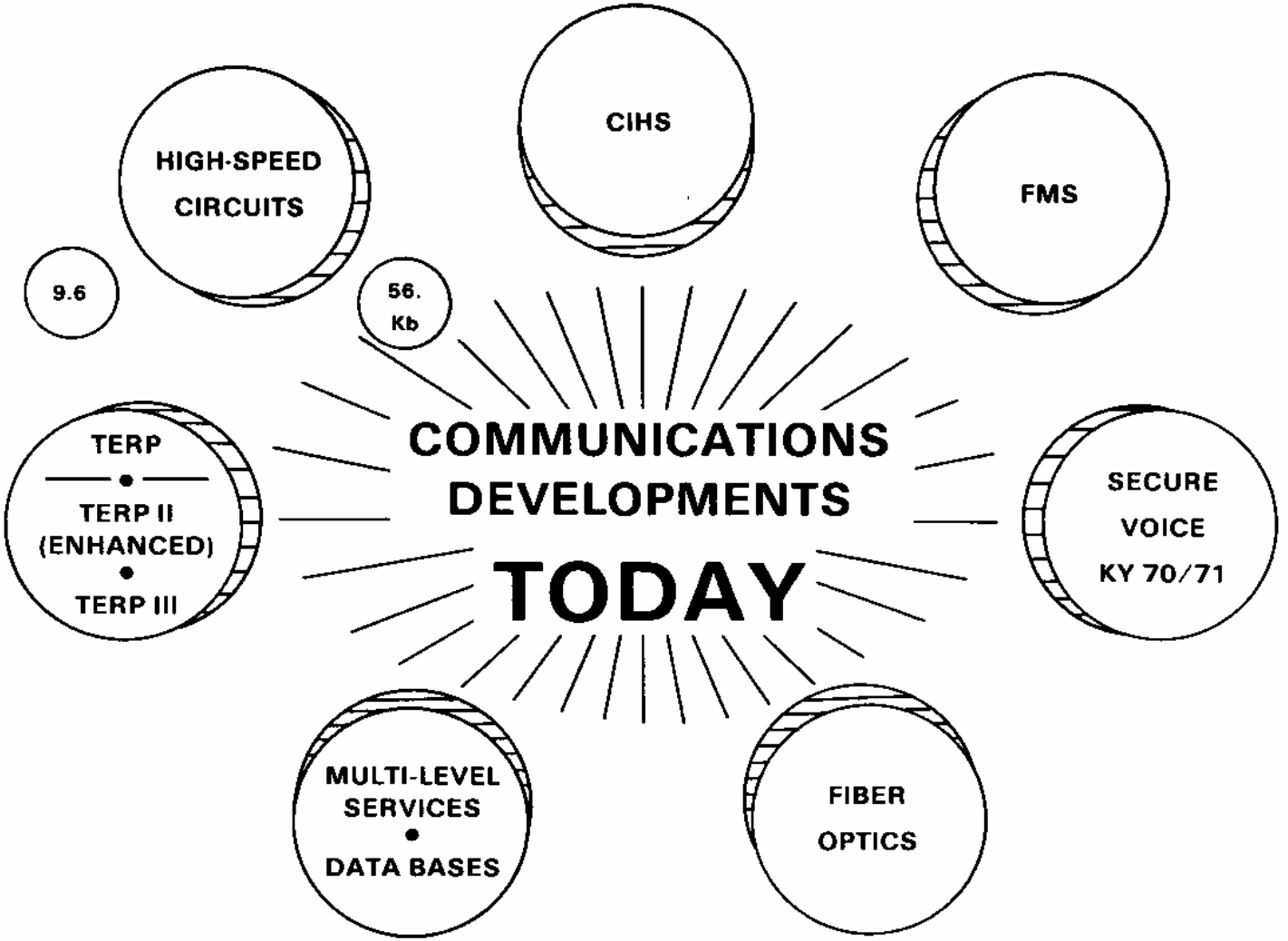
Office of Communications

Presidential Directives

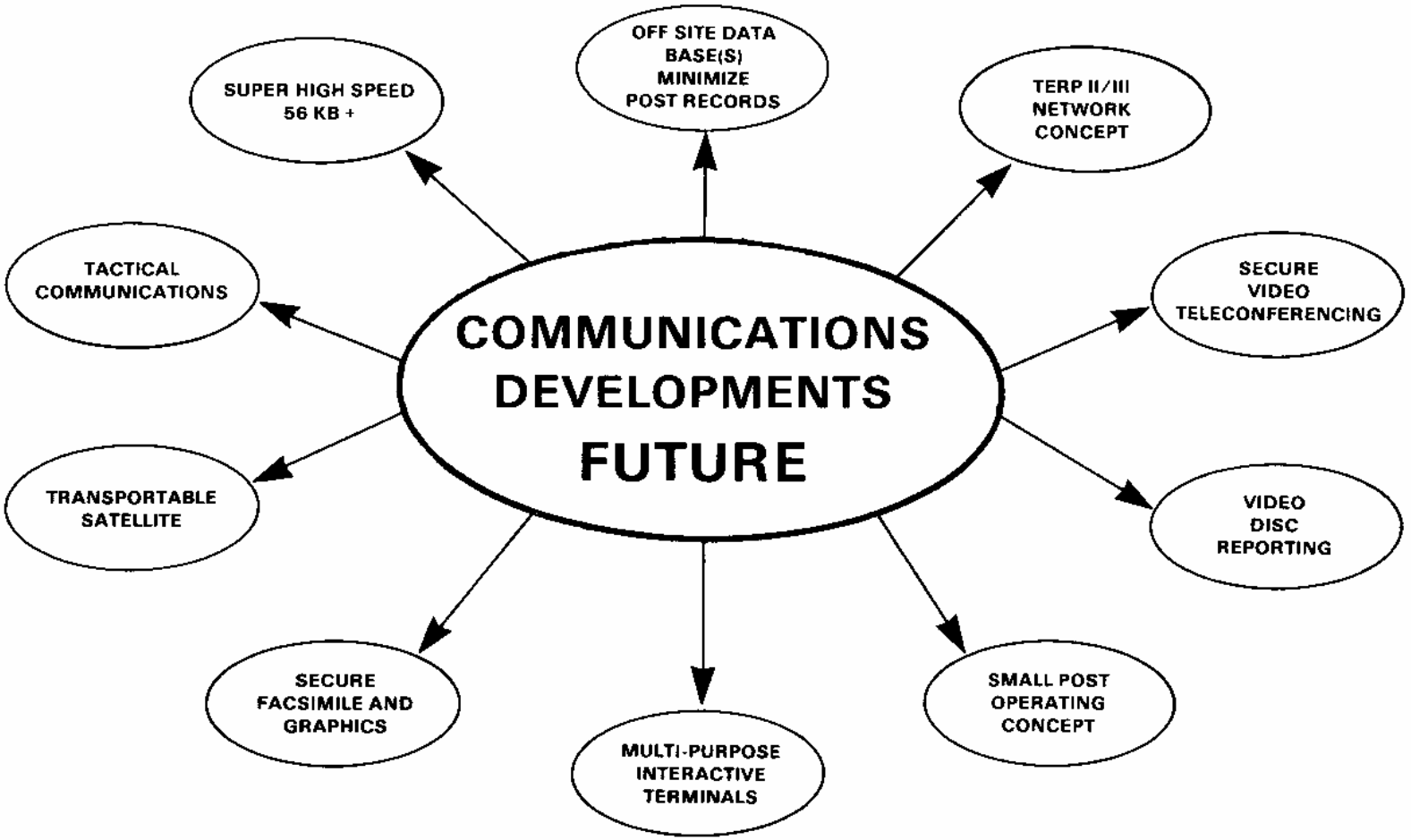


- **Communications Support for National Security Responsibilities**

Office of Communications

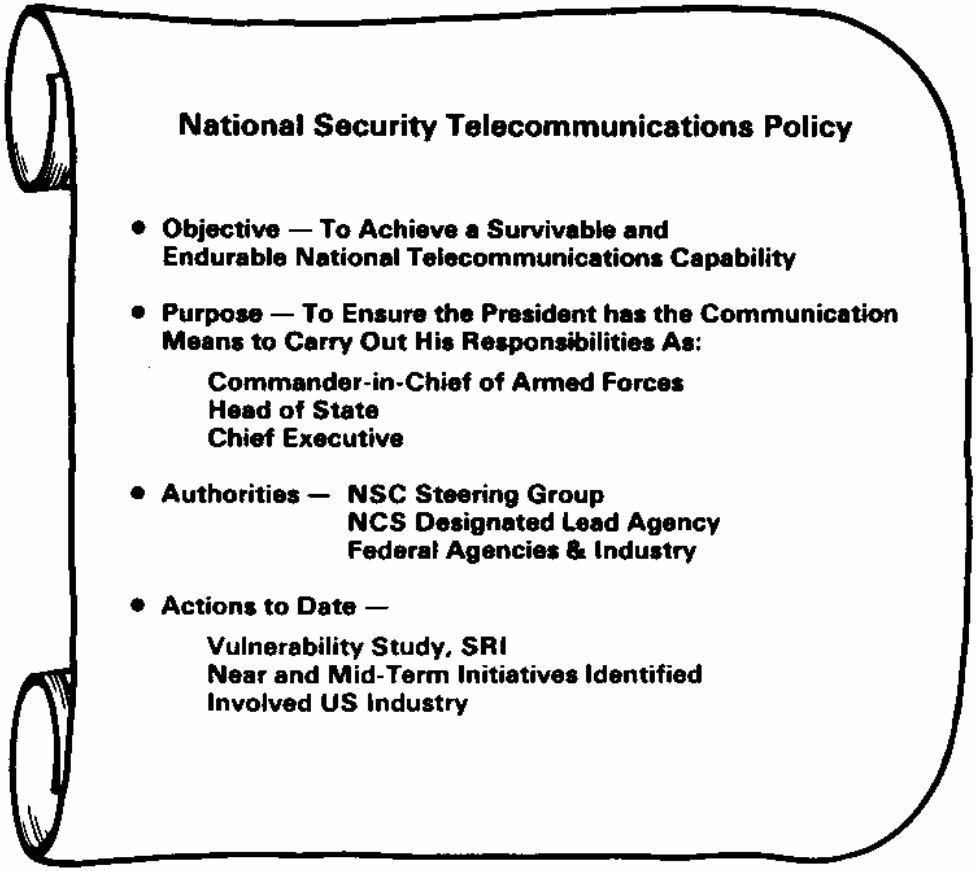


Office of Communications



Office of Communications

Presidential Directive 53



National Security Roles for the Department of State

- War Avoidance Through Diplomacy
- Negotiation Washington/Moscow DCL (Hot Line)
- Negotiate End to Hostilities
- Reconstitute International Relations
- Maintenance of Command Control Communications for Foreign Affairs Community

PD-53 INTERNATIONAL TELECOMMUNICATIONS INITIATIVE (March 24, 1983)

- **OBJECTIVE:** Ensure that USG will have Telecommunications Facilities adequate to satisfy needs of Nation during times of stress.

- **RESPONSIBILITIES:** Department of State assess availability and sufficiency of circuitry leased from non-U.S. carriers, and to propose remedial measures.

- **ACTIONS TO DATE:** Political underpinning agreed with foreign ministries in eight Western European capitals. Provide basis for Embassy/PTT discussions. Target to reach key capitals in all geographic areas.

Diplomatic Telecommunications Service
EXECUTIVE ORDER

- The DTS is the organization in DOS which is the Provider of Telecommunications Services to all U.S. Diplomatic and Consular Missions Overseas.
- Federal Agencies represented at U.S. Diplomatic and Consular Missions Overseas will utilize DTS resources in meeting Telecommunications Requirements.
- Agencies shall present all of their Telecommunications Requirements to the DTS. The DTS will see that these requirements are met.
- The DTS will insure rapid, reliable and secure Telecommunications Services in time of Peace and Crisis.
- The DTS will include a mix of Government owned and Non-government owned Transmission Systems.

ROLE FOR NSTAC

- 30 Chief Executive Officers called by President to examine PD-53 Objectives.

- Determine private U.S. International Resources and how such could be utilized by USG in times of stress.

- Using NSTAC mandate and framework, draw on members' knowledge of Telecommunications Facilities, Networks and Services in our examination of Vulnerabilities; Assessment of risks; and identification of practicable remedial action.

- Description of how U.S. carriers assure the continuity of Foreign Governments' Diplomatic Telecommunications in U.S. provide basis for requesting reciprocal treatment abroad.

APPENDIX B

THE WHITE HOUSE

EXECUTIVE ORDER NO. 12472

- - - - -

ASSIGNMENT OF NATIONAL SECURITY AND EMERGENCY PREPAREDNESS TELECOMMUNICATIONS FUNCTIONS

By the authority vested in me as President by the Constitution and laws of the United States of America, including the Communications Act of 1934, as amended (47 U.S.C. 151), the National Security Act of 1947, as amended, the Defense Production Act of 1950, as amended (50 U.S.C. App. 2061), the Federal Civil Defense Act of 1950, as amended (50 U.S.C. App. 2251), the Disaster Relief Act of 1974 (42 U.S.C. 5121), Section 5 of Reorganization Plan No. 1 of 1977 (3 C.F.R. 197, 1978 Comp.), and Section 203 of Reorganization Plan No. 3 of 1978 (3 C.F.R. 389, 1978 Comp.), and in order to provide for the consolidation of assignment and responsibility for improved execution of national security and emergency preparedness telecommunications functions, it is hereby ordered as follows:

Section 1. The National Communications System.

(a) There is hereby established the National Communications System (NCS). The NCS shall consist of the telecommunications assets of the entities [emphasis added] represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals and the Manager. The NCS Committee of Principals shall consist of representatives from those Federal

departments, agencies or entities, designated by the President, which lease or own telecommunications facilities or services of significance to national security or emergency preparedness, [emphasis added] and, to the extent permitted by law, other Executive entities which bear policy, regulatory or enforcement responsibilities of importance to national security or emergency preparedness telecommunications capabilities.

(b) The mission of the NCS shall be to assist the President, the national Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in:

(1) the exercise of the telecommunications functions and responsibilities set forth in Section 2 of this Order; and

(2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal government under all circumstances, including crisis or emergency, attack, recovery and reconstitution.

(c) The NCS shall seek to ensure that a national telecommunications infrastructure is developed which:

(1) Is responsive to the national security and emergency preparedness needs of the President and the Federal departments, agencies and other entities, including telecommunications in support of national security leadership and continuity of government;

(2) Is capable of satisfying priority telecommunications requirements under all circumstances through use of commercial, government and privately owned telecommunications resources;

(3) Incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability and

security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances, including conditions of crisis or emergency; and

(4) Is consistent, to the maximum extent practicable, with other national telecommunications policies.

(d) To assist in accomplishing its mission, the NCS shall:

(1) serve as a focal point for joint industry-government national security and emergency preparedness telecommunications planning; and

(2) establish a joint industry-government National Coordinating Center which is capable of assisting in the initiation, coordination, restoration and reconstitution of national security or emergency preparedness telecommunications services or facilities under all conditions of crisis or emergency.

(e) The Secretary of Defense is designated as the Executive Agent for the NCS. The Executive Agent shall:

(1) Designate the Manager of the NCS;

(2) Ensure that the NCS conducts unified planning and operations, in order to coordinate the development and maintenance of an effective and responsive capability for meeting the domestic and international national security and emergency preparedness telecommunications needs of the Federal government;

(3) Ensure that the activities of the NCS are conducted in conjunction with the emergency management activities of the Federal Emergency Management Agency;

(4) Recommend, in consultation with the NCS Committee of Principals, to the National Security Council, the Director of the Office

of Science and Technology Policy, or the Director of the Office of Management and Budget, as appropriate:

a. The assignment of implementation or other responsibilities to NCS member entities;

b. New initiatives to assist in the exercise of the functions specified in Section 2; and

c. Changes in the composition or structure of the NCS;

(5) Oversee the activities of and provide personnel and administrative support to the Manager of the NCS;

(6) Provide staff support and technical assistance to the National Security Telecommunications Advisory Committee established by Executive Order No. 12382, as amended; and

(7) Perform such other duties as are from time to time assigned by the President or his authorized designee.

(f) The NCS Committee of Principals shall:

(1) Serve as the forum in which each member of the Committee may review, evaluate, and present views, information and recommendations concerning ongoing or prospective national security or emergency preparedness telecommunications programs or activities of the NCS and the entities represented on the Committee;

(2) Serve as the forum in which each member of the committee shall report on and explain ongoing or prospective telecommunications plans and programs developed or designed to achieve national security or emergency preparedness telecommunications objectives;

(3) Provide comments or recommendations, as appropriate, to the National Security Council, the Director of the Office of Science and Technology Policy, the Director of the Office of Management and Budget,

the Executive Agent, or the Manager of the NCS, regarding ongoing or prospective activities of the NCS; and

(4) Perform such other duties as are from time to time assigned by the President or his authorized designee.

(g) The Manager of the NCS shall:

(1) Develop for consideration by the NCS Committee of Principals and the Executive Agent:

a. A recommended evolutionary telecommuniations architecture designed to meet current and future Federal government national security and emergency preparedness telecommunications requirements;

b. Plans and procedures for the management, allocation and use, including the establishment of priorities or preferences, of Federally owned or leased telecommunications assets under all conditions of crisis or emergency;

c. Plans, procedures and standards for minimizing or removing technical impediments to the interoperability of government-owned and/or commercially-provided telecommunications systems;

d. Test and exercise programs and procedures for the evaluation of the capability of the Nation's telecommunications resources to meet national security or emergency preparedness telecommunications requirements; and

e. Alternative mechanism for funding, through the budget review process, national security or emergency preparedness telecommunications initiatives which benefit multiple Federal departments, agencies, or entities. Those mechanisms recommended by the NCS Committee of Principals and the Executive Agent shall be submitted to the Director of the Office of Management and Budget.

(2) Implement and administer any approved plans or programs as assigned, including any system of priorities and preferences for the provision of communications service, in consultation with the NCS Committee of Principals and the Federal Communications Commission, to the extent practicable or otherwise required by law or regulation;

(3) Chair the NCS Committee of Principals and provide staff support and technical assistance thereto;

(4) Serve as a focal point for joint industry-government planning, including the dissemination of technical information, concerning the national security or emergency preparedness telecommunications requirements of the Federal government;

(5) Conduct technical studies or analyses, and examine research and development programs, for the purpose of identifying, for consideration by the NCS Committee of Principals and the Executive Agent, improved approaches which may assist Federal entities in fulfilling national security or emergency preparedness telecommunications objectives;

(6) Pursuant to the Federal Standardization Program of the General Services Administration, and in consultation with other appropriate entities of the Federal government including the NCS Committee of Principals, manage the Federal Telecommunications Standards Program, ensuring wherever feasible that existing or evolving industry, national, and international standards are used as the basis for Federal telecommunications standards; and

(7) Provide such reports and perform such other duties as are from time to time assigned by the President or his authorized designee, the Executive Agent, or the NCS Committee of Principals. Any such

assignments of responsibility to, or reports made by, the Manager shall be transmitted through the Executive Agent.

Sec. 2. Executive Office Responsibilities. (a) Wartime Emergency Functions. (1) The National Security Council shall provide policy direction for the exercise of the war power functions of the President under Section 606 of the Communications Act of 1934, as amended (47 U.S.C. 606), should the President issue implementing instructions in accordance with the National Emergencies Act (50 U.S.C. 1601).

(2) The Director of the Office of Science and Technology Policy shall direct the exercise of the war power functions of the President under Section 606 (a), (c)-(e), of the Communications Act of 1934, as amended (47 U.S.C. 606), should the President issue implementing instructions in accordance with the National Emergencies Act (50 U.S.C. 1601).

(b) Non-Wartime Emergency Functions. (1) The National Security Council shall:

a. Advise and assist the President in coordinating the development of policy, plans, programs and standards within the Federal government for the identification, allocation, and use of the Nation's telecommunications resources by the Federal government, and by State and local governments, private industry and volunteer organizations upon request, to the extent practicable and otherwise consistent with law, during those crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law; and

b. Provide policy direction for the exercise of the President's non-wartime emergency telecommunications functions, should the President so instruct.

(2) The Director of the Office of Science and Technology Policy shall provide information, advice, guidance and assistance, as appropriate, to the President and to those Federal departments and agencies with responsibilities for the provision, management, or allocation of telecommunications resources, during those crises or emergencies in which the exercise of the President's war power functions is not required or permitted by law;

(3) The Director of the Office of Science and Technology Policy shall establish a Joint Telecommunications Resources Board (JTRB) to assist him in the exercise of the functions specified in this subsection. The Director of the Office of Science and Technology Policy shall serve as chairman of the JTRB; select those Federal departments, agencies, or entities which shall be members of the JTRB; and specify the functions it shall perform.

(c) Planning and Oversight Responsibilities. (1) The National Security Council shall advise and assist the President in:

a. Coordinating the development of policy, plans, programs and standards for the mobilization and use of the Nation's commercial, government, and privately owned telecommunications resources, in order to meet national security or emergency preparedness requirements;

b. Providing policy oversight and direction of the activities of the NCS; and

c. Providing policy oversight and guidance for the execution of the responsibilites assigned to the Federal departments and agencies by this Order.

(2) The Director of the Office of Science and Technology Policy shall make recommendations to the President with respect to the test,

exercise and evaluation of the capability of existing and planned communications systems, networks or facilities to meet national security or emergency preparedness requirements and report the results of any such tests or evaluations and any recommended remedial actions to the President and to the National Security Council;

(3) The Director of the Office of Science and Technology Policy or his designee shall advise and assist the President in the administration of a system of radio spectrum priorities for those spectrum dependent telecommunications resources of the Federal government which support national security or emergency preparedness functions. The Director also shall certify or approve priorities for radio spectrum use by the Federal government, including the resolution of any conflicts in or among priorities, under all conditions of crisis or emergency; and

(4) The National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget shall, in consultation with the Executive Agent for the NCS and the NCS Committee of Principals, determine what constitutes national security and emergency preparedness telecommunications requirements.

(d) Consultation with Federal Departments and Agencies. In performing the functions assigned under this Order, the National Security Council and the Director of the Office of Science and Technology Policy, in consultation with each other, shall:

(1) Consult, as appropriate, with the Director of the Office of Management and Budget; the Director of the Federal Emergency Management Agency with respect to the emergency management responsibilities assigned pursuant to Executive Order No. 12148, as amended; the

Secretary of Commerce, with respect to responsibilities assigned pursuant to Executive Order No. 12046; the Secretary of Defense, with respect to Executive Order No. 12333; and the Chairman of the Federal Communications Commission or his authorized designee; and

(2) Establish arrangements for consultation among all interested Federal departments, agencies or entities to ensure that the national security and emergency preparedness communications needs of all Federal government entities are identified; that mechanisms to address such needs are incorporated into pertinent plans and procedures; and that such needs are met in a manner consistent, to the maximum extent practicable, with other national telecommunications policies.

(e) Budgetary Guidelines. The Director of the Office of Management and Budget, in consultation with the National Security Council and the NCS, will prescribe general guidelines and procedures for reviewing the financing of the NCS within the budgetary process and for preparation of budget estimates by participating agencies. These guidelines and procedures may provide for mechanisms for funding, through the budget review process, national security and emergency preparedness telecommunications initiatives which benefit multiple Federal departments agencies, or entities.

Sec. 3. Assignment of Responsibilities To Other Departments and Agencies. In order to support and enhance the capability to satisfy the national security and emergency preparedness telecommunications needs of the Federal government, State and local governments, private industry and volunteer organizations, under all circumstances including those of crisis or emergency, the Federal departments and agencies shall perform the following functions:

(a) Department of Commerce. The Secretary of Commerce shall, for all conditions of crisis or emergency: (1) Develop plans and procedures concerning radio spectrum assignments, priorities and allocations for use by Federal departments, agencies and entities; and

(2) Develop, maintain and publish policy, plans, and procedures for the control and allocation of frequency assignments, including the authority to amend, modify or revoke such assignments, in those parts of the electromagnetic spectrum assigned to the Federal government.

(b) Federal Emergency Management Agency. The Director of the Federal Emergency Management Agency shall:

(1) Plan for and provide, operate and maintain telecommunications services and facilities, as part of its National Emergency Management System, adequate to support its assigned emergency management responsibilities;

(2) Advise and assist State and local governments and volunteer organizations, upon request and to the extent consistent with law, in developing plans and procedures for identifying and satisfying their national security or emergency preparedness telecommunications requirements;

(3) Ensure, to the maximum extent practicable, that national security and emergency preparedness telecommunications planning by State and local governments and volunteer organizations is mutually supportive and consistent with the planning of the Federal government; and

(4) Develop, upon request and to the extent consistent with law and in consonance with regulations promulgated by and agreements with the Federal Communications Commission, plans and capabilities for, and provide policy and management oversight of, the Emergency Broadcast

System, and advise and assist private radio licensees of the Commission in developing emergency communications plans, procedures and capabilities.

(c) Department of State. The Secretary of State, in accordance with assigned responsibilities within the Diplomatic Telecommunications System, shall plan for and provide, operate and maintain rapid, reliable and secure telecommunications services to those Federal entities represented at United States diplomatic missions and consular offices overseas [emphasis added]. This responsibility shall include the provision and operation of domestic telecommunications in suppport of assigned national security or emergency preparedness responsibilities.

(d) Department of Defense. In addition to the other responsibilities assigned by this Order, the Secretary of Defense shall:

(1) Plan for and provide, operate and maintain telecommunications services and facilities adequate to support the National Command Authorities and to execute the responsibilities assigned by Executive Order No. 12333; and

(2) Ensure that the Director of the National Security Agency provides the technical support necessary to develop and maintain plans adequate to provide for the security and protection of national security and emergency preparedness telecommunications.

(e) Department of Justice. The Attorney General shall, as necessary, review for legal sufficiency, including consistency with the antitrust laws, all policies, plans or procedures developed pursuant to responsibilities assigned by this Order.

(f) Central Intelligence Agency. The Director of Central Intelligence shall plan for and provide, operate, and maintain

telecommunications services adequate to support its assigned responsibilities, including the dissemination of intelligence within the Federal government.

(g) General Services Administration. Except as otherwise assigned by this order, the Administrator of General Services, consistent with policy guidance provided by the Director of the Office of Management and Budget, shall ensure that Federally owned or managed domestic communications facilities and services meet the national security and emergency preparedness requirements of the Federal civilian departments, agencies and entities.

(h) Federal Communications Commission. The Federal Communications Commission shall, consistent with Section 4(c) of this Order:

(1) Review the policies, plans and procedures of all entities licensed or regulated by the Commission that are developed to provide national security or emergency preparedness communications services, in order to ensure that such policies, plans and procedures are consistent with the public interest, convenience and necessity;

(2) Perform such functions as required by law with respect to all entities licensed or regulated by the Commission, including (but not limited to) the extension, discontinuance or reduction of common carrier facilities or services; the control of common carrier rates, charges, practices and classifications; the construction, authorization, activation, deactivation or closing of radio stations, services and facilities; the assignment of radio frequencies to Commission licensees; the investigation of violations of pertinent law and regulation; and the initiation of appropriate enforcement actions;

(3) Develop policy, plans and procedures adequate to execute the responsibilities assigned in this Order under all conditions or crisis or emergency; and

(4) Consult as appropriate with the Executive Agent for the NCS and the NCS Committee of Principals to ensure continued coordination of their respective national security and emergency preparedness activities.

(i) All Federal departments and agencies, to the extent consistent with law (including those authorities and responsibilities set forth in Section 4(c) of this Order), shall:

(1) Determine their national security and emergency preparedness telecommunications requirements, and provide information regarding such requirements to the Manager of the NCS;

(2) Prepare policies, plans and procedures concerning telecommunications facilities, services or equipment under their management or operational control to maximize their capability of responding to the national security or emergency preparedness needs of the Federal government;

(3) Provide, after consultation with the Director of the Office of Management and Budget, resources to support their respective requirements for national security and emergency preparedness telecommunications; and provide personnel and staff support to the Manager of the NCS as required by the President;

(4) Make information available to, and consult with, the Manager of the NCS regarding agency telecommunications activities in support of national security or emergency preparedness;

(5) Consult, consistent with the provisions of Executive Order No. 12046, as amended, and in conjunction with the Manager of the NCS, with the Federal Communications Commission regarding execution of responsibilities assigned by this Order;

(6) Submit reports annually, or as otherwise requested, to the Manager of the NCS, regarding agency national security or emergency preparedness telecommunications activities; and

(7) Cooperate with and assist the Executive Agent for the NCS, the NCS Committee of Principals, the Manager of the NCS, and other departments and agencies in the execution of the functions set forth in this Order, furnishing them such information, support and assistance as may be required.

(j) Each Federal department or agency shall execute the responsibilities assigned by this Order in conjunction with the emergency management activities of the Federal Emergency Management Agency, and in regular consultation with the Executive Agent for the NCS and the NCS Committee of Principals to ensure continued coordination of NCS and individual agency telecommunications activities.

Sec. 4. General Provisions. (a) All Executive departments and agencies may issue such rules and regulations as may be necessary to carry out the functions assigned under this Order.

(b) In order to reflect the assignments of responsibility provided by this Order,

(1) Sections 2-414,, 4-102, 4-103, 4-202, 4-302, 5-3, and 6-101 of Executive Order No. 12046, as amended, are revoked;

(2) The Presidential Memorandum of August 21, 1963, as amended, entitled "Establishment of the National Communications Systems", is hereby superseded; and

(3) Section 2-411 of Executive Order No. 12046, as amended, is further amended by deleting the period and inserting, "except as otherwise provided by Executive Order No." and inserting the number assigned to this Order.

(c) Nothing in this Order shall be deemed to affect the authorities or responsibilities of the Director of the Office of Management and Budget, or any Office or official thereof; or reassign any function assigned any agency under the Federal Property and Administrative Services Act of 1949, as amended; or under any other law; or any function vested by law in the Federal Communications Commission.

Sec. 5. This order shall be effective upon publication in the Federal Register.

RONALD REAGAN

THE WHITE HOUSE,

April 3, 1984