Nationwide Emergency Telecommunications Service for National Security Telecommunications: Interim Report to the National Communications System (1987)

Pages
87

Size
8.5 x 10

ISBN
0309320836

Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications; Board on Telecommunications-Computer Applications; Commission on Engineering and Technical Systems; National Research Council

Nationwide Emergency Telecommunications Service for National Security Telecommunications

Interim Report to the National Communications System

by the Committee on Review of Switching, Synchronization
and Network Control in National Security Telecommunications
Board on Telecommunications-Computer Applications
Commission on Engineering and Technical Systems
National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. August 1987

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Frank Press is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Robert M. White is president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Samuel O. Thier is president of the Institute of Medicine.

The National Research Council was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Frank Press and Dr. Robert M. White are chairman and vice chairman, respectively, of the National Research Council.

The project is supported by Contract No. DCA100-87-C-0069 between the National Communications System and the National Academy of Sciences.

Available from:

Board on Telecommunications and Computer Applications
Commission on Engineering and Technical Systems
National Research Council
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

Printed in the United States of America

COMMITTEE ON REVIEW OF SWITCHING, SYNCHRONIZATION AND NETWORK CONTROL IN NATIONAL SECURITY TELECOMMUNICATIONS

JOHN C. McDONALD (Chairman)
Vice President, Chief Scientist
CONTEL Corporation, Inc.

PAUL BARAN
Chairman
METRICOM

FLOYD BECKER
Visiting Lecturer
University of Colorado

CULLEN M. CRAIN
Department Head
Engineering and Applied Sciences Dept.
The Rand Corporation

HOWARD FRANK
President
Howard Frank Associates

LEWIS E. FRANKS
Professor of Electrical and Computer Engineering
University of Massachusetts

PAUL E. GREEN, JR.
Staff Member
Computer Sciences Department
IBM-Yorktown

E. FLETCHER HASELTON
Vice President
Teknekron Infoswitch Corp.

AMOS E. JOEL, JR.
Executive Consultant

DONALD M. KUYPER
Group Vice President, Business Services
GTE Telephone Operating Group

DAVID L. MILLS
Professor
Department of Electrical Engineering
University of Delaware

LEE M. PASCHALL
Chairman, Retired
American Satellite Company

CASIMIR S. SKRZYPCZAK
Vice President, Science and Technology
NYNEX CORPORATION

DANIEL J. FINK (Ex-Officio)
President
D.J. Fink Associates, Inc.

ERIK K. GRIMMELMANN (Observer)
Head, Government Communications Systems Department
AT&T Bell Laboratories

STAFF

Richard B. Marsten, Director
Wayne G. Kay, Study Director
Karen Laughlin, Administrative Coordinator

BOARD ON TELECOMMUNICATIONS AND COMPUTER APPLICATIONS

STAFF

Richard B. Marsten, Executive Director
Anthony M. Forte, Senior Staff Officer
Karen Laughlin, Administrative Coordinator
Lois A. Leak, Administrative Assistant

PREFACE

This is the first of two reports to be rendered by the National Research Council's Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications for the National Communications System. The Committee was established October 31, 1986 at the request of the Manager, National Communications System (NCS). It conducted this phase of the study over the period November 3, 1986 to April 30, 1987. In this phase the purpose of the committee was to conduct an evaluation of the Nationwide Emergency Telecommunications System* (NETS), including component and system vulnerability, the technical longevity of the system design, and the possible suitability of alternative technical approaches to achieving program objectives.

The Nationwide Emergency Telecommunications Service (NETS) is one of three programs that will provide survivability improvements in national security emergency preparedness (NSEP) telecommunications capabilities as required by Presidential order in National Security Decision Directive (NSDD) 97. The other two programs are Commercial Satellite Communications Interconnectivity (CSI) and Commercial Network Survivability (CNS). These programs are designed to meet current and future requirements of the federal government for national security and emergency preparedness telecommunications. NETS is the largest of the three programs and is intended to provide survivable, switched, voice and data service.

The Committee review and report in this first phase had a tightly focused and specific purpose. Because of the critical timing of program and budget decisions, the Manager, NCS, requested a quick-reaction assessment, to culminate in a briefing six months after study

---

*During but not as a result of the Committee's studies the NCS changed the S in the acronym NETS from "system" to "service." Nevertheless, because the functions NETS must provide remain the same, the Committee's conclusions stand. It did, indeed, conduct its studies regarding NETS as a service with a proposed system implementation as an "existence proof."

inception, and a formal, written report within three months after the briefing. The Committee, consisting of experts in telecommunications from government, industry and academia, held its first meeting on November 3, 1986. The Committee operated by having formal briefings interspersed with executive sessions where issues were identified, analyzed, and resolved. At the Committee's inaugural meeting, Mr. Benham Morriss, Deputy Manager, NCS, noted that the NRC has conducted two previous, related studies for the NCS. The current study was most important because the NCS was at a decision point concerning the NETS. The Committee was to look at the whole picture: technology, longevity, survivability, performance effectiveness, cost effectiveness, and program parameters, and assess whether or not the NCS was on the correct program path. Particularly, he asked if the NCS plan makes sense in light of technology advancements, applications, and changes in the industry, keeping in mind that NETS survivability and the ability to reconstitute communications are of paramount importance.

In-depth briefings were presented by members of the NCS staff covering: 1) the NCS and its structure, mission, and relationship to other government agencies; 2) the NETS: its evolution, parameters, and components to date; 3) national security emergency preparedness (NSEP) requirements and the threat; and 4) the public switched network (PSN) and its relationship to NETS.

Five additional Committee meetings were held. For these, the Committee wishes to acknowledge presentations on aspects of NETS given by officials of the National Communications System, the Departments of Agriculture and Justice, the Federal Emergency Management Agency, and the General Services Administration. The Committee also wishes to acknowledge presentations on NSEP telecommunications made by U.S. Sprint, MCI, AT&T Communications, GTE, Contel, Bell Communications Research, American Satellite Company, Northern Telecom, AT&T Bell Laboratories, and Booz Allen & Hamilton, who provided rich insights into the subject matter and facilitated the Committee's understanding of the planning, technology, issues, and operations relating to the PSN, NETS and NSEP telecommunications.

The Committee's formal briefing was given to Lt. Gen. Winston Powers, Manager, NCS, and his key staff on April 22, 1987. This document constitutes the Committee's formal, written report.

The committee concept of the National Research Council operates successfully and effectively in large part because of the rapport with, cooperation, and support from the agency it is assisting, the committee members themselves, and the staff behind it all. From the NCS, we sincerely appreciate the contributions and support of Mr. Benham Morriss, Dr. Bruce Barrow, Mr. Kenneth Boheim and Mr. Edward Greene, our NCS Contract Officer's Technical Representative.

The Committee is particularly grateful to Dr. Richard B. Marsten, Executive Director of the Board on Telecommunications and Computer

Applications (BOTCAP), for his counsel, guidance, continued support, and contributions throughout this project. The Committee also extends its sincere appreciation to Wayne G. Kay, consultant and study director. In addition, I personally wish to acknowledge the contributions of my assistant, John Wohlstetter.

A committee effort of this scope imposes extraordinary requirements on the administrative staff. With pleasure, the Committee acknowledges Karen Laughlin for her expert administrative and secretarial support.

Finally, as the Committee chairman, I want to express my personal thanks to my colleagues, the Committee members, for their dedicated efforts.

John C. McDonald, Chairman
Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications

COMMITTEE ON REVIEW OF SWITCHING, SYNCHRONIZATION AND NETWORK CONTROL IN NATIONAL SECURITY TELECOMMUNICATIONS

BOARD ON TELECOMMUNICATIONS-COMPUTER APPLICATIONS
COMMISSION ON ENGINEERING AND TECHNICAL SYSTEMS

STATEMENT OF TASK

The Committee will review and assess the effectiveness of the Nationwide Emergency Telecommunications System* (NETS), a network control system for provision of survivable national security emergency preparedness (NSEP) telecommunications under development for the National Communications System; provide an independent review of the survivability of synchronization in digital networks; and assess the vulnerability of switching and signaling control in view of the increasing centralization of these functions. Specifically, the Committee will perform the following tasks:

1. The Committee will review the objectives of the NETS program, assess the approach that has been followed and the work that has been done, review technological developments that could provide alternatives to NETS, and make recommendations to ensure that future NETS work will be effective and can take advantage of advances in technology and of changes in the telecommunications environment. The Committee will comment on the vulnerability of NETS, its technical longevity, and possible alternative technical approaches to achieving its network control and survivability objectives. This review will be conducted prior to engaging in the succeeding two tasks.

2. The Committee will conduct a review to assess the inventory of synchronization assets and will assess the extent to which synchronization vulnerabilities might be mitigated by exploiting distributed, interconnected subsets of the public switched network. It will assess whether adequate synchronization capabilities are likely to exist to support national security emergency preparedness (NSEP) telecommunications during the weeks or months of NSEP telecommunications restoration and reconstitution after natural disaster or attack on the country, including nuclear attack. It will

---

* This was the original statement of the study task. Midway through the NETS study the NCS changed from "System" to "Service." The Committee has attempted to assess NETS in both systems and service aspects. Hereafter, in accordance with that change, the Committee views apply to a service, not a system.

recommend technical approaches to developing cost-effective, survivable synchronization and will suggest technical programs and management plans to realize these approaches.

3. The Committee will review the inventory of switching installations for survivability of switching and control functions after nuclear attack, considering redundancy and alternative connectivity. It will investigate emerging technologies such as burst and fast-packet switching for their possible applicability to cost-effective, survivable, switching and network-control facilities. It will assess the adequacy of surviving facilities to support or restore NSEP telecommunications switching, and recommend enhancements or alternative technology approaches likely to enhance survivability. In particular, it will consider opportunities to decentralize routing control for precedence traffic and alternative technologies that could provide cost-effective decentralization with enhanced survivability. Technical programs and management plans will be suggested to realize the recommended approaches.

DATE: November 3, 1986

CONTENTS

I. EXECUTIVE SUMMARY

A. What is the Nationwide Emergency Telecommunications Service (NETS)?

NETS is designed to provide survivable, switched voice and low-speed data communications for 20,000 authorized, Federal government users. The service will make a substantial pre-attack contribution to deterrence and resistance to terrorist attack and would provide essential communication after the U.S. is attacked by a large number of nuclear warheads. Left unmodified, the public switched network (PSN) could be rendered ineffective or inaccessible under a terrorist or nuclear attack. NETS gives the PSN a robust capability to provide communications with large portions of the PSN destroyed.

NETS must combine ease of use, ubiquity, adaptive routing capabilities, priority channel selection, robustness, and geographic diversity with the flexibility to incorporate new technologies. Ubiquity must not only include a large number of access locations to NETS but also include the ability of those individuals who need the service actually to access it.

The Committee has concluded that the only feasible source that can provide the full panoply of capabilities required for NETS is the aggregate of networks that constitute the PSN. The PSN comprises the transmission links and switching nodes maintained by the local-exchange and interexchange carriers, whether their services are offered to the general public by facilities-based or resale service providers. The PSN is, in effect, a network of networks, with in-place assets valued at roughly 250 billion dollars. NETS draws on this rich national asset to provide a unique NSEP capability.

While the current PSN is vulnerable to the destructive effects of a nuclear strike, no alternative to the PSN affords nearly comparable ease of use, ubiquity, adaptability, robustness, geographic diversity, or flexibility (see Chapter III for supporting detail).

NETS is intended to meet national security emergency preparedness (NSEP) objectives of providing communications services to federal, state and local government users. It must operate in pre-, trans-, and post-attack nuclear war environments. NETS is intended to be delivered through an applique to the PSN. By itself, the PSN is not sufficiently survivable to meet NSEP objectives. During a nuclear attack, much of the PSN would be damaged and many calls could not be completed even though surviving facilities might be available to route calls to the desired destination. NETS is designed to locate and use those surviving facilities through a robust, alternate-routing capability presently not resident in the PSN. In addition, NETS will restrict access to unauthorized users to prevent overload and sabotage, and will provide priority and preemption.

The PSN, however, has a distinctive vulnerability in its signaling means. Most network signaling now flows through common channels over packet switched networks using standards set by the International Consultative Committee for Telephone and Telegraph (CCITT). These common channels are very thin routes. For example, AT&T employs only 14 packet-like, signal-transfer switches for its entire network, and explosives in 14 locations could render the entire AT&T network useless. The NETS applique must negate this vulnerability.

Finally, NETS will employ centralized maintenance and administration to maintain a constant state of service readiness.

B. Issues Identified by the Committee.

The Committee raised 14 issues during the course of the NETS evaluation. These issues are itemized below. Issue descriptions and their resolutions are contained in Appendix A.

1. A means must be provided to enhance survivability of PSN signaling for NETS purposes.

2. Call-controller-to-call-controller access must have priority. [A call controller is a NETS hardware device. It may be either a call control module[1] (CCM) and its host switch or a switch internal module[2] (SIM). See Appendix B.]

3. Subscriber access to the originating call controller must be available in times of overload.

4. Access to the NETS must meet NSEP requirements.

5. Path selection must converge on available routes quickly.

6. NETS development strategy and field testing must ensure a reliable system.

7. NETS evolutionary capabilities and strategies must allow for incorporation of new technology.

8. Transmission and equalization requirements must be appropriate to the special uses of NETS under damage conditions.

---

[1] Call Control Module (CCM)-- A piece of equipment that is attached to a host switch via trunks and that provides NETS functions.

[2] Switch Internal Module (SIM)-- A set of hardware and software that is integrated into a host PSN switch to provide NETS functions.

9. The signaling protocols between call controllers must be robust.

10. NETS must provide for post-attack facility restoral.

11. How do interexchange carriers handle NETS calls?

12. Are there reasonable alternatives to NETS?

13. What are the capabilities and uses of the SIM versus the CCM?

14. Does NETS satisfy the 1986 predecessor committee's final report[1] objectives?

C. Conclusions and Recommendations

The Committee views the following NSEP requirements as basic:

1. Survivability of a voice capability must be independent of targeting scenarios.

2. The system must be cost-effective to prevent elimination from future budgets.

3. Access to the system must be ubiquitous in geography and in allowing those with legitimate need to use the service.

4. Use during an emergency must be restricted.

5. The system should allow rapid restoration after an attack.

There are many alternative ways to create an NSEP capability, including special, dedicated systems and overlays to existing systems. Targeting-scenario independence virtually eliminates dedicated systems, which, within reasonable cost considerations, would be too thin and vulnerable. An overlay to an existing system benefits from an existing asset base. Clearly the most ubiquitous, diverse, and intelligent of the assets available is the PSN.

The strength of the PSN lies in its large investment in place, estimated to exceed 250 billion dollars in value, and in its design for high reliability. The PSN is ubiquitous in its access and diverse in topography. Through the use of redundancy, it is robust in availability and traffic-handling capacity. Use of the telephone is familiar to everyone and the network is undergoing continuous modernization.

---

[1] The Policy Planning Environment for National Security Telecommunications (final report), National Academy Press, Washington, D.C., July 1986.

But what are the PSN's weaknesses? The PSN is only as strong as its weakest link, which may be any of common channel signaling, standby-power fuel-storage capacity, availability of maintenance personnel and spare parts, and traffic congestion during emergencies. In addition, the PSN is a network of networks with divided ownership of facilities and divided responsibility for an end-to-end call. Network technology is changing rapidly and new vulnerabilities could possibly creep in unnoticed. But virtually any other solution would suffer from comparable or greater vulnerabilities, and no alternative solution would embody strengths comparable to those in the PSN.

The Committee's conclusion is that the PSN is the preferred, existing network on which to build an NSEP capability. Its ubiquity, size, and value eliminate any possibility of constructing a new network for NETS from scratch.

The NETS applique to the PSN as it is currently defined has a series of strengths and weaknesses. The strengths are:

- NETS enables post-attack PSN use;
- It can be deployed in phases;
- It is widely available to intended users; and
- It is readily expandable.

While NETS can be deployed in phases, the Committee feels that at least 100 call controllers must be deployed to obtain a minimum NSEP capability. The Committee also feels that it is mandatory that NETS include a signaling transmission scheme that enhances the survivability of common signaling in the PSN. Pre-attack exercising of the system should be made automatic to ensure its effective use when actually needed. The Committee also urges emphasis of the deterrent value of NETS in strategic planning and publicizing of its existence once installed so that it become widely known internationally.

The major weaknesses of NETS are as follows:

- Cost makes it subject to budget cuts;
- It does not support unprogrammed users; and
- It suffers from PSN access congestion.

The Committee concludes that NETS, as currently conceived, is a "proof of existence"-- a demonstration with at least one physical system-- that the PSN can be suitably modified to create the desired NSEP capability. However, we are concerned that since NETS will be procured as a service, the actual system implementation might contain subtle vulnerabilities. The National Communications System (NCS) must

guard against this eventuality. One particular vulnerability may well be that the 20,000 designated, federal-government users may not be where they are most needed post-attack. The predecessor committee's reports [1,2] have commented on this and the likely appearance of grass-roots leaders at critical points. The NCS may well want to guard against this vulnerability by making NETS maximally available to a user population undefinable in advance, by making NETS access information easily accessible. Personal credit cards for Personal Identification Numbers constitute one approach.

The Committee recommends that the National Communications System consider the following modifications to NETS:

1. Substitute a Personal Identification Number such as a "credit card" in place of the Access Security Device (ASD) that gives authorized users access to NETS. This may reduce system cost and be more effective in a bottom-up reconstruction than that limited by ASD availability.

2. NETS traffic must contend with public traffic between the originating user and the originating call controller. The Committee recommends that NETS traffic be given priority at all locations in the PSN and that enabling legislation be enacted if required.

3. NETS calls use transmission compensation to ensure secure voice traffic in a heavily damaged network. The Committee recommends a limited deployment of compensation units since secure voice is only a major requirement during the pre-attack phase, when the network is undamaged. Limited deployment could serve the post-attack requirements.

4. Many of the functions of the call controllers and the controllers used to enhance the PSN signaling are duplicated. The Committee recommends that the system architecture be changed to save cost through a new call controller which incorporates survivable signaling implementation.

In summary, the Committee recommends that the NCS proceed with NETS along the lines recommended by this report.

---

1 The Policy Planning Environment for National Security Telecommunications (Annual Report); National Academy Press, Washington, D.C., May 1985.

2 The Policy Planning Environment for National Security Telecommunications (Final Report); National Academy Press, Washington, D.C., July 1986.

II. AN OVERVIEW OF THE NATIONAL EMERGENCY TELECOMMUNICATIONS SERVICE

A. Introduction

This chapter describes the Nationwide Emergency Telecommunications Service (NETS) as defined by the National Communications System (NCS). That definition has been refined further by several groups that briefed the Committee. The Committee recognizes that NETS may be a tariffed or leased service and that final implementation is the responsibility of the service providers. Thus, the implemented NETS may deviate from the Committee's present understanding.

B. Purpose

The purpose of NETS is to provide a highly survivable telecommunications service capable of supporting voice and low-speed (2400 b/s) data communications for up to 20,000 users and up to 3000 Erlangs of traffic, which is specified by the NCS. NETS is a national level program of the National Communications System (NCS). This initiative is for the improvement of national security emergency preparedness (NSEP) telecommunications services to authorized federal, state and local government users in the event of natural or man-made disasters, including nuclear war. It will provide telecommunications service that can be used for voice and such voiceband data services as secure voice, facsimile and low-speed data. The concept has been shaped by National Security Decision Directive 97, Executive Order 12472, the threat environment, and the requirements of the diverse user community.

C. Summary of Requirements

The following list summarizes the NETS requirements:

- Voice, secure voice, facsimile, and 2400b/s data services.
- Survivability during and after a nuclear attack.
- Ubiquitous access and connectivity throughout CONUS.
- Unattended operation until restoration and reconstitution are possible.

- Access and signaling security to prevent unauthorized use or hostile exploitation.

- Priority-service features for selected users when resources are limited.

- Backup, unhardened capacity in support of dedicated, user systems prior to attack.

- Compatibility with existing government and commercial telecommunications systems.

- Maintenance of state of readiness.

- Immediate user access without "third-party" intervention.

- Flexible design, permitting evolutionary expansion and adaptation of new technologies.

In addition to the above, peacetime operations and maintenance require the keeping of call records and billing functions.

D. System Description

The NETS will provide a highly survivable capability for voice and voiceband data communications services by exploiting the surviving switching and transmission facilities of the PSN and, where feasible, private and government networks. The successful use of the PSN for NETS will require flexible and innovative routing of calls through the networks that form the PSN. This is accomplished by adding considerably enhanced routing capabilities at several points distributed throughout the PSN. The added routing capabilities will enable the NETS to route calls using options that do not exist for other calls. The NETS can continue to complete calls through a damaged or congested network by the "probing and routing" functions of its elements. Because the successful routing of NETS calls may require many more links in a damaged network than normal calls, some transmission compensation may be needed. This transmission compensation helps to ensure the usefulness of connections established over diversified and non-standard routes.

In addition to the enhanced routing capability which NETS adds to the PSN, the following functions are also essential:

- Ubiquitous access: enables a user to place a NETS call from any telephone having access to the PSN using the North American Numbering Plan.

- Ease of use: calls on NETS will be made in the same manner as toll calls on the PSN. Voice prompts are provided when needed, and voice responses inform the user of call progress.

- Priority call treatment: provides NETS callers with priority treatment over other PSN traffic by the use of network management techniques within the PSN.

- Access and signaling security: tests the authenticity of calls to allow access to authorized users only and ensures the nondisclosure and integrity of call-related data.

- Precedence and preemption: determines whether a NETS call can preempt another NETS call and enables assigned-user call privileges to be used.

- Preset connection: enables the establishment of route-specific connections to avoid known targets and provide for trans-attack communications.

- Retry: provides the capability to establish a new call through NETS using resources gained through a prior NETS call.

- Restoration and reconstitution: provides the basic communications links for maintenance and repair activities.

The order in which the service performs or uses these functions in setting up a NETS call is shown in Fig. 1. The previous listing of NETS requirements follows this pattern.

The following elements will provide the NETS functions:

- The PSN, which is a network of many networks,

- Call controllers (CCs),

- Access security devices (ASDs),

- Remote user modules (RUMs), and

- the NETS Maintenance and Administration Center (NMAC).

The PSN comprises the Interexchange Carrier (IC) networks and the Bell Operating Company (BOC) and Independent Telephone Company (ITC) Local-Exchange Carrier (LEC) networks. With the benefits and the limitations of using the PSN as an emergency communications medium, NETS is designed so that it will augment current PSN functions with little or no effect on PSN operations and without enormous changes in the present system. The PSN provides the communications connectivity and capabilities on which NETS builds.

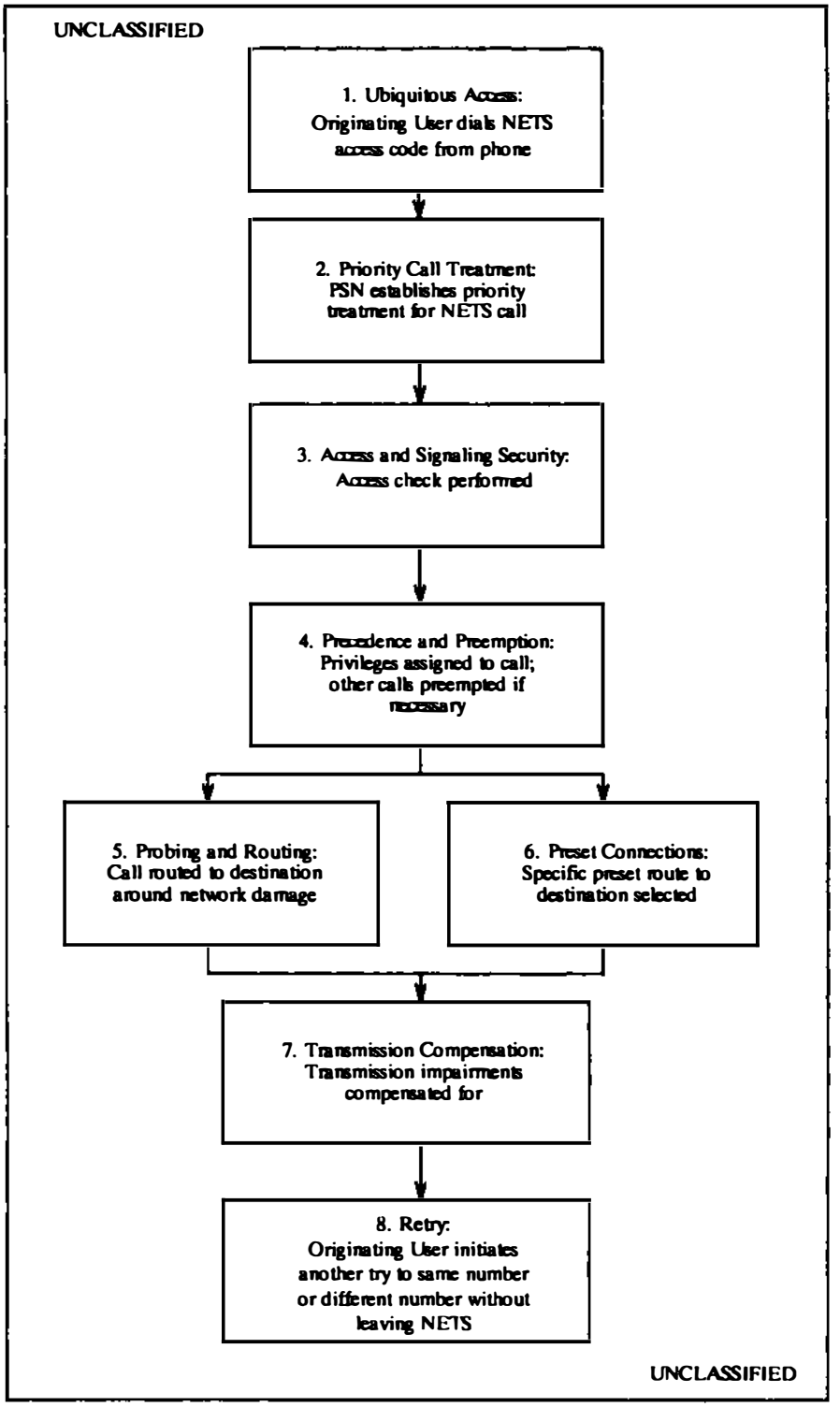

Figure 1: Relationship among Functions

The call controller (CC) adds appropriate NETS functions to a PSN switch. The primary function of the CC is to provide routing capabilities to enable use of connectivity in ways not provided by standard PSN routing. Two particular implementations of the CC functions are the Call Control Module (CCM) and the Switch Internal Module (SIM). The CCM is an electronic device that is external to, but connected to, a host switching system. The SIM is an added group of features, implemented by a combination of hardware and software within a PSN switch, that provides the CC functions. This feature group allows the switch to provide NETS services in addition to its PSN services. Functionally the CCM, with its host switch, is equivalent to the SIM. The term "CC" will refer to either a CCM or a SIM.

The Access Security Device (ASD) and Remote User Module (RUM) are elements that can be used from the NETS user premises. The ASD is a device that couples to a user's telephone electrically or acoustically, employing encrypted identification coding to gain authorized access to NETS and to enter the destination number and indicate user privileges. The RUM is an element that allows transmission compensation to be performed on the connection between the RUM and a CC or another RUM. Such devices would be placed on users' premises, possibly behind a PBX, and some may be incorporated in CC's.

The NETS maintenance and Administration Center is an operations center that assists in providing the logistic support for NETS. This function is not required for processing calls during emergencies.

E. Network Architecture

Figure 2 gives an overview of the NETS architecture of a network of networks and summarizes the relationships among the NETS elements. The figure has as its basis the PSN architecture, consisting of LEC networks interconnected by IC networks. The call is placed from the originating station. Two terminating stations are shown: one with a RUM and one without.

The nodes in the figure represent PSN switching locations and may be PSN switches with or without CC functions added. The figure illustrates typical placements of CCs in the network. Network configurations identifying the specific locations of the CCs and the order of their placement have not yet been decided and remain under study by the government.

RUMs are located at a limited set of selected customer premises. The figure shows one location of the RUM in the local loop [the RUM may also be associated with a customer-premise Private Branch Exchange (PBX)]. ASDs are issued to users and must be used for authorized access to NETS. An ASD can be used with telephones anywhere within the CONUS to authorize access to NETS service.

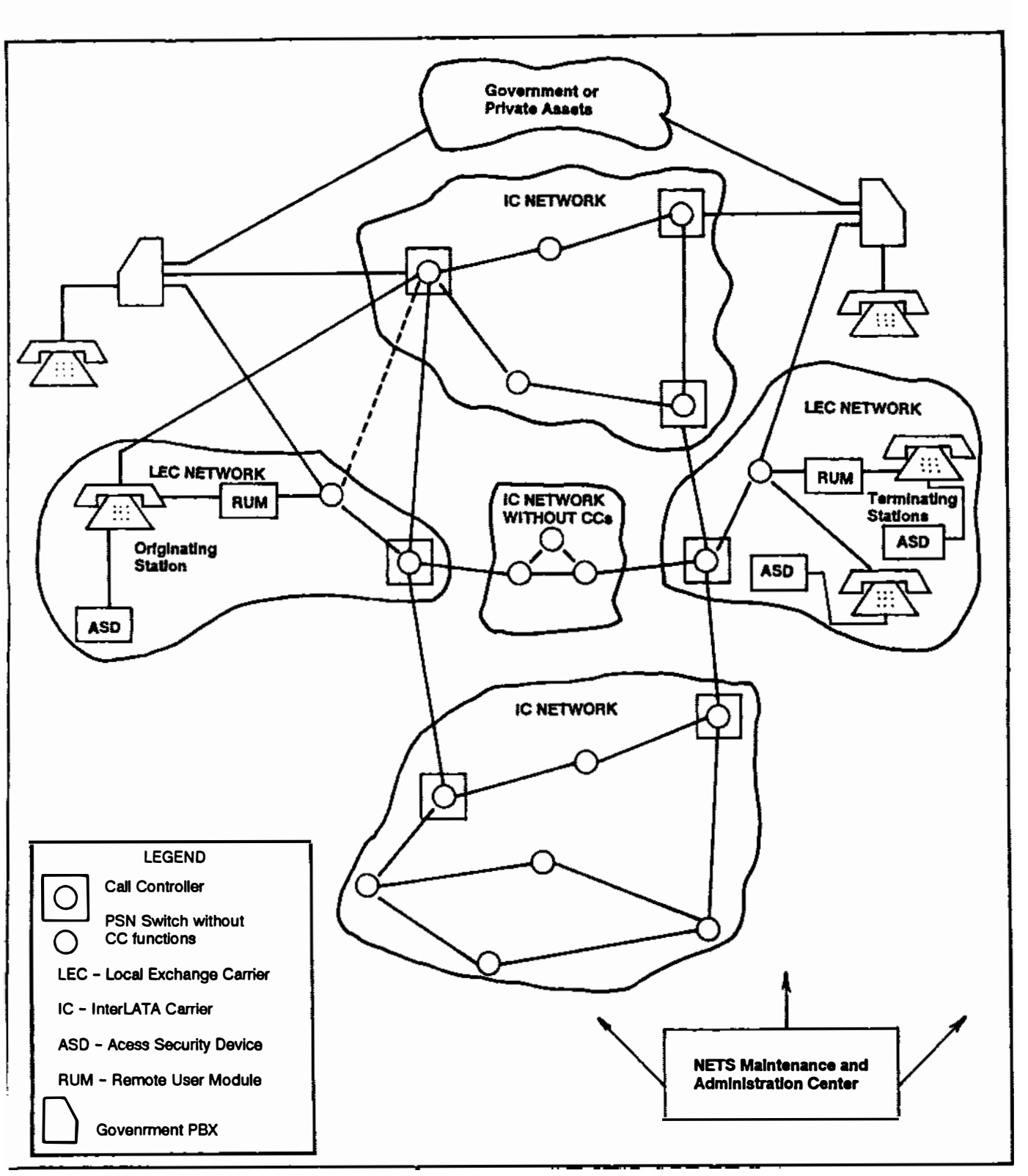

Figure 2: NETS Architectural Overview

F. Call Types

As shown in Table 1 there are four types of NETS calls: standard, preset connection, exercise, and test. The foremost characteristic of a standard call is that the system will search out any available route to complete it. To initiate a standard call, the destination number, which is a regular telephone number, of the terminating user is entered into the ASD and the NETS access code is dialed on the originating station. Using any available route, a standard call is routed to its terminating station by PSN switches and CCs.

Table 1: Purpose of NETS Call Types

UNCLASSIFIED

Call Type	Purpose
Standard	Establish an authorized user's call using any possible route
Preset Connection	Establish an authorized user's call using a predetermined set of CCs to reach a predetermined terminating station
Exercise	Allow users to experience the use of the system under simulated conditions of damage or congestion
Test	Allow testing of the system

UNCLASSIFIED

A preset call is distinguished from a standard call in that the CCs through which the system will route the preset call are predetermined. To initiate a preset call, a preset path number (PPN) is entered into the ASD in place of the destination number, and the NETS access code is dialed by the originating station. The particular CCs through which this call will be routed are predetermined and identified to the system by the PPN.

An exercise call will be routed by the system like a standard or preset call; however, it is subject to simulated network damage. The system will preempt exercise calls, if necessary, to process standard or preset calls. An exercise call is initiated like a standard or preset call, with the ASD being used to identify the call type in the exercise. Identifying the call as an exercise attempt enables the system to route the call like a standard or preset call, but without interfering with the completion of standard or preset calls. Exercise calls are subject to simulated network damage or congestion, which may affect their completion. Their value is that they allow the users to experience the use of NETS without interfering with normal use.

A test call, designed to test portions of NETS connections, will be routed by the system like a standard or preset call. However, the system will preempt test calls, if necessary, to process standard, preset, or exercise calls. A test call is initiated like a standard or preset call, with the ASD being used to identify the call type as a test. A call identified by a CC as a test call will be routed like a standard or preset call. As with the PSN, CC routing of test calls will not interfere with the completion of standard, preset, or exercise calls. Test calls allow testing of portions of the system without affecting the completion of other types of calls.

Figure 3 is illustrative of a regular call that utilizes many of the NETS enhancements of the PSN. The user attaches the ASD and, upon receiving dial tone, places a call to 1-950-0627 using the facilities of the local exchange carrier. The call is routed to the serving call controller, CC1. CC1 issues an encrypted challenge to the originator, which is answered by the originator's ASD. Upon the successful exchange of signals by CC1 and the ASD, the ASD dials the desired station using the standard, 10-digit, North American Numbering Plan. Through its translation tables, CC1 probes network status to determine whether CC2 can be reached through ordinary PSN nodes or whether the call must go through another CC en route, then determines that CC2 is the terminating or via CC for this call. Upon receipt of encrypted signaling information, CC2 determines that CC4 is the next CC in the call. If CC2 determines there are no available routes to CC4, it then seeks alternative routes to CC4 by way of CC3. In this case it is assumed also that there are no available trunks to CC3 because of congestion or outage; therefore CC2 notifies CC1 that it cannot complete the call (this action is called "crankback"). CC1 examines its translation tables for an alternate route and signals toward CC3. CC3 determines that CC4 is the destination, whereupon the call is eventually routed to the intended terminating station. Each sector of the transmission facilities between CCs is compensated for amplitude and delay distortion while the call progresses to the next CC. During these signaling and switching actions of the CCs and the PSN, verbal call progress information is given repeatedly to the user.

The priority service features available to NETS users are invoked only when resources are limited, i.e., when a prioritized calling party cannot gain egress from a CC toward the desired CC. Precedence and preemption rules determine the system treatment of the parties.

G. Observation

Both the NETS requirements and their possible implementations have evolved over time. This chapter has described a particular technical implementation for providing the National Emergency Telecommunications Service. While the Committee has received extensive briefings on this particular approach, the final system implementation to provide NETS service could look somewhat different. Possible directions for such variations are suggested in Chapter IV.

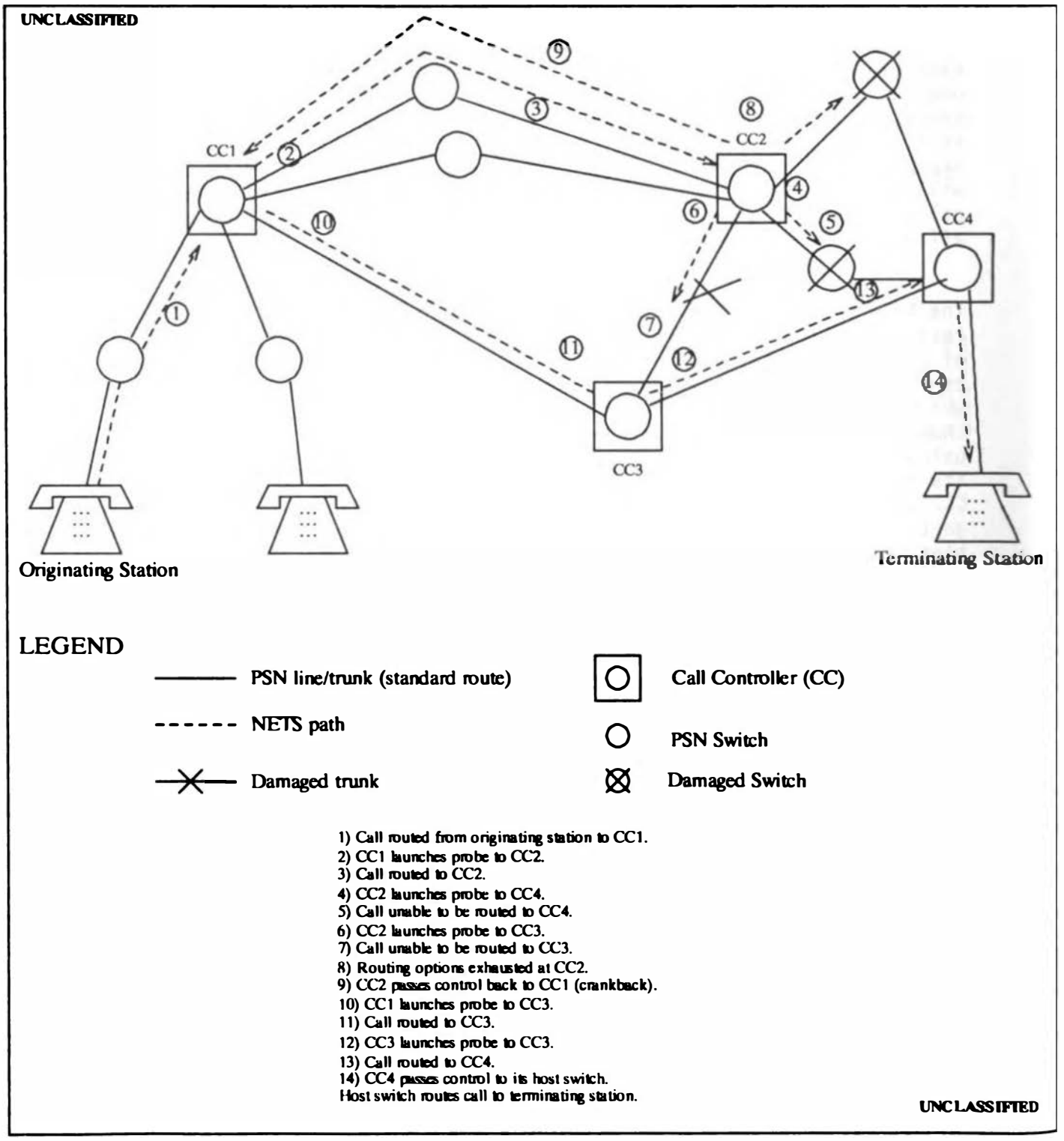

Figure 3: Example Illustrating the Enhanced Probing and Routing Capability of NETS

III. THE PUBLIC SWITCHED NETWORKS

A. Introduction

This chapter describes the public switched networks of the United States and why they are the facilities most likely to provide a framework for the successful implementation of a Nationwide Emergency Telecommunications Service (NETS).

There are several telecommunication networks in the United States. Some serve the public generally, while others are considered private, although they often lease facilities that are owned by those providing public service. Private networks have generally developed for specific services and are limited in their capabilities, e.g., one-way transmission. Networks of broadcast stations and cable TV networks are of this type. Some networks are used for specific services, e.g., packet data networks. Radio amateurs form a network that is capable of two-way telecommunications but amateur radio channels are not generally used to establish selective communication between specific individuals or organizations on a demand basis other than amateur packet radio. There are now about 20,000 packet radio repeaters generally exchanging text files at 1200 bits/second on a user to user basis.

The public telephone system of the United States is unique in that it provides selective, two-way telecommunications for voice as its primary service objective. This service is not provided by a single supplier using a single network but by a cohesive set of networks with well defined standard interfaces. There is a national numbering or station-addressing plan that makes it possible to identify the points of both service origination and termination. It continues to grow in a pattern that ultimately is intended to afford users universal access to services offered by network-based and non-network service providers.

This service is made possible by two basic factors: the universal North American Numbering Plan for addressing all telephone stations and terminals and by the interconnection of many local and long-distance

networks. By this addressing plan and interconnection, a national asset has been formed that makes possible ubiquitous telephone and other telecommunication services.

Networks are formed from physical facilities. While the operators of some of these networks compete to carry the traffic offered by the public, they all utilize the same nationwide addressing or numbering plan. This network of networks has become known as the "public switched network (PSN)."

B. Dimensions

The PSN[1] represents an investment of about 250 billion dollars. It has been designed with the objective of rendering ubiquitous service throughout the country. The public telephone network is accessible through more than 19,000 telecommunication centers. Reaching most business, industrial, and government locations, more than 90% of the homes, coin telephones, and emergency roadside telephones, fully interconnected and used by all facets of the population, is what makes it public.[2] The functional technology of the network that enables each user to select a called point from among 150 million addresses in the North American Numbering Plan is known as "switching."

Because of this great, addressable connectivity or ubiquitousness, the network is called the public switched network. Most think of the network from the standpoint of its essential transmission quality-- the ability to convey intelligence over long distances by a combination of terrestrial, multi-pair, copper, coaxial, and optical-fiber cables, (relay) microwave radio, and through space using communication satellites.

---

[1]While the essential public network evolved on the basis of providing telephone services, most organizations that have offered only voice telecommunications in the past are now looking forward within the next few years to providing variable telecommunications bandwidth that can be used for any desired telecommunication by the users, encompassing data, voice, facsimile, video, or full motion pictures.

[2]The fact that the network is for the public is indicated by its availability for "common carriage," i.e., the content-insensitive offering of communications services for hire, its regulation by political entities, the use of public franchises for its use of public streets and rights-of-way, and the offering of public services with coin and other public telephone stations.

C. What is the PSN?

For the purposes of public telecommunication, the United States is divided into approximately 18,000 geographical divisions known for purposes of regulation and tariffing as "exchanges." Only one company provides public telephone service to users within an exchange. This company is known as the local-exchange carrier (LEC). It operates equipment in one or more buildings, called end offices, within the exchange and has franchises from the cities and towns where it operates to provide the service, including the placement of outside plant in the form of conduits, poles, cables, crossconnect boxes, etc. There are approximately 1450 LECs in the United States.

The end office contains the equipment needed to render the services. It includes power equipment and standby generator with fuel storage, vaults where cables terminate, switching equipment, transmission terminal equipment and security to control personnel access. Depending upon the number of terminals or stations served by the exchange there may be more than one switch in the end office. Furthermore, each switch may serve more than one end- or central-office code(s) used to identify and address stations. These end- or central-codes are known as NNX codes, where N stands for the digits 2 to 9 and X for the digit values 0 to 9. There are approximately 20,000 NNX codes in use in all areas. These codes are assigned to some 19,000 local-office switches, some of which serve more than one NNX. It is from these local or end-office switches that most users obtain dial tone when placing calls.

Bell Operating Company (BOC) and General Telephone operating companies (GTOC) exchanges of dominant LECs are grouped into local access and transport areas (LATAs). With some exceptions, LECs provide all interexchange services within the LATAs and interexchange carriers (ICs) provide services between LATAs. Some interexchange carriers, as well as international carriers, provide service between the United States and other countries. There are also companies that obtain lines from LECs and ICs to resell interexchange service.

There is a small number of ICs and resellers that own and operate their own switching and transmission equipment. Independent telephone companies, those not affiliated with Regional Bell Operating Companies (RBOCs), operate their own exchanges and offer interexchange service by connecting with ICs either directly or through Bell or GTE LECs. There are 183 LATAs in the United States. Most are within state boundaries but there are a few that extend over contiguous state boundaries.

Each interexchange carrier or reseller offering interLATA service has been assigned a three-digit carrier identification code of the form XXX. The code is used to reach a specific IC from a station-connected local office. More than 400 of these codes have been assigned, although only a few are well known and publicized, such as 222 for MCI, 288 for ATT, and 777 for U.S. Sprint.

The technologies in the switching offices of the United States PSN are varied, using many forms of electromechanical and electronic switching. However, 73% of the lines are now served by electronic switching, most of it using the technique of stored program control (SPC). Most IC switching is of the SPC type. Since 1986 all local SPC offices of the Bell Operating Companies and GTE of greater than 10,000 lines have been arranged for giving subscribers "equal access" to all ICs. The process of providing equal access from other companies' local switching offices is continuing. All subscribers associated with these offices have been required to choose a preferred IC to carry their interLATA traffic.

To reach a specific IC without presubscription the XXX carrier code is used. From non-equal-access offices, 950-0XXX or 950-1XXX, depending on the carrier, is dialed. The number 950-0627 has been assigned as an address for local offices to recognize NETS calls. (For equal-access local offices, prefixes of the form 1XXX are used to reach non-presubscription ICs.) The local and access tandem switches use these numbers to direct the call to the nearest known call controller. The ICs connect with local stations of the LEC over facilities they provide or lease that reach the transmission meeting points, known as "points of presence (POP)" within each LATA. The LECs provide facilities to reach each of the POPs and operate approximately 350 access tandem (AT) switching offices that, among other functions, gather and distribute traffic to and from ICs. Most access tandems are of the SPC type. The ICs operate approximately 300 of their own switches, which have been loosely called "toll" switches since they are provided for long-distance, or toll, service.

The North American Numbering Plan includes three-digit area codes currently of the form NOX or N1X (NO/1X). Calls between stations with different area codes are in most cases served by ICs. Prefixes to called station addresses, 0, 1, 01, 00, 011, as well as certain area codes such as 800, are used to distinguish services. Codes starting with 1, such as 1NX, are used within networks to designate special system action. These codes are not recognized by local-office switches if dialed by the public. Some of these codes are used by NETS to access special routing tables within host toll switches.

Calls within LATAs are routed over direct trunks connecting local switches or through access tandems. Most ICs have trunks to and from access tandems. Where there is heavy traffic there may be trunks from local offices directly to specific ICs. Between LATAs, each IC has its own arrangement for bringing calls to its switches. Those with only a few switches favor the use of long transmission facilities such as fiber-optic routes for carrying calls from the points of presence to the small number of switches. AT&T has switches in almost all LATAs. On the average each call sent to an IC passes through slightly more than two switches. AT&T has reduced its former four-level hierarchical network to one of two levels with a new form of routing, known as "dynamic non-hierarchical routing (DNHR)." In this network there is a maximum of 16 alternate routes between any two switches. There is no

set minimum: local minima are set by the designers in response to economic and traffic constraints on the network.

Besides using the routing in long-distance networks in the usual manner, NETS CCs would include routing tables that would probe routes not normally taken in establishing commercial calls between a particular pair of switching nodes. To aid in this process, 1NX codes would be dialed by the CCs and the receiving toll switching offices would respond by using special routing tables to select trunk groups in attempting to complete NETS calls.

The glue that binds the network and its address plan together is the signaling that is used between the calling station and its associated local office and between offices over the entire country. Signaling provides for the transfer of information about the call between switching nodes, including such items as call origination or trunk seizures, called address (XO/1X-NNX-XXXX), where necessary the calling address, and answer and disconnect indications. For many years this signaling took place over the same paths used to transmit the speech (sometimes known as "in-band" or "in-slot" signaling). Since 1976 the trend in signaling in long-distance networks has been away from this use of the speech paths to the use of separate data channels for signaling messages. This form of signaling is known as "Common Channel Signaling(CCS)." The switching nodes for the signaling network are known as signal transfer points (STPs). AT&T has implemented this form of signaling in its network and is currently using it to serve over 90% of its calls. Other ICs are expected to employ this technique within the next few years.

For signaling purposes the AT&T network divides the United States into seven regions. There is one pair of STPs in each region to serve all calls that originate, terminate, or pass through switching offices in the region. To ensure service reliability, considerable redundancy is built into the CCS network. Each STP of the pair is located in a different city and is reached over data links that take diverse routes. Each STP includes redundant processors. Within the next few years, when all AT&T calls are served using CCS, fourteen STPs throughout the nation will handle the signaling message for the entire AT&T network. Although this is efficient and economical from the carrier's point of view, the network has greater vulnerability to enemy attack than would be the case if the switching control were distributed over a larger complex of (smaller) switches.

The CCS networks of other ICs also provide redundancy to ensure service continuity. Being smaller, they have fewer STPs but longer, more vulnerable data links. The major LEC operating companies are planning to use CCS. Currently announced plans contemplate the use of this form of signaling only for special services, such as for 800-number and credit-card calling. It might also be used for signaling between LECs and ICs. However, most calls within LATAs are

not likely to depend upon CCS for successful call completion in the near term.

For most of the new and special services, data bases are added to the CCS networks, usually at some STP locations. In its present form the NETS calling does not depend for its operation upon the availability of these data bases.

Besides the stations that are connected directly to local, central offices, there are stations connected to switching nodes for communication within premises, such as in businesses, schools, industrial, and governmental locations. These switching nodes are generally known as private branch exchanges (PBXs). It is estimated that there are about 30 million stations served by PBXs. Stations served by private switching nodes need not be part of the national numbering plan, in which case they are not part of a PSN. These switches and their associated transmission facilities form the many private networks in the United States. Usually stations on private networks also have access to trunks that terminate on local PSN switches. As a result the stations may place and receive calls from the PSNs as well as within the private network. Those with private network facilities may lease their use to provide telecommunication services to others. The Federal Telecommunication Service 2000 (FTS-2000),currently up for bid, is an example of a service that may utilize private facilities. As such, it may not be part of the PSN and therefore not be considered as a contender for the NETS. However, as with other private networks, many stations served by FTS-2000 will be able to place and receive PSN calls and therefore will not be excluded from the NETS.

Also part of the PSNs are cellular mobile and Airfone services. When they utilize addresses in the North American Numbering Plan, they may be considered as access or terminating points for NETS calls.

D. Vulnerability of the PSN

Since the PSN serves population centers it is most vulnerable to countervalue attacks aimed at these centers. The Committee examined the effect of various attack scenarios on the PSN. The heavier the attack, the greater the loss of facilities and the more "islands" are formed from the damaged PSN.

The Committee also examined the effects of nuclear fallout and electromagnetic pulse (EMP) on the PSN. As indicated in footnote 1, next page, tests of specific terrestrial telecommunications equipment have shown that where facilities survive destructive hits, the EMP and other environmental effects are only temporary. Carrier systems, buried optical-fiber cables, and switching systems may be expected to continue or resume operation within a short time after an attack. They should be able to provide service until exhaustion of fuel or the

normal attrition of components causes the failure of primary and redundant system elements.[1]

The ubiquity of the long-distance networks of the PSN is highly dependent upon the survivability of the AT&T network. Currently, many ICs use the AT&T network to reach points where they do not yet have their own facilities. With the dependence of the AT&T network upon CCS, the survivability of the CCS network is vital for the successful operation of NETS in the post-attack period. Thus the NETS implementation must include supplementing the AT&T STP-CCS signaling network, since these nodes and data channels may be destroyed or become inaccessible under accurately planned attack. Alternatives proposed by AT&T include provision of a form of CCS associated with interswitch or trunk routes. The data channels for this associated method of CCS have been given various names, the most studied being known as "S-links" (See Chapter IV).

E. Survivability of the PSN

The PSN serves all of the United States population in their residences, their businesses and industries, and local, state and federal governments. Even where private networks are used for service, the facilities for these networks are usually derived by using segments of the PSN. Excluding the PSN from a role in the post-attack period would imply rewiring the country.

---

[1]During its examination of the overall survivability of NETS, the Committee raised the following question: will the influence of the electromagnetic pulse (EMP) radiated by high-altitude (> 100 km or so), high-yield, nuclear detonations be a serious problem in the proper implementation of NETS and its operational performance? To update and to understand this issue better, the Committee received a briefing by the NCS on recent NCS field testing of major components of the public switched network (PSN), using EMP simulators. These components include the AT&T 5ESS™ switch, the FT3C Multi-Mode Optical Fiber Communication System, and the T1 System including the D4 Channel Bank. In addition, future tests are planned for the AT&T 4ESS™ and the Northern Telecom DMS-100 switches. The results of tests to date have indicated that although there were some minor transient upsets experienced,there were no major system failures (burnout). While certain unexplained effects have been uncovered in special situations, none of the problems is beyond reasonable technical and economic resolution. The Committee has found the NCS program for EMP vulnerability assessment and mitigation to be well conceived and conducted. Further work on 4ESS and DMS-100 switch testing and assessment is recommended, since EMP has been quite controversial and more hard evidence will be useful. The EMP test results on components of the PSN have confirmed quite well the major results expected and discussed in previous NRC committee reports to the NCS.

No matter what type of attack the nation sustains, islands of the PSN will survive. It is the NETS objective to permit calling within and between these surviving islands. Stated inversely, some PSN facilities would survive, even after massive nuclear attack.

All ICs are planning or employing common channel signaling. Since the number of nodes in the signaling networks is small, this portion of the public switched network is particularly vulnerable. Proposals have been made to circumvent the common channel signaling in the AT&T network in the event of an attack. These proposals might be costly to implement and maintain.

The regional Bell holding companies are all planning common channel signaling for special types of calls such as 800 and credit-card. However, there are no current plans for general use of common channel signaling for plain old telephone service (POTS). Introduction of new access methodologies such as ISDN are causing the RBOCs to restudy this position.

Survivability studies have shown that improvements can be made in extending islands of service in the post-attack period by appropriately augmenting the public network. These facilities would be in addition to those normally required by the PSNs. While costly to install and maintain, these augmentations to the public networks could increase the size of the post-attack service islands.

Augmentation would also be useful in establishing bridges between public networks, particularly between ICs, where competition generally precludes such considerations. Separate NCS programs such as Commercial Satellite Interconnectivity (CSI) and Commercial Network Survivability (CNS) are directed to providing for these limited needs in the post-attack environment.

To utilize the surviving portions of the public networks requires access through stations. These stations connect directly to more than 19,000 local switching offices of the Bell and Independent operating companies, or behind PBXs that reach the local offices over trunks. These trunks are generally in the same cables as subscriber lines, even when many are gradually being converted to use the newer digital technology.

The access through the local office to an access tandem or other switch is used to reach the ICs for long-distance calling (NETS is directed primarily at long-distance service. Local service may well be served by other forms of communications). Congestion in the local switches may impede and delay, but not necessarily prevent, calls placed in local offices congested by a post-attack surge in network traffic from reaching trunks to the location of an originating CC. These CCs are most likely to be associated with an access tandem.

The first step in processing a call attempt through a local office is to provide dial tone. This indicates that the office is ready to accept the call. Different arrangements exist in the local switches to allocate dial tone to lines in times of severe overload. The algorithms or design strategies used are complex. Several different strategies exist in the variety of switching systems that exist in the local offices in service today. Limited-length queues or buffers are established with different disciplines. The most-used examples are the "first in first out" (FIFO) and "last in first out" (LIFO) buffers.

For NETS calls to avoid being placed into these queues they need only be identified by originating line. However, in some state jurisdictions prioritizing of lines or calls is currently illegal. Furthermore, many NETS users are behind government PBXs. Therefore, and to avoid inefficiencies associated with setting up separate, small, preferential trunk groups within PBXs, all trunks from these PBXs, whether or not they were being used for NETS calls, would receive preferred treatment.

It may not be known from where NETS calls will originate, and thus it would be difficult to establish a priority for lines from which such calls may originate. Tying NETS callers to prioritized lines, even if permitted, would greatly reduce flexibility in the use of ASDs.

It is difficult to implement special priority for NETS calls in local offices. However, the Committee was assured that persistence in remaining off-hook for dial tone will eventually succeed, i.e., these call attempts would be processed for trunk selection to an access tandem.

NETS calls are distinguished in local offices by the number dialed. To ensure that the calls, once dialed, reach an access tandem where a CC is likely to be located, some provision is needed in NETS to ensure availability of idle trunks between local and access tandem offices in times of congestion. This will require some modification of the trunking arrangements between local and tandem offices. These modifications would consist of dividing the tandem trunk groups and providing a trunk subgroup for NETS calls. This division of the trunk groups could be used routinely with provision for confining the trunk subgroup to NETS calls being initiated pre-attack.

Fragmentation of the PSN into islands of service may pose a problem in synchronization of transmission and switching facilities. Synchronization is critical in minimizing errors introduced into networks' multiplex transmission systems. Today the national networks are synchronized from centralized, highly stable, single-frequency sources: a Cesium clock with a stability of 1 part per (pp) 10^{12}/day, used as reference for 30 master frequency supplies in the AT&T long-distance network with free-running stability of better than 1 pp 10^{7} day. Each frequency supply mimics the next higher level supply stability when referenced to it. The worst free-running tolerances in end- or

central-office switches will allow islands of the system to run satisfactorily for at least six months. Even in an extreme situation of as many as 268 frame slips/hour a frame slip will appear only as a "pop" in transmission and will not require resynchronization. In actual operation switches may well experience failures other than synchronization that will require maintenance attention weekly or even daily, and crews will also check synchronization drifts under routine maintenance procedures. If, as recommended by the predecessor committee's reports, simple, standard procedures are posted prominently at every switching office, it appears to the Committee that synchronization is not a problem insofar as NETS is concerned. It may well, however, require attention in NSEP situations beyond NETS. The Committee will address that question in its subsequent report, on synchronization and switching in NSEP telecommunications.

F. Endurability of the PSNs

An advantage of NETS, using the PSN, is that NETS may be tested and maintained as part of the regular networks' routines. The use of the public networks has other built-in advantages. As these networks grow and change, the implementation of NETS service will also be revised, particularly to take advantage of improvements in technology. The industry is very volatile and many technological and service improvements are foreseen for the future. Terms representing these improvements are "fiber optics," "DACS," "ISDN," "broadband switching," etc., and are found regularly in the trade press and represent future investments in the PSN. With the deployment of NETS as a regular part of the public network services, NETS would automatically be considered as a regular part of PSN growth and rearrangements.

In particular, the emergence of the integrated services digital network (ISDN) capability has been much discussed. ISDN will provide end-to-end digital transmission and permit telephone lines to be used for voice, data and other services that take advantage of this transmission. While this might also extend to NETS calls once established, it does not provide for the routing necessary for the initial establishment of NETS calls. Furthermore, the provision of ISDN on a nationwide basis anticipates the use of common channel signaling, one of the major elements in the PSN requiring augmentation to survive for NETS use.

Specifically, regulatory requirements and decisions for equal access, Comparably Efficient Interconnection (CEI), and Open Network Architecture (ONA) have influenced and will continue to influence the design and use of the PSN. These concepts have been and are being considered for introduction into the PSNs to achieve competitive parity between network-based and non-network service providers. The impact of these decisions on services offered by the PSN, such as ISDN and other so-called intelligent network services, is uncertain. NETS should not

depend upon these considerations. However, to the extent that regulation may skew network topology, the NCS should be alert to the possible need for obtaining waivers of rules that might impede deployment of network assets necessary to meeting NETS requirements.

G. Summary of Concerns About the Use of the PSN

The committee has eight principal concerns about the use of the PSN for NETS.

- Switching offices throughout the PSN will have to be modified for the proper routing of NETS calls.

- Augmentation of the transmission facilities of the PSN should be implemented to improve post-attack connectivity.

- Signaling in the PSN is increasingly dependent upon common channel signaling which, while efficient and economical for the carriers, makes PSN services more difficult to provide should these signaling facilities be disrupted.

- Post-attack, there is likely to be heavy demand and associated congestion in local offices and intraLATA networks in general. This would make it difficult to place a NETS call to an originating CC. Without access to the first or originating CC, NETS would be ineffective. Users generate requests for service. If the associated switching system can serve the call the system allocates facilities and indicates this by returning dial tone. Algorithms or strategies designed into electronic switching systems decide the order in which lines originating these call attempts will be served. There are several algorithms in use in different, modern, switching systems and these are still being modified. After examining these different strategies the Committee concluded that by waiting, even in periods of severe overload, originating NETS calls will eventually be able to receive dial tone and place their calls to NETS; however, priority should be given to those lines known to originate NETS calls.

- During periods of heavy congestion, the availability of trunks to and from the access tandems is also critical to NETS operation. Therefore, the Committee recommends that the trunk groups to and from access tandems be engineered and provisioned in the pre-attack period so that NETS calls will be assured access to an adequate number of these trunks. Provision should also be made to reject non-ASD-originated calls using these trunks and quickly restoring the trunks for NETS use.

- Almost all carriers provide for their own emergency power for a limited time period should commercial power supply be

interrupted. For the long term after an attack it will be necessary to ensure the continuity of power to operate the surviving telecommunication facilities. This has been noted in previous reports on NSEP telecommunications[1,2,3].

- There is a need to ensure the availability of continuing support for NETS in the form of trained maintenance personnel and availability of spare parts.

- To survive a nuclear attack, new equipment placed in the telecommunication infrastructure must continue to be resistant to fallout and electromagnetic impulse (EMP).

After due consideration by the Committee, the following table summarizes where, in its judgment, further action is required on these items.

Disposition of Committee's Concerns with PSNs

Areas of Concern	Further Action Required	
	within NETS	beyond NETS
Switching	X	
Transmission Connectivity	X	
Signaling	X	
Synchronization		X
Congestion	X	X
Availability of Power		X
Maintenance of PSNs	X	X
Nuclear Weapons Effects		X

---

[1] Telecommunications Initiatives Toward National Security and Emergency Preparedness (Final Report); National Academy Press, Washington, D.C., March, 1984.

[2] The Policy Planning Environment for National Security Telecommunications (Final Report); National Academy Press, Washington, D.C., July 1986.

[3] The Policy Planning Environment for National Security Telecommunications (Annual Report); National Academy Press, Washington, D.C., May 1985.

H. CONCLUSIONS

The public switched network (PSN), a network of networks in the United States, and possibly Canada, provides the most generally available form of telecommunication facilities that could be used in a post-attack period. The PSN provides ubiquitous availability, with a known address or numbering plan. It is expected that some parts of its vast component networks will survive. The parts that do survive could be used as islands of communication and eventually these islands could be reconnected as restoration of critical paths proceeds. Some of these critical paths could be implemented pre-attack as augmentations to the networks. Other arrangements are also needed in the plans for use of the PSN to ensure signaling and access despite local-area congestion.

IV. VARIOUS MEANS OF PROVIDING THE NATIONAL EMERGENCY TELECOMMUNICATIONS SERVICE

A. Introduction

There is a number of alternative ways to meet NETS requirements, including special dedicated systems and overlays to existing systems. In order to evaluate alternative implementations, the Committee established the following guidelines and evaluation criteria:

- Survivability of the voice capability must be independent of specific targeting scenarios;
- The system must be cost-effective to be fundable and to prevent elimination from future Government budgets;
- Access to the system must be ubiquitous and simple;
- The system should allow rapid restoration after attack; and
- Use during an emergency should be restricted.

With the above evaluation criteria, several potential NETS alternatives can be dismissed. Specifically, the needs for affordability, scenario independence, and ubiquitous access prevent dedicated systems from being feasible NETS alternatives. Such systems would be prohibitively expensive to develop and operate if they are to survive even moderate threat levels that might target portions of the network.

As discussed in Chapter III, the PSN is undergoing significant changes. NETS can, however, be made flexible enough to accommodate PSN enhancements as they become available. The Committee is confident that whatever precise form these enhancements take, they will not make NETS obsolete.

The Committee evaluated other possible methods of providing National Emergency Telecommunications Service and for a variety of reasons found them unsatisfactory compared to the PSN. None possessed the ubiquity, diversity, redundancy, survivability and robustness that

are all PSN characteristics. Indeed, they all in one form or another either rely on the PSN for their interconnections or simply cannot match its utility. To be effective in a post-attack environment, cellular systems have to access some vestige of the PSN. Mobile radio is very localized and generally has only limited PSN access. Satellites could be fairly ubiquitous if significantly more earth stations were available, but they are not. The wide coverage of the down-link footprint of some satellites could be considered ubiquitous, but internetting/interconnecting of satellite systems depend on the PSN. The Integrated Services Digital Network (ISDN) is a concept which carries message and destination information but relies totally on the PSN to carry its data. The envisioned ISDN service cannot find routes, nor can it reroute or crank back to complete message transmissions. FTS-2000 is also virtually dependent upon the PSN because it is a dedicated network possessing access points into the PSN. None of these has the number nor range of characteristics to challenge that of the PSN.

It is the opinion of the Committee that use and augmentation of the Public Switched Network (PSN) provides the most viable and, indeed, the only realistic alternative for meeting NETS requirements. Given this conclusion, it is necessary to examine means of using the PSN for basic connectivity in the post-attack environment, implementation alternatives and phasing approaches, and the minimum elements required to ensure a survivable PSN capability for NETS.

B. NETS Requirements

Briefly stated, NETS must handle clear and secure voice, facsimile, and low-speed data. It must prevent unauthorized access and hostile intelligence exploitation. It must be available immediately when needed, without the intervention of some central authority. And it must survive a range of attacks and targeting scenarios that may inflict serious damage to the basic transmission or switching systems of the PSN.

Specific NETS requirements are discussed in Chapter II. The key requirements that impose constraints on the NETS implementation are summarized below. The proposed NETS implementation may be viewed as an "existence proof" that a viable NETS system can be assembled from elements of the PSN along with the special procedures, devices, hardware, and software that allow the requirements to be met. Major NETS requirements that constrain the system are:

- NETS is to provide a highly survivable system for unencrypted voice, secure voice, facsimile, and up to 2,400 bps data;

- NETS must be survivable during and after a nuclear attack and must provide a base for reconstitution of the PSN after attack;

- NETS must allow unattended operations until communications restoration and reconstitution are possible;

- NETS must have nationwide access, egress, coverage, and connectivity throughout the CONUS;

- NETS' security measures must prevent unauthorized access and hostile exploitation of NETS-related traffic and user information;

- NETS must provide priority-service features for selected users when resources are limited;

- NETS must accommodate backup and unhardened capacity where desired in support of dedicated special-user systems prior to attack, and be interoperable with existing Government and commercial telecommunications systems;

- NETS must maintain a state of readiness and provide immediate user access without third-party intervention; and

- NETS must have a flexible design that allows for evolutionary expansion and the addition of new technologies.

In conjunction with NCS contractors, the staff of the NCS analyzed a variety of architectural approaches to arrive at a NETS architecture containing several elements: access devices, encryption, call controllers, enhancements to the PSN, and special-access codes for NETS calls. These elements are used in a novel manner to meet the NETS requirements. The salient characteristics of the NETS implementation are summarized below and key issues associated with these characteristics are discussed in subsequent subsections.

- Use of the public switched (telephone) network (PSN) to provide ubiquitous access and egress and the greatest degree of potential survivability. The Committee concurs with this selection.

- Use of devices called Call Controller Modules (CCMs) or Switch Internal Modules (SIMs) installed in telephone-company electronic switches to find longer paths through the PSN when shorter ones have not survived. The Committee believes that the NCS approach is viable but that improvements in conjunction with ensuring that PSN signaling will survive will be necessary.

- Encrypted signalling between the user and CC, requiring access through ASDs which are provided in the pre-attack world to specific individuals or stored at specific locations. The Committee believes alternatives discussed below are possible.

- Improvement of the voice signal through transmission compensation to allow for very poor, unusually long paths in the PSN which may be the only surviving routes after an attack. The Committee believes that transmission compensation in extreme situations is needed but in many cases a simple implementation might suffice.

- Encrypted signaling between CCs during normal operation to protect against unauthorized intelligence-gathering and exploitation. The Committee feels that the system should be expected to operate in the clear after an attack and believes that such an approach is feasible.

- Enhanced PSN routing of voice calls by augmenting the switch routing tables and routing procedures of the participating long-distance telephone carrier(s) to find routes in the degraded environment of a post-attack PSN. The Committee concurs with the proposed approaches, i.e., CCMs, SIMs, S-links and RUMs.

- Priority treatment of NETS calls in the PSN via special area codes or class marks, to recognize NETS calls and to supply priority treatment for special users when surviving switching and transmission capacity is limited. The Committee believes that reliable NETS access at the local and regional levels will require further analysis and Government action.

- PSN augmentation, including potential connections between alternative long-distance suppliers in selected areas of the CONUS to increase redundancy and alternate routing opportunities. The Committee believes that the approaches suggested are viable.

C. NETS Implementation Issues

Because the Committee believes that using the PSN is the only viable approach, it is necessary to examine two related questions to evaluate the proposed NETS implementation:

- Is the proposed NETS implementation sufficient to guarantee that the requirements will be met?

- Are there better ways to use the PSN than those currently proposed?

D. Survivable Signaling on S-Links

The PSN approach seems clearly the best possible NETS alternative, presuming that the PSN continues to operate after an attack that might damage a significant portion of the system, albeit in a degraded mode. Since the dominant portion of the PSN is represented by the facilities of AT&T, it is essential to examine the survivability of the AT&T network. The signaling for call addressing and supervision for this network employs common channel signaling (CCS). The toll networks of the other long-distance carriers and regional, local-exchange carriers are also expected to use CCS but to a lesser extent.

For the AT&T network, the United States is divided into seven signaling regions. Two signal transfer points (STPs) in each region are located in two cities, usually about 100 miles apart. The address

and supervisory signals pass through these for all toll calls within and between regions. These 14 STPs are significant points of vulnerability, whose loss would prevent any communication through AT&T facilities unless provision is made for a more survivable, backup signaling scheme.

To this end, an alternative signaling system to be developed specifically for NETS has been proposed. This alternative arrangement is known as "S-link" signaling. This approach would use from 350 to 600 dedicated data links (called S-links) tied together by microprocessor-based packet switches connected to each of the 104 No. 4ESSs™ that form the basic switching capability of the AT&T network. Depending upon location, some offices would act as signal transfer points and pass signals from one S-link to another. The S-links would use analog data transmission at 4800 bps, a well-known and tested transmission technique.

The microprocessor packet switches and the dedicated data links would constitute an alternative, packet-switched, NETS signaling system which would back up the normal CCS systems. The S-link packet system described to the Committee is a state-of-the-art, engineering-practice system which would be adaptable and robust. The robustness sought derives from the basic character of packet-switched routing, which supports the more sophisticated, enhanced (e.g., "crankback") routing schemes proposed for the PSN. The survivability characteristic stems from the density of the packet-switched signaling network in terms of the number of links connected to each node. With 550 S-links, the emergency signaling system would be expected to complete 95% of the NETS calls without blocking because of lack of signaling capacity.

The S-link approach appears to be a feasible means of providing a survivable signaling system. However, the Committee was not able to determine in the time available how effective or economical this approach is, nor whether more effective or less costly alternatives might be developed and deployed. It is the strong belief of the Committee that a survivable signaling system is essential and that NETS should not be implemented without one.

E. Transmission Compensation

The heart of the proposed NETS concept is the use of CCMs and SIMs, which incorporate special routing techniques in conjunction with augmentation of the PSN to find paths among its surviving transmission and switching elements. The designers of NETS must provide for the situation where the only usable paths in the PSN after an attack will be especially long (say ten or more intermediate points) compared to the normal two or three intermediate points in an undamaged PSN. These exceptionally long paths can be expected to offer significant signal degradation.

The need to accommodate secure voice and/or low-speed data will require some form of transmission compensation to operate in a degraded environment. Compensation would be required between the end user and the CC and between CCs in order to pass the data in intelligible form. The Committee views the secure voice and data requirements as primarily pre-attack requirements, necessary for the system to be used in a routine fashion for maintaining user training and for testing and exercising NETS in order to meet the requirements that NETS be ready immediately when needed. The use of call compensation increases the cost of the system for a primarily pre-attack requirement.

The Committee suggests that the ability to use NETS for clear voice after attack is its single, most essential requirement. Since the PSN will be operating in its normal mode during the pre-attack period, long transmission paths need not be encountered. Therefore, data and encrypted voice should be readily accommodated without call compensation and simplification of the system appears possible.

F. Ubiquitous Access, Protection and Flexibility

Two special aspects of the NETS architecture are aimed at protecting the system against unauthorized use and hostile intelligence exploitation: access to the system requires use of a special device, the ASD; and signaling between the CCMs is encrypted. The combination of the two approaches appears to provide ample protection.

In the post-attack period many individuals not previously identified will need access to NETS to aid in the reconstitution and recovery period. Therefore, NETS will be required to handle a potentially large but undefinable recovery need. The NCS is currently planning to meet this potential need by storing ASDs at government field sites and other key locations. It is not clear that this approach is sufficient to meet the currently unknown future requirement because the field sites may not be there or access to them may be blocked post-attack. This argument would suggest that access should not be restricted to users with ASDs, but that a backup system, possibly involving personal identification numbers (PINs), should also be available. Further, the access protection requirement can be satisfied with either an ASD or a PIN approach. If PINs are used instead of ASDs, there will be a greater risk (and expense) of unauthorized calls in the pre-attack period. However, the lower cost of implementation and deployment might compensate for the added expense, and the use of PINs in lieu of ASDs will facilitate post-attack access for NETS users.

G. Access and Priority

The briefings and analyses presented to the Committee suggest that mechanisms for using and adapting the long-distance carrier elements of NETS are reasonably well understood. The proposed changes to PSN routing, such as the incorporation of otherwise unattractive,non-

hierarchical routes, are well conceived approaches to improving performance in the post attack period. Other techniques have been suggested that will give NETS calls priority access to surviving PSN resources.

The situation is not nearly as well understood or under control at the local or regional levels. For a user to be successful with an attempted NETS call, it is necessary to ensure access to dial tone, connections to the regional telephone company access tandems, and then access to long-distance carrier switching facilities. This may require some form of load control or preferential treatment by the local telephone company, an approach both sensitive and complicated to implement because of the many different types of equipment used for local access. While technically feasible for newer types of switching equipment, significant Government effort directed to the local-telephone-company level and possibly in Congress may be needed to provide NETS users with reliable post-attack access to the PSN.

H. Cost

Because of the sensitive issue of the upcoming NETS procurement, the Committee was presented with only preliminary and very incomplete cost information. While the data suggested seems reasonable from an order-of-magnitude viewpoint, the Committee was not able to assess the cost information provided nor was it able to develop its own cost estimates.

I. Implementation Options

The issues and implications of the discussion above suggest several reasonable alternatives to elements of the proposed NETS implementation that seem workable either as stand-alone approaches or in combination with one another. In combination, they suggest a phasing plan that could begin with a lowest-capability NETS and then add features and elements with time.

Option 1: Replace ASDs with a Personal Identification Number (PIN) system.

Call controllers must maintain data bases of allowable PINs. Use of the system in peacetime must be restricted to maintain control. One means of doing this could be to have the Network Management and Analysis Center (NMAC) periodically initiate commands to inhibit access to the system. Without these NMAC commands the system would be open to all valid PINs. In the event of destruction of the NMAC, the system would be open automatically to all entrants with valid PINs. The risk of this alternative would be less controllable access in the pre-attack period. The reward is in eliminating the cost of ASDs and more flexible access during the post-attack period. In particular, during the reconstitution effort a PIN system would enable previously unforeseen

users to access the system more easily than an approach requiring physical devices such as ASDs. The NCS may be interested in a backup PIN system to supplement the ASDs.

Option 2: Reduce Transmission Compensation.

The NCS should consider seriously relaxing the requirement for secure voice and 2400bps data in the post-attack period. Recognizing that in the pre-attack period NETS will be operating with clean communication lines and short paths, encrypted voice and data should be readily accommodated with reduced transmission compensation. In the post-attack period, these features would be less essential than the ability to pass ordinary voice. The encryption of inter-Call-Controller and Call-Controller-to-NMAC traffic would still be possible. The fail-safe mode in the post-attack period would be to fall back to unencrypted traffic between the CCs. This alternative would have a negligible impact on the pre-attack requirements. Only clear voice would be likely in the post-attack period. The reward: reduction in cost for the Call Controllers.

Option 3: Combine Call Controllers and Survivable Signaling Systems.

A substantial task remains in providing survivable signaling for the long-distance and access telephone networks. The NETS CCs subsystem derives its link capacity by creating links made up of paths from the circuit-switched PSN. The CCs can only find paths if the PSN signaling system is functioning. The NETS traffic of 3,000 Erlangs represents a call rate of a few calls per second. At this rate, the existence of a signaling path between two NETS users is sure to imply the existence of a voice path following the same physical routing.

The S-link approach described to the Committee provides an analogous and superior packet-switched system. Since a survivable signaling system such as the S-link system is mandatory to survivability of communications, and since the S-link approach improves on the routing and probing approach proposed for the Call Controller system, the two systems could be combined into the same software and processor. At a minimum this would eliminate the need for CCs at the AT&T switching centers. The reward would be an improved and possibly lower-cost routing system within the long-haul network. If S-link signaling is adopted, additional routing capacity is available. However, the LEC segment of the system will require equal signaling protection. No description of the techniques used to ensure survival of the LEC access switches has been described to the Committee. It would seem that a uniform approach based on a consolidated, packet-switched signaling system would make the most sense. Unless such a unified scheme is developed, it is likely that call controllers would still be needed at the local-access tandem switches.

Based on the above approaches,many phasing plans are possible. One such plan might be the following.

- Develop a minimal capability CC, augment PSN long-haul routing approaches as proposed by the NCS, and use a PIN-based system without call compensation.

- Add a survivable signaling system, incorporating the CCMs and/or SIMs if possible and economical.

- Add CC-to-CC encryption and access security features.

- Add, as budget allows, new and redundant physical transmission links to the facilities of the long-distance carriers and as interconnections between long-distance carriers.

J. Conclusions and Recommendations

The Committee concluded that use and augmentation of the PSN provides the most viable and only realistic alternative for meeting NETS requirements.

NETS must handle clear and secure voice, facsimile, and low-speed data. It must prevent unauthorized access and hostile intelligence exploitation. It must be available immediately when needed and must survive a range of attacks and targeting scenarios.

The Committee found three reasonable alternatives to elements of the proposed NCS NETS implementation schema that could work as stand-alones or in combination with each other. Option 1 would replace ASDs with a Personal Identification Number (PIN) system. Option 2 replaces the requirement for secure voice and 2400bps data in the post-attack period, thereby reducing the need for transmission compensation. Option 3 combines call controllers and survivable signaling systems, e.g., S-links.

The Committee recommends that the following be made mandatory characteristics of any NETS implementation :

- Enhanced PSN routing;

- Survivable PSN signaling;

- Access restriction pre-attack;

- Access facilitation for authorized users post-attack;

- Implementation with a critical mass (100-150 minimum) of call controllers;

- Unattended operation and routine exercise in the pre-attack period; and

- A Network Management Administration Center.

Desirable characteristics that could be added to NETS are:

- Priority and preemption;
- Transmission compensation;
- Augmentations to the PSN;
- Billing;
- CC-to-CC encryption; and
- ASDs.

The Committee believes that if NETS is implemented with the mandatory characteristics it will meet the essential needs for emergency communications in the post-attack period for its limited set of predesignated users.

V. THE VALUE OF NETS FOR NSEP

A. Introduction

This chapter of the report reflects the Committee's judgments about the effectiveness of NETS in support of various NSEP situations (see Issue 14 in the Appendices for related comments). It does not purport to assess the cost-effectiveness of the various levels of implementation for NETS, nor implementation options such as SIM vs. CCM or augmented S-links vs. other survivable signaling schemes. These matters were discussed in Chapter IV, where it was made clear that while there are several alternative levels of implementation possible at different levels of cost, the widely varying cost estimates that the Committee has seen provide little confidence that any one estimate can be trusted until actual bids are received.

What is clear is that a NETS system consisting of 100-150 CCs (CCMs or SIMs) and the use of S-links or some other means of avoiding the "few critical points of failure" situation with today's Common Channel Signaling, i.e., one robust enough to provide nationwide telecommunications recoverability for large levels of destruction, will be expensive, with life-cycle cost in the hundreds of millions of dollars. This chapter attempts to put such cost levels in perspective by presenting the Committee's thinking about the match between NETS capabilities and the NSEP job the NETS is expected to do.

The Committee's opinion is that while NETS is not needed for peacetime emergencies, even of very large magnitude, a robust NETS will make a substantial pre-attack contribution to deterrence, especially to the "decapitation" type of attack, provided the potential attacker believes that NETS will work. The greatest potential value of NETS occurs after a nuclear war in which the U.S. is attacked with large numbers (hundreds or more) of nuclear warheads.

The Committee has assessed the value of NETS in three wartime periods: (1) pre-attack, up to the time that the initial enemy weapons are detonating on the U.S., (2) trans-attack, for whatever length of time the nuclear exchange continues, and (3) post-attack, when reconstitution and national recovery are taking place. We accept the

view that reconstitution efforts will be more or less continuous if the trans-attack period is prolonged, as in the unlikely event that a nuclear war would take a protracted form.

B. The Pre-Attack Phase

In the pre-attack period, the Committee sees only a negligible military value for NETS, considering its cost, but a considerable contribution to the intangible and unquantifiable factor of deterrence.

If the NETS is implemented, a would-be attacker, viewing the U.S. several years hence, will have to take into account the rich telecommunications fabric of the country as one of its largest national assets. There will be a number of networks whose capabilities will be of particular interest to his calculations: the various military networks and the NETS augmentation of the civil networks, the PSN.

Over the years, the defense community has built up numerous dedicated, special-purpose systems and networks designed to survive early attacks and to enable execution of war plans. These networks exist and can respond in seconds or minutes for specific functions. NETS can have some military value in providing backup to some of those networks by using preset connections called up on warning. It could also serve headquarters elements which have deployed to austerely equipped alternate locations possessing few communications routes and channels.

However, these military systems all have one disadvantage that the NETS does not possess: they do not support the bottom-up recovery need, whereas a properly configured NETS system does. As our predecessor committee pointed out[1,2], this Committee also believes that the idea of top down reconstitution after a heavy attack is unworkable since the individuals and groups that will perform the reconstitution are most unlikely to be the same individuals and groups that had been assigned that federal responsibility before the attack. But this is exactly the premise upon which most of the military networks are built. The presence of the NETS and its capability for accelerating post-attack recovery would have to be taken into account by a would-be attacker.

---

[1]The Policy Planning Environment for National Security Telecommunications (Annual Report), National Academy Press, Washington, D.C., May 1985.

[2]The Policy Planning Environment for National Security Telecommunications (Final Report), National Academy Press, Washington, D.C., July 1986.

In the pre-attack period, other government agencies having little or no access to the specialized DOD networks will confront serious communications difficulties when attempting to use the public switched network, particularly if the pre-attack period is one of rising tension and danger with consequent rapid growth of traffic demands on the PSN. However, there are solutions to this problem that are less costly than the NETS. Among them are the more efficient traffic-handling techniques that are evolving in the PSN itself, such as dynamic non-hierarchical routing, preferential traffic controls such as dial-tone restriction, and the many other manual and automatic techniques that PSN managers use today to take care of traffic overload conditions. There could also be traffic management controls implemented in the FTS that could limit access to only the most important users.

If the NETS is installed, it is important that it be given some pre-attack function, to be sure that it is continually exercised and debugged. The possibility of a joint arrangement with FEMA should be explored.

C. The Transattack Phase

In the transattack phase, the value of a "robust" NETS (at least 100-150 CCMs and/or SIMs with survivable signaling) increases as the amount of damage to the nation's telecommunications infrastructure grows. As the system is presently designed, its continued utility during the transattack period is heavily dependent upon the survival of those who have access security devices (ASDs), and the extent to which surviving switching and transmission facilities continue to operate with on-site power-generation equipment. There are simply too many imponderables for the Committee to be able to assess the value of lesser levels of NETS implementation against the myriad of possible damage scenarios.

When the transattack period is relatively short, as in the case of massive nuclear exchange, the post-attack period arrives quickly. It is the prolonged transattack environment, as in the case of protracted war, that poses the most difficulties for the Committee in trying to judge the value of NETS. To illustrate, consider the following: If the enemy attack consists of a few tens of weapons over some period of time, the resulting damage is not likely to fragment the PSN into small, widely separated islands of connectivity. Rather, there will be islands of destruction to bypass or to penetrate. However, the traffic demands on the PSN will be astronomical and the NETS, with its preferential routing and traffic management controls, would provide a much higher probability of call completion than would simple access to the PSN, even with the full menu of regular traffic management controls applied by the network managers. But if specialized access (e.g., with a "travelling class mark") can be available to critical users of the PSN, a lower-cost solution than the NETS is possible. The NETS thus provides "insurance" for the more catastrophic situation, yet has utility in lesser cases at a much higher marginal price.

D. The Post-Attack Phase

1. General Comments

The Annual Report of the predecessor committee[1] recommended that post-attack telecommunications capabilities be designed for the maximum degree of scenario independence. After analyzing the threat models defined in that report, the committee recommended that preference be given to the simpler and more robust arrangements amenable to bottom-up reconstitution in the post-attack environment. It also recommended avoiding reliance on a predetermined, top-down, management structure.

The Committee considers telecommunications to be a crucial resource in reconstituting the nation, especially in the more severe end of the threat-model spectrum. A surviving NETS will be of very great value, but only if those who need to use it will be able to do so. Thus, the availability of access and usability to those leaders who emerge in such a chaotic environment becomes critical. There are two aspects to this: making a path available physically and making the service sufficiently easy for the emerging individual leaders in post-attack environments to understand and use. Without some means of easy-to-use access for surviving local authorities, the system's value will depend upon the survival of those who had been given access and NETS training in the period before the war, a circumstance basically incompatible with the bottom-up recovery situation that we believe to be the most realistic one for the heavy-damage case and also incompatible with the Committee's chosen premise of scenario independence.

E. NETS for Reconstitution

The Committee believes that there will be significant utility in NETS in the first phases of reconstitution. The post-attack period will require major efforts to reestablish lines of governmental authority, to care for the survivors, and to reconstruct damaged and destroyed segments of the nation. One key to this is the "bootstrap" function the NETS can play in reconstituting the telecommunications structure itself. Once a few NETS circuits have been used as order-wire facilities, other traditional order-wire methods will be applied by surviving telecommunications operating and management people. As this process proceeds, the islands of telecommunications connectivity left in the wake of an attack will be enlarged and interconnected, and new directory information built up on the basis of identifying "who is where now and with what responsibilities" in the reconstituted nation.

---

[1] The Policy Planning Environment for National Security Telecommunications (Annual Report), National Academy Press, Washington, D.C., May 1985.

Thus, the reconstitution value of the NETS will be at its highest point in the time period just when the residual telecommunication structure begins to be reconnected. Of course, the duration of that period will depend upon the amount of damage done to the network structure and the ability to obtain the resources required to rebuild. Resource identification and allocation will be critical functions, and the ability to use the NETS for those purposes could be very important for critical items not available locally or in nearby areas.

Identification of needs, and matching resources and allocations to the most important needs will be critically important tasks for other government bodies that do not possess the order-wire asset. Hence, the NETS could be the only means available for such purposes, pending some reconstitution of the PSN. One can assume safely that lives would be saved and reconstitution speeded by the existence of a surviving NETS provided the surviving NETS has adequate access procedures.

F. Universal Access

As discussed in Chapter IV, one of the Committee's greatest concerns has been that in the post-attack environment the people who need the NETS most will not be able to use it, either because they cannot access it or because they will be prevented from using it after they do access it.

In order to provide dial tone to the subscriber lines most likely to be used by post-attack NETS users it will be necessary to make a modest redesign of the system. The present emphasis on the customer set as "20,000 federal employees" must be replaced with the view that the customer set is "20,000 NSEP users." This leads to the need for preferential dial tone provision to hospitals, armories, police and fire stations, perhaps certain pay phones, and other likely spots by means of line load control (limitations on what calls are queued) and essential service protection (inserting calls from certain lines into preferential positions in the queue).

Once the NSEP user is connected to a CCM or SIM, the signaling between them must proceed (see Issue 2 in Appendix A). As discussed in Chapter IV, the special area code, special NETS trunk reservation, and other means will accomplish this.

G. Encryption

The Committee is concerned that the present NETS design, with its emphasis on encipherment not only of control traffic but also of user access, adds complexity to the system (see Issue 4 in Appendix A). We agree that some level of protection is required in the pre-attack period to prevent spoofing and unauthorized access. The Committee's concern arises from the fact that the post-attack problem must shift from limiting access to facilitating such access by unprogrammed users,

if bottom-up reconstitution is to take place. Thus, to the extent that implementing the relatively high level of protection requires a device like the ASD, the Committee believes that other options such as simpler password or PIN techniques should be examined carefully with the intent of choosing the simplest access method even at the expense of less protection.

H. Simplicity within NETS

Just as the NETS will be presented with users of almost no training, craftsmen working within the system itself may not happen to be those that have been trained in NETS. As argued in Issue 12 in Appendix A, high technology has reached the point at which automation continually eliminates the human in favor of the automated machine. That is the basis of the entire NETS design. Much thought should be given to providing easy-to-use, manual, backup capability to the currently designed signaling between CCs, to route-finding, to equalization, and to other NETS functions.

I. Conclusions and Recommendations

1. Pre-attack exercising of the system should be made automatic, perhaps by making the emerging NETS service an agreed-upon, shared resource of another agency, e.g., FEMA.

2. The deterrent value of the NETS should be emphasized in strategic planning, and at the appropriate time NETS should be made public so that it is widely known internationally.

3. To make the NETS maximally available post-attack to a user population undefinable in advance, NETS access information should be made easily accessible, perhaps on personal "credit cards" for PINS or prestocked quantities of ASDs at various public safety locations at the local level.

4. Legal and regulatory roadblocks should be removed so that preferential queuing for dial tone at end offices can be provided nationwide to locations likely to have post-attack NSEP significance.

APPENDICES

APPENDIX A

COMMITTEE ISSUE AND RESOLUTION STATEMENTS

1. Survivability of PSN Signaling for NETS Purposes

Signaling for call addressing and supervision for the dominant AT&T network uses common channel signaling (CCS). The toll networks of the other common carriers (OCCs) and the regional local-exchange carriers (LECs) are expected to use CCS in the future, but to a lesser extent.

For the AT&T network, the United States is divided into seven signaling regions. Each region has two signal transfer points (STPs) located in or near two cities, usually 100 or so miles apart. Through each of these STPs pass the address and supervisory signals for all AT&T toll calls within and between regions. Due to the vulnerability of the 14 AT&T STPs, an alternative signaling arrangement developed specifically for NETS has been proposed. This arrangement is known as "S-link" signaling.

The Committee examined the effectiveness of S-links and whether there were other more effective or less costly signaling alternatives, such as "ringdown," that might be developed and deployed.

Issue Resolution:

The AT&T network employs common channel signaling (CCS). The address and supervisory signaling for all calls are processed by signal transfer points (STPs). Each toll office connects with two STPs. There will be a maximum of 7 STP pairs in 14 cities by 1988. Should the data links to STPs or the STPs themselves be removed from service, all of the interoffice signalling to and from subtended offices would be lost. To remedy this, AT&T has proposed to provide for interoffice signaling using from 350 to 650 data links, called "S-links." At least one S-link would connect with each of the 104 No.4ESSs™ that form the basic switching capability of the AT&T network. Depending upon location, some offices would act as signal transfer points and pass signals from one S-link to another. Information on the success of probes made over S-links which is time stamped is stored in the No. 4 ESSs™ and updates are numbered so that all nodes are working from a consistent and current set of data.

The S-links would use analog data transmission with modems operating at 4800 bits per second. This form of technology was chosen because it is well known, tested, and requires no new development. The S-link signals would be similar in level 2 and 3 protocols to those used with common channel signaling system No. 7. The number of S-links to be provided would depend upon the locations of potential users and related, anticipated, damage scenarios. With 650 S-links, the emergency signaling network would be expected to complete more than 95% of the NETS calls without blocking from the lack of S-link signaling chain. A minimum of 350 links would encounter marginal blocking of about 65%. To decrease blocking if the smaller number of S-links were installed, regular trunks equipped with the now-outmoded, single-frequency signaling could, with added complexity in the programming of the No. 4ESSs™, provide for establishing greater connectivity in a sparse, 350-S-link network.

The S-links would be used not only to pass NETS call probes, but also to pass disconnect messages on calls that existed in the network pre-attack as on-hook signals were detected. As a result, it might be possible to develop S-link channels. While this technique might be less costly, it is expected to increase the time required to restore service and incur a risk that the S-links might not work when needed.

Provision is needed for regularly checking the operability of the S-links. Also, the routing tables for the S-links would be updated as changes are made in facilities routing.

The U.S. Sprint network is also implementing common channel signaling, and is expected to be in operation in 1988. The signaling network would use STPs at each switching office (there may be more than one switch per office). These STPs would communicate with service control points (SCPs) that would pass signaling information between STPs. The U.S. Sprint network is being planned with redundant pairs of SCPs in each of its three regions. Loss of the SCPs in all three regions would incapacitate the network.

2. Call-Controller-to-Call-Controller Access

The usefulness of the NETS network is dependent upon the ability of call controllers to communicate with each other in a reliable fashion over the remaining public switched network in an emergency situation. This is particularly critical since the public switched network will become extremely congested, with resulting, severe, trunk-group blocking under emergency conditions. It is therefore necessary to develop alternatives to provide for a viable NETS network.

Issue Resolution:

AT&T Bell Laboratories presented several possible, workable alternatives to the Committee to solve this issue. Two of the more interesting possibilities are a trunk-reservation-based algorithm and a

queueing algorithm. Both these algorithms rely on the fact that NETS calls can be identified within the PSN by the assignment of a unique area code (e.g., 701) for all NETS call-controller-to-call-controller calls. Under full-load conditions, the reservation algorithm reserves one trunk for NETS call-controller-to-call-controller traffic between 4ESSs™. NETS traffic is immediately assigned to this reserved trunk when it arrives at the fully loaded 4ESS. In addition, the next time a trunk becomes vacant at that 4ESS it is reserved for the next NETS call. This process continues indefinitely.

Under the queueing algorithm NETS calls are put in a queue as they arrive at a fully loaded 4ESS. They are then assigned to the next idle trunk. Both these approaches are technically feasible and solve the blocking problem for NETS calls when the PSN is congested. It is important to point out, however, that both these approaches require a surviving common channel signaling system. Further work is necessary to determine if this approach can be extended to Regional Bell Operating Company (RBOC) access tandems and to non-AT&T inter-exchange-carrier networks.

3. Subscriber-to-Originating-Call-Controller Access

This issue deals with subscriber access to the NETS call controller (CC). There were three sub-issues involved: obtaining dial tone, user authentication, and the unplanned-user authentication problem.

The usefulness of NETS is dependent upon the user's establishing a telephone connection to an originating call controller (OCC) located in an access tandem or toll office of an interexchange carrier (IC). To reach an access tandem or toll office requires placing a call through a local or end (class 5) office, to which the user is connected either directly or through a PBX trunk.

In the post-attack period it is expected that surviving end offices, and perhaps the access tandems, will be heavily congested with local traffic. This means that it may be difficult, if not impossible, for the NETS user to obtain dial tone to place a call to the OCC. Furthermore, the trunks that the call required to reach the OCC may also be congested. Congestion in bypass networks, such as FTS-2000, that might also be used to reach toll networks must also be considered.

It is expected that the terminations on local offices by assigned ASD users may require and receive special priority treatment. However, in time of crisis, the ASDs, PINS (if implemented), and accompanying authority may pass to users other than those originally intended, known as unprogrammed users. In such cases special-access authentication treatment may be required.

By the time NETS is implemented, it is expected that the concept of the Integrated Services Digital Network (ISDN) may be implemented

and in use by government agencies where ASD users are located. Therefore, the local-access solution should also deal with the serving of lines subscribing to ISDN. How will access through the local intraLATA networks be ensured for the use of NETS by both programmed (originally authorized) and unprogrammed users?

Issue Resolution

Obtaining Dial Tone

All lines and PBX trunks that terminate in a local, central office are given an equal chance to access those portions of the hardware and/or software required to receive the digits to be dialed by a call originator. An indication that the central office is ready to receive a call is to return "dial tone" to the caller. Under normal traffic conditions (95% of the time) the caller should receive dial tone in less than 3 seconds during an average hour.

Electromechanical and electronic switching systems have included in their designs provision for dealing with extremely heavy loads, such as those encountered during a disaster. This feature is known as "line load control" and is the one that must be depended upon should NETS be activated. Any special provisions for NETS in local offices, of which there are approximately 18,000, would be prohibitive in cost.

Line load control divides the line (and PBX trunks) into at least two categories. The telephone company makes these assignments on what it perceives to be the relative priority of need for service during emergencies. The highest priority category includes the lines of emergency service bureaus, hospitals, police and fire, etc. Frequently, coin telephones and doctors' lines are also placed into this category. Some states, however, may have rules against the implementation of line load control.

In electromechanical offices line load control is activated manually. It is rarely used since there is a reluctance for managers to assume responsibility for its initiation. Generally, in electronic switching offices there are only two classes of lines: priority and nonpriority. In some electronic switching systems the line load control feature is quite sophisticated, giving priority lines preference when they originate calls but serving non-priority lines to the extent possible should there be any remaining capacity. Since most offices in the United States will use electronic switching techniques within the next decade, lines with or without priority will be able to obtain service from their local offices if they wait long enough for dial tone.

The originating call control modules (OCCMs) will generally not be in local switches. They are more likely to be associated with access tandems. The trunks from local offices are shared generally by all traffic that uses the access tandems, including traffic primarily

intended to reach interexchange carriers (IC). While a unique access code (950-0627) is dialed to reach the OCCM, a separate trunk group is not currently required . It is recommended that steps be taken to assign a sub-group of the trunks to access tandems when OCCMs are located there, so that in a pre-attack period they could be automatically reserved for the 950-0627 traffic.

Should government and other locations originating NETS traffic have direct access to ICs, there appears to be no difficulty in reaching OCCMs associated with IC switches.

User Authentication

The Access Security Device (ASD) provides the means by which a user accesses NETS. It prevents unauthorized use and intrusion ("spoofing"). The ASD contains the user's authorized precedence and pre-emption, and other calling privileges such as preset connections and retry limits. It also governs the extent of the probing and routing activity. The availability of an ASD or some equivalent means of providing assurance of access to the user is absolutely essential, and hence critical, to the functioning of NETS.

The ASD is a device that couples to a user's telephone. It is not clear whether or not the ASD could be used by a PBX operator to provide NETS calling capability to a telephone without an ASD served by that PBX. If that capability does not exist, the effectiveness of NETS will be overwhelmingly dependent upon the foresight of those who determine the pre-conflict distribution of ASDs.

The ASD must be able to "talk" to a call controller to initiate NETS access. Depending upon the location of the ASD, the transmission path to the CC could be very poor if a remote user module was not available to condition the transmission path.

The Unplanned Users

Our predecessor committee placed great emphasis on the role to be played by local and state authorities in reconstitution activities in the post-attack time period. Who will survive and rise to the leadership challenges of that environment cannot be forecast. Availability of NETS to those local authorities could be crucial to their activities. Yet, without an ASD it will be denied them. Some number of dispersed, pre-war stockage of ASDs is imperative and should probably have only a standardized, limited set of calling privileges. In any case, NETS will be of minimal value if some means is not found to provide access to local authorities in the post-attack period.

The unplanned user access problem remains open. NCS must identify a means to ensure unplanned user access. Pre-stocking, Personal Identification Numbers (PINs), and "credit cards" represent some of the options available.

4. Access Security for NETS

This issue considers the signaling and data encryption scheme embodied in NETS.

As with an ASD, the signaling security function has as its primary purpose the protection of the network signaling activity from intrusion ("spoofing") or hostile traffic analysis. It also has the added function of protecting the data exchanges between the call controllers and the NMAC from hostile intercept. While the value of network signaling protection in the post-attack environment is uncertain (depending upon the magnitude of the nuclear exchange), their importance in the pre-and early trans-attack time frames is evident.

The continued functioning of the signaling security feature to and from ASDs to the CCs and among the CCs themselves is critical to the functioning of NETS. Data encryption to and from the CCs and the NMAC is not. The entire probing and routing process (including features such as retry, crankback, precedence and preemption) depends upon the successful exchange of enciphered signaling messages among the system elements. It appears that many of these exchanges must take place before any transmission compensation is needed.

Bit-error rates and timing synchronization are usually the "villains" in encryption systems. The trans- and post-attack periods will certainly produce an extremely high bit-error-rate environment.

At the minimum, there must be a very robust coding scheme employed by the security system, together with very good error-correction techniques. A better solution, but probably harder to implement, would be to incorporate a "fail clear" capability when and if the system appears to be failing because of security-system malfunction. Such a "fail clear" feature might only be implemented on command by the NMAC, or enabled for automatic implementation, when required, by the destruction of the NMAC.

Issue Resolution

The signaling security system is planned to be dual-tone, multi-frequency (DTMF) signaling with a robust encryption scheme. It will operate as though it were a telephone call on a CC-to-CC basis. This appears to be a satisfactory approach, and the NCS should oppose efforts to make this scheme more complex under the guise of added cryptographic strength.

5. Path Selection

The current route-finding strategy assumes that it is necessary to probe each hop on a possible new route as though no information on that

set of trunks were available from previous probes (information is in fact saved on which called party was busy and which areas are known to be congested; the trunk information is not saved). This strategy is based on the assumption that just because trunk capacity was found to be available/unavailable on a given hop on a previous probe is not assurance that it still will be available/unavailable on the next probe. This procedure discards information that is in principle available from previous probes. Two examples are: (1) the reason one trunk is not available is because none are available due to the total outage of the set of trunks on the hop, and (2) information on whether a trunk was previously seized left one percent of the capacity remaining or 99 percent. The issue is important because the present probing mechanism, based on time-outs, takes a long time to complete if there are many hops between source and target node.

Issue Resolution

To get an upper bound on the possible benefits of using information stored from previous probes, computation should be made of the route setup speed, if at each node there is an all-knowing "ideal observer" which knows at any instant of time how many trunks on each hop are actually available. If the results show large speedup and/or increase in call completion probability to be possible, suitable algorithms to use the information should be derived or adopted from the large literature on this subject.

6. Development Strategy and Field Testing

NETS will not be created in so short a period of time that it will be satisfactory to await completion, or near completion, of the system before beginning testing. The Committee is concerned about planning for demonstration site testing of the CCs and the growth of the NETS in a manner that maximizes the utility of the existing system at any point in its installation period. As the system grows (i.e., as more CCs are brought on line), increasingly difficult tests must be conducted to verify system performance. An issue is how the system will be used and/or tested in a cost-effective fashion during peacetime to ensure the confidence of its intended users.

Issue Resolution

NETS is a service that will be introduced in stages in a two-dimensional manner; i.e., initially the number of CCs or augmented switches will be small and will have less capability than later systems. The prime contractor will progress through four stages of increasing numbers of CCs and increased capability of each CC. NETS capability and readiness will be demonstrated through continuous testing programs.

The question of cost effectiveness during peacetime for user familiarization must be decided from opposing considerations: 1) because each CC-to-CC connection is billed as a separate call, NETS is not the service to use in placing normal business calls; but 2) exercises will be held with the prime contractor to use NETS in order to familiarize users with its functionality. These costs will be part of the NETS service.

7. NETS Evolutionary Capabilities and Strategies

The NETS design point presented to the Committee was based on 1987 technology. The same is true of some of the possible modifications to the design point, such as S-links. Yet the planned lifetime of NETS must be on the order of one or two decades in order to justify the expenditure levels proposed. It is thus imperative that the NETS program not be the victim of technological surprise or significant shifts in user requirements (an example of the latter might be that the need to support data traffic post-attack becomes significant).

The next five years are apt to be particularly volatile ones as far as the structure of the PSN is concerned. Analog plant is being written off at a rapid rate. New telecommunication carriers are being set up and others are going out of business or merging. The technology is also in a particularly dynamic state. It is already clear now, in 1987, that at least four mature or emerging technologies are in the process of affecting the transmission, switching and management of PSN. These are:

- Rapid deployment of fiber transmission facilities, first for interoffice, then for subscriber loops ("metropolitan area networks") and LANs;

- ISDN user interfaces, changing rates from 16 kbs to more than DS-3 (45 Mb/s) rates;

- Proliferation of digital cross-connects, which can in the future be commanded over the ISDN D-channel by the end user. DACS units are already at DS-3 speeds (45 Mbs). Switchover times are on the order of seconds; and

- Intelligent networks based on software-controller "intelligent nodes," significantly increasing the ability to expand network functionality and customize it to meet unique individual customer needs.

Issue Resolution

The move to procure NETS as a service rather than a system is to the Committee a wise move to guard against technological obsolescence,

since it is then very much in the contractor's interest to use the latest, most economical technologies to provide the specified service.

The Committee has mentioned elsewhere that NETS is most likely to receive funding approval if the installation is incremental over several years. The Committee endorses this concept for several reasons, not the least of which is that this allows the latest technical advances to be incorporated. We recommend that NETS be evolved gradually. The design point should be revisited continually.

It is likely that the evolving technology and architecture of the network will tend to enhance NETS rather than make it obsolete. For example, the deployment of ISDN and intelligent networks could serve to diminish concerns raised earlier over the ability of NETS users to draw dial tone and gain access to the CC during periods of PSN congestion.

8. Transmission and Equalization

NETS is expected to carry voice and data (or encrypted voice) at 2400 bits/sec. Specific requirements are for "good" or "better" grade of service on at least 95% of calls and a bit error rate (BER) less than 0.0005 on 85% of the connections. The need for some form of transmission compensation is readily established. Paths containing only two CCs would typically fail to meet the BER requirement on data transmission. The issues of concern to the committee are:

(1) Effects of a tandem connection of several adaptive equalizers operating in a dynamic, or tracking, mode during a call;

(2) Build-up of quantization noise due to a large number of analog-to-digital/ digital-to-analog conversions encountered in a transmission path using digital techniques for equalization and switching; and

(3) Cost of implementing the proposed equalizer.

Issue Resolution

The proposed compensation strategy calls for link-by-link equalization during call setup. The equalization for each link is then frozen before adaptation of the successive link begins, so there is no issue to resolve about the performance of a tandem connection of continually tracking equalizers.

That strategy does, however, raise a new issue that has not been addressed by the Committee, namely whether or not equalization readjustment might be required during a call. The issue of quantization noise build-up was tentatively resolved by a demonstration prepared by AT&T Bell Laboratories showing voice quality over a multilink path with compensation activated and deactivated. All members of the Committee

participated in listening tests as part of the demonstration. The consensus was that uncompensated paths produced unacceptable quality due to increased path loss and channel dispersion.

However, this demonstration raised the issue of cost effectiveness of the proposed equalizer design since, as far as clear voice communication is concerned, a strategy that provides only gain compensation and crude equalization at each link in the path might be adequate. The proposed equalizer structure is a 255-tap, digitally-implemented, transversal filter with tap adjustments made by a stochastic-gradient algorithm to minimize mean-squared error during the training period. This is rather more complex than equalizers found in voiceband data modems; however, it does provide effective channel equalization for a broad class of signal formats, including voice and data at various bit rates and modulation techniques. A looser set of requirements on the variety of signal formats to be handled might result in a substantial cost reduction of this component of the CCM.

9. Signaling Protocols

The Committee was briefed on signaling protocol design. The features of this protocol involve (a) user authentication, (b) selection and call-progress message exchanges with the PSN, (c) link call establishment with the next CC on the path, (d) link call clearing in case of crankback, and (e) end-to-end call establishment and clearing.

A question was raised on the reliability of DTMF signaling between the users and the CC and between the CCs. The general consensus of the Committee was that DTMF would be adequate for the job. While it would seem readily possible to increase the signaling rate above the DTMF ten-digit-per-second nominal rate, most of the call-setup delay appears to be in the PSN itself, so the additional complexity and cost do not seem justified.

There was concern that the user-CC and CC-CC protocols might have hidden hazards and may fail in deadlock, livelock or other protocol instability. A briefing was given to the Committee which shows progress on the issue of protocol verification with respect to the state description of a single CC; however, the robustness of the entire system of interconnected CCs may still be suspect. While it may not be possible to verify correctness of the entire system due to its sheer size and nondeterministic interconnections, it should be able to verify correctness of a single connection attempt involving crankback.

From the briefings presented, it appears analysis and design have been concentrated on the view of a single connection attempt fighting the debris of broken CCs, links and other hazards to complete a connection. However, it is instructive also to look at the state of the network itself being attacked by individual connection attempts unknown to each other. This situation is well known to the packet-switching community and requires study in its own right. In

the face of limited resources, links, and CCs, scenarios leading to deadlock are indeed possible. It is not clear that pre-engineered routing tables can always avoid deadlock while ensuring that all routes are thoroughly probed.

Issue Resolution

Attention needs to be given to the survivability of the connection-initiation process, especially with respect to resource contention and fairness. It is also important that facilities that become isolated due to link failures or congestion can be reliably recovered when connectivity returns. The most likely case of concern may be when a set of CCs becomes fragmented or deadlocked while in a holding state for a number of connection attempts. The solution is to realize this at each CC concerned and rapidly return the deadlocked assets to the available inventory.

As a related subject, there was concern about the effectiveness of S-links and the possibility that restoration of the switch signaling protocol might become an integral part of NETS itself. There is, of course, a problem in orderly layering, but computer scientists and protocol designers have solved these problems many times (sometimes in ugly, ad-hoc ways, to be sure). The clear win is that NETS becomes intrinsic to the survivability of the PSN itself, and thus more attractive to the PSN designers.

10. Post-Attack Facility Restoration

Sophistication Versus Simplicity: Reliance on Common Channel Signaling (CCS) has taken away trunk signaling sets that could have allowed craftsmen to restore circuits and signaling on one facility. Now the first confirmation of continuity between two switching nodes has to be the CCS paths; only then can the integrity of the transmission path be verified. Therefore, the build-back capability is contingent upon establishing communications among the field forces that have survived the disaster.

Issue Resolutions

Build Back Capability -- Primitive Order Wire: One means for ensuring communication between switching nodes is to guarantee basic order-wire circuits that do not rely upon CCS. These order-wire circuits should be maintained as direct linkages during normal times and the common carriers should be encouraged to avoid sophistication in such basic circuits. In some circumstances, it can be visualized that the only surviving circuit path could be the order wire. In the future, when the copper wire disappears, the fiber, order-wire facility must be contiguous or else the opportunity for reconnection will be completely blocked.

Manual Process: High technology has reached a point in which automation objectives continually eliminate the human from our

systems. The entire NETS and CCs concept is based on the auto-operator approach. Much thought must be given to the post-attack conditions that can exist, in which complete reliance can easily return to the human beings that must reestablish connectivity. It will certainly be catastrophic if our endeavor to automate eliminates the very tools with which the human forces must work under duress to reconnect the network. The Committee feels that common carriers must continue to maintain the necessary tools and equipment that humans can use with established manual processes to build back the network.

Qualifications and Training of Craftsmen: Craftsmen must receive training in the restoration procedures that will not follow the normal, unstressed type of maintenance and circuit restoration. These craftsmen should become familiar continually with the tools necessary for such restoration. In particular, they should be trained so well in such basics as the order-wire functions that under the most severe outages they will be confident that they can contact the distant end.

Qualifications of Operators -- The Role of Human Operator Versus the CCM Auto-Operator: As the PSN has progressed from direct distance dialing (DDD) and beyond, the role of the inward and outward operators has nearly disappeared. Remembering back to the days of such operators and the ringdown trunk, many an operator established a call under natural-disaster conditions by knowing how to route through another office. Now, with a network that requires CCs to do the search for us, there seems little that an operator can do except use the switch machine. Some thought should be given to how the human, as an operator in the system, could enhance the ability to reestablish connectivity. At the moment, the persons operating the network control and the toll test desks and stabilizing the switching machines seem to be the strongest contributors in reconnecting the network.

Directory Services:

If the damage level is high, much of the previously available information associating individuals or departments with specific telephone numbers in a specific area code will be lost. One of the potential capabilities that NETS offers as part of the build-back process is the reconstitution of directory information. The problem of how to build directories from traffic information and then manage them once they are built is an important present area of computer communication research and implementation, some of whose consequences may be of use in the NETS context. Although this study item is of lower priority than a number of the others, as NETS moves ahead it will be worthwhile to add to the agenda the development of a directory regeneration strategy.

11. Availability of Interexchange Carriers to Handle NETS Calls

What telecommunications network resources are available for emergency use?

The AT&T interLATA network is the largest public network resource in North America. For the NETS project, it is in the public interest to examine the other public and private telecommunications resources of North America to examine how they might be used and integrated to benefit the NETS concept.

Issue Resolution

While the resources of the ICs collectively, and the AT&T network in particular, are extensive, there is the question as to how they might be used in the post-attack period. From available data it appears that switching systems located beyond a direct-blast area might survive. They could be used until commercial electricity or emergency fuel supply is exhausted, provided that emergency generators were energized prior to the attack. The NETS is predicated upon the assumption that useful transmission facilities and switching offices might be found that normally would not be used in the commercial routing of calls between originating and terminating NETS CCM locations.

The information built into the surviving switching offices is limited to intelligence and routing algorithms about the pre-attack network. The NETS is designed to attempt the completion of post-attack calls by probing and developing information about the network that survives. This means that routes for calls are developed and used that differ from those used in commercial service.

In undamaged areas NETS traffic competes with islands of heavy public traffic. The public traffic is subject to automatic, network-management controls that should prevent switches from being overloaded with useless attempts to reach unavailable areas. NETS traffic must be processed by the same switches, circumventing where possible the network management controls.

The AT&T interexchange network reaches all local access and transport areas (LATAs). In many cases it has direct trunks to local offices, avoiding access-tandem switching . The other ICs are accessed primarily through tandems. They reach many terminating points through foreign-exchange lines and AT&T's wide area telephone service (WATS) lines. As these networks grow, there will be fewer WATS crossovers. There is also an increase in the number of private, corporate networks.

To utilize the telecommunications facilities of the United States most effectively, some consideration should be given to implementing appropriate crossovers between IC and large private networks so that all possible public and private facilities could be accessed and used by the NETS. This is not only a facilities problem but also involves

knowledge of addressing plans within these networks. Software defined networks (SDN) use public network facilities as if they were private networks. As a result, these facilities may be accessed by the NETS.

Since the NETS accesses public facilities, it is necessary to provide secure access to the network routing tables that are to be used exclusively by it. This is one reason for confining these tables to the CCs instead of including them in each tandem and toll switch through which a NETS call might pass. With the NETS call routing it is possible that the call will pass through more switches than normally encountered in a commercial call. As a result transmission compensation must be included in the CCs. Access to local exchanges is necessary to complete calls. The interexchange networks appear to be the only facilities that could be used to complete calls into these exchanges through what remains of the long-distance telecommunications infrastructure.

12. Reasonable Alternatives to the NETS

The NETS focuses on using the public switched telephone network (PSN) to carry NSEP traffic in a post-attack period. Characteristics of the NETS architecture include:

- Restricted user access for NETS by requiring access through ASDs;
- Improvement of the voice signal through call compensation to allow for very poor, unusually long voice paths;
- Enhanced PSN routing of voice calls through augmentation of switch routing tables to test noneconomic routes;
- Priority treatment of NETS calls by the PSN via special area codes or class marks;
- Use of CCs to find especially long paths in the case when shorter ones have not survived; and
- Augmentation of the PSN in selected areas to increase redundancy and alternate routing opportunities.

A question posed by the Committee is whether there are reasonable alternatives to the presently proposed NETS.

Issue Resolution

The issue may be broken into two related questions: 1) are there reasonable alternatives to using the PSN, and 2) if the PSN is used, are there better ways to use it?

The resolution of question one appears straightforward. The PSN approach seems clearly the best possible NETS alternative, presuming that the PSN signaling system survives a scenario-independent attack.

The Committee evaluated other possible methods of providing Nationwide Emergency Telecommunications Service and for a variety of reasons found them unsatisfactory compared to the PSN. None possessed the ubiquity, diversity, redundancy, survivability, and robustness that are all PSN characteristics. Indeed, in one form or another they all either rely on the PSN for their interconnections or simply cannot match its utility. To be effective in a post-attack environment, cellular systems have to access some vestige of the PSN. Mobile radio is very localized and generally has only limited PSN access. Satellites could be fairly ubiquitous if significantly more earth stations were available, but they are not. The wide coverage of the downlink footprint of some satellites could be considered ubiquitous; but internetting or interconnecting of satellite systems depend on the PSN. ISDN is a software concept which carries message and destination information but relies totally on the PSN to carry its data. ISDN cannot now find routes, reroute, or crank back. FTS-2000 is also virtually dependent upon the PSN because it is a dedicated network possessing access points into the PSN. None of these has the number nor range of characteristics to challenge that of the PSN. Thus, the NETS concept appears viable if the S-link (or another equivalent subsystem) is added to the PSN to ensure signaling-system survival.

As previously discussed, the NETS CC subsystem is a packet-switched network which derives its link capacity by creating "virtual links" made up of paths from the circuit-switched PSN. The CCs can only find paths if the PSN signaling system is functioning.

The NETS traffic of 3,000 erlangs represents a call rate of a few calls per second. At this rate, the existence of a signaling path between two NETS users is sure to imply the existence of a voice path following the same physical routing. Thus, since the S-link approach described to the Committee provides an analogous and superior[1] packet-switched system, the CC routing functions could be embedded in the S-link packet nodes. (Note: no description of the techniques used to ensure survival of the local telco access switch has been given to the Committee. This segment of the system will require equal signaling protection and it would seem that a uniform approach based on a consolidated, packet-switched signaling system would make the most sense.)

Therefore, as the Committee believes that survivable signaling is mandatory for NETS, then a superior approach to NETS can and should be

---

[1]The S-link approach described to the Committee appears to utilize a range of adaptive-routing techniques common to today's packet-switched systems.

constructed by incorporating the system's call routing directly into the survivable signaling system and simplifying the CCs.

13. Capabilities and Uses of the SIM Versus the CCM [Alternatives to the Call Control Modules (CCMs)]

The specification for NETS assumes that separate devices (CCMs) will be connected to access tandems and toll offices using incoming and outgoing trunk terminations. Tariffs for the use of these access ports are intended to give NETS access to the public network.

An alternative to CCMs is to build the CCM software and hardware capability into the stored-program(software)-controlled switches at the access tandem and toll offices. The principal switches in use today for these functions are the DMS-250 and the No. 4ESS™. This alternative is known as "switch internal module" or SIM. An evaluation of this alternative and comparison with the CCM capability and cost are needed.

Issue Resolution

The name of "switch internal module" (SIM) has been used by two vendors of alternatives to the CCMs. SIMs are developments by switch manufacturers that attempt to gain advantages over the general-purpose CCMs by including some or all of the CCM capabilities in the access tandem and toll switches. This approach has the advantage that, as new features are proposed for NETS call handling, they may be included in future update issues of switch programs. To implement new features with CCMs requires changing hardware and software designs that are specific to this development. Also, since SIMs are embedded in switches, it is more likely that they will be exercised regularly and will perform properly when needed.

AT&T has proposed a SIM hardware and software development to be associated with No.4 and No.5 ESS offices in their network. It uses ISDN-type common channel signaling between SIMs and a standard ISDN, basic-rate termination (for 23 B channels) so that it may communicate with the switch control. AT&T's SIM includes transmission compensation, security hardware, and connection with a network maintenance and administration center (NMAC). The 23 channels are considered adequate since the switch can provide as many equivalent CCM paths as needed. As with CCMs, the SIMs probe and establish connections on an adaptive basis.

Northern Telecom has proposed a system based on developing only software for their DMS family of switches to provide a form of NETS routing. Predetermined routing trees are placed into each switch along with commercial routings. Presumably the NETS routings are utilized only on NETS calls. No secure access, transmission compensation, or NMAC interface were described. Also, there appears to be no adaptive routing based upon the probe results when the DMS SIM software is used.

14. NETS in the Context of the 1985 NAS Report: Does NETS Satisfy the 1985 Academy Report Objectives?

Summary

1. We distinguish the terms "Enemy Force Employment Options" and "scenarios (that relate to each option)."

2. NETS appears to meet its stated objective, given the explicit assumption of a particular Enemy Force Employment Option.

3. NETS will be expensive. A significant cost component is in the continuing expense of a large, distributed, packet-switched network needed to back up the telephone CCS system .

4. The cost of NETS, its limited objectives together with a multi-agency, pro-rata funding scheme, and its service to a limited user population raise concern over continuous, long-term, NETS funding.

5. This paper considers these questions: could NETS be evolved into the missing national communications resource envisioned in the 1985 Academy Report[1]? If so, how might this be done?

Introduction

The 1985 Academy Report[1] recommends that post-attack telecommunications capability be designed for the maximum degree of attack-scenario independence. Further, it recommends that preference be given to the simpler and more robust arrangements amenable to bottom-up reconstitution in the post attack environment. It also recommends avoidance of reliance upon a narrowly preprogrammed, predetermined, top-down management structure.

Definitions

Before reviewing NETS in this context, a little sharpening of some definitions is helpful. "Scenario independence" is best regarded as a comparative adjective and not an absolute condition. One can always come up with a scenario so devastating as always to make the term "scenario independence" meaningless. Let us use the term "Enemy Force Employment Options" to describe "scenario" solely as a subcase.

---

[1] The Policy Planning Environment for National Security Telecommunications (Annual Report), National Academy Press, Washington, D.C., May 1985.

Enemy Force Employment Options

A. Counterforce only (attacking only military targets).
B. Counterforce only plus external (non-public, switched network), command, control, and communication (C^3) targets.
C. Countervalue (a euphemism for destroying cities and population centers).

NETS Survivability Assumption

We believe that the NETS addresses only Enemy Force Employment Options A and B. Option C is countervalue. Fundamental to the NETS survivability assumption is that the "city-busting" Option C will not occur or, at least, if Option C does occur, then the NETS is not expected to be of value. What we are dealing with is the axiomatic assumption that presupposes that the attack planner carefully avoids targeting cities.

Two Issues

This limitation of NETS raises two issues:

1. Is it reasonable to imagine any scenarios under either Options A or B in which the CCS switch points can be taken out by a small number of weapons without necessarily targeting cities--such as by targeting the communication links in low-population-density areas rather than the better targets of switching nodes located in the cities?

2. How confident can we be that Option C will in fact not occur? Or if Option C does occur, will it be so devastating that attention need not be paid even to think about a planned, top-down reconstitution capability?

1985 Academy Report[1] and the NETS

The 1985 Academy Report did not define sharply the boundaries of the targeting options it considered, nor did it narrow them precisely to Options A and B and not C.

A new issue we might wish to consider is: given the relatively high cost of NETS solely to serve a predetermined population of 20,000 federal employees for a worst-case assumption of attacks for Option A or B only, might the NCS be better off if it reconsidered the objectives of the NETS in terms of the 1985 Academy Report? The limitations of the NETS in this context are:

---

[1]The Policy Planning Environment for National Security Telecommunications (Annual Report), National Academy Press, Washington, D.C., May 1985.

1. The NETS has not been optimized, nor designed for ready, bottom-up reconstitution after attack to aid revitalizing a badly damaged public switched network.

2. The NETS user constituency is limited to approximately 20,000, predetermined, federal employees organized in a top-down structure, blocking communications physical access to all others in the field who may, in the chaotic post-attack world, need some telephone access more urgently.

3. Some of the complexity and inflexibility in the NETS derives in part from its given requirement to support encrypted voice in a post-attack environment.

Funding Likelihood of NETS

The limited access to the NETS, coupled with its likely survivability under attacks for Option A or B, will require effort by the NCS to provide broad-based understanding of the NETS' strong deterrent capabilities (for supporting restoration, reconstruction, and continuity of government). A reasonably robust level of NETS implementation with an adequate number of S-links is not cheap. Combine this with the apparent reluctance, even today, of the proposed multi-federal-agency user base to pay its share of the cost. The Committee anticipates pressures to give up the level of added facilities needed for even moderate levels of survivability in response to the political necessity of reducing visible costs to gain funding approvals.

Evolving NETS to Meet the 1985 Academy Report Recommendations

Sharing the Resource

Is the NCS asking too much or too little of the NETS? Would the NCS be better off if it broadens the range of users that a NETS-like system could accommodate, thus raising its allowable cost? It is cheaper to share a larger, distributed, survivable network. There is a critical-mass effect at work here. Terrestrial, survivable, network design is based upon connecting nodes together with redundantly connected network links so that the number of weapons required for cutting the network with an acceptable probability of success exceeds that of an alternative target. Reconstitution arrangements that patch up broken links, combined with very fast, flexible switching raises the survivability level even further.

In essence, the NETS concept would use S-links to form such a survivable network, constituting a distributed, packet-switched network of the scale needed to provide a significant and very important improvement in the robustness of the telephone signaling infrastructure.

A New National Resource

If built, such a network could constitute a new, national, communications resource, usable for more than the initial, limited, NETS requirements. Once achieving the threshold level of redundancy (which does represent a significant annual operating cost), it may be prudent to consider broadening the application, sharing this capability to beef up the entire nation's public switched telephone network to create a more broadly based, post-attack survivability, for all targeting options or scenarios.

Access-Rationing Mechanism

A user access-rationing mechanism is mandatory. Here one might, for example, envision using a national, line-load-control approach to limit access to the network by rationing out the dial tone in duress. One benefit of having the S-links form the underlying, distributed, packet-switching network is that they already convey the CCIS-7 signals necessary for a more sophisticated management of the telephone plant. Whether this is feasible or not is unclear.

Reconstitution

This potentially increased survivability of long-haul telecommunications could serve better, in part, as the order-wire structure necessary for patching up and reconstituting the surviving pieces of the telephone network.

There are other resources that might be used as well. For example, there has been a recent, explosive growth in amateur packet radio. There are now tens of thousands of these units in operation. Radio amateurs historically have had an interest in emergency communications. Amateur packet radio together with a broadened-base, survivable, S-link network might be used to help form very important missing elements of the national infrastructure reconstitution means sought in the 1985 Academy Report.

APPENDIX B

GLOSSARY OF TERMS

Access and Signaling Security-- A NETS function that verifies the authorization of a user to gain access to NETS and that employs encryption techniques to preserve the security of information transmitted during the setup of a NETS call.

Access Security Device (ASD)-- A small device employed by a NETS user to gain access to NETS.

Access Tandem Switch-- A switching system that provides a traffic concentration and distribution function for interLATA traffic.

Alternate Route-- When a call is offered to the direct trunk group and all trunks are busy, the call may be manually or automatically offered to one of several other routes. Such routing of calls is referred to as alternate routing.

Automatic Alternate Routing-- A method whereby a call that encounters an "all trunks busy" condition on the first route tested is automatically and rapidly "route advanced" and offered to one or more alternate routes, in sequence, for completion. See Alternate Route.

Availability-- The capability of establishing a connection between two station sets served by NETS.

Bell Operating Company (BOC)-- A telecommunications service provider that was at one time part of a national telecommunications company and one that provides local telecommunications service in a given geographic area.

Call-- An attempted or completed means of communication over a (communications) channel.

Call Attempt-- Any request to set up a call, whether completed or not.

Call Controller(CC)-- Either a CCM and its host switch or a SIM.

Call Control Module (CCM)-- A piece of equipment that is attached to a host switch via trunks and that provides NETS functions.

Call Record-- A record made of each NETS call linked by a CC.

CCS(Hundred Call-Seconds)-- A measure of telephone traffic load obtained by multiplying the number of calls in an hour by the average holding time per call in seconds and dividing the product by one hundred. The maximum possible CCS that can be handled by one circuit in one hour is 36.

Channel-- A communication path via a pair of wires, phantom carrier, or microwave radio (including satellite). In a crossbar office, it is the path connecting the incoming and the outgoing circuits.

Channel, Four-Wire-- A two-way circuit where the signals can travel in opposite directions simultaneously without mixing with each other. With physical facilities, two cable pairs would be required. Carrier channels are four-wire circuits.

Channel, Two-Wire-- One cable-pair or one-half of a carrier channel.

Circuit-- All or part of a path in which electrical energy travels between two or more points.

Clear Voice-- Voice that is transmitted without encryption.

Crankback-- The process, during call setup, in which call control is returned from one CC to the previous CC when no forward paths are available.

Crypto Period-- The period of time during which a cryptographic key is valid.

Cut-Through-- Establishment of the talking path through a switch.

Destination Code-- A routing code that specifies a specific terminating office regardless of the originating point. It consists of the three-digit NPA code plus the three-digit NNX code.

Destination Number-- The 10-digit number that uniquely identifies the terminating station.

Digit-- Usually one of the symbols 0,1,2,3,4,5,6,7,8,9, and sometimes letters. Also used in telephony to describe the impulse sequence produced by the dial contacts or the audible tones from the DTMF subset.

Diversified Route-- Refers to 25% to 50% of the circuits serving a location being assigned to a separate supporting structure (pole line, radio route, and/or conduit run) for all except 20% of the route with the maximum joint route limited to two miles.

Dual-Tone Multifrequency (DTMF) Signaling-- The generic name for the tone signaling scheme used to signal from telephones to switching equipment, in which characters are represented by selecting two frequencies of the following group: 697, 770, 852, 941, 1209, 1336, 1447, 1633 Hz.

Echo Cancellation-- The process of detecting transmitted speech signals, generating a signal that is a replica of the echo, and subtracting this signal from the actual echo, thereby canceling it.

End Office (EO)-- The switching equipment in a building that provides exchange telephone service for a given geographical area. The building is usually given a name, such as "Broad St."; and in some cases there is more than one end office serving the same area. An end office may include more than one end-office unit.

End-to-End Signaling-- A signaling system capable of generating and transmitting signals directly from the originating to the terminating end after the connection is established, without disturbing the connection. DTMF signaling is such a system. Its tones can be used for sending or receiving information, such as to or from computers or controlling a variety of devices.

Equalization-- The procedure applied to a channel so that the component frequencies of the material transmitted have about the same relationship at the two ends of the channel.

Erlang-- A dimensionless unit of telephone traffic intensity used to express the average number of calls underway. Traffic in erlangs is the sum of the holding times of paths divided by the period of measurement. (1 erlang = x call-minutes/hour).

Exercise Call-- A type of NETS call that simulates network damage and the routing of the call around such damage.

Four-Wire Switching-- Two electrical paths, one two-wire for transmitting and one two-wire for receiving, per trunk that are provided through a system.

High-Usage Group-- A trunk group between two points for first-routed traffic, so engineered that all the traffic offered cannot be handled during the busy hour. A certain amount must overflow to a second group, or to a final group, which is more liberally engineered.

Holding Time-- The total duration of one completed call.

Host Switch-- A PSN switch that has a CC.

Independent Telephone Company (ITC)-- A telecommunications service provider that is not affiliated with any BOC or with AT&T and that provides local service in a specific geographic area.

Interexchange Carrier (IC)-- A telecommunications service supplier that provides service between exchanges.

Key Pulsing (KP)-- A process of pulsing by use of a key set involving either direct current (dc) or multifrequencies, which uses a form of two-wire, dc, marginal pulsing from key set to senders and from sender to sender.

Line--(a) A pair of wires carrying direct current between a central office and a customer's station; (b) the side of a piece of central office equipment that connects to or toward the outside plant.

Link-- In automatic switching, a link is a path between two units of switching apparatus within a central office.

Local Access and Transport Area (LATA)-- A geographic area within each BOC's franchised area that has been established for the purpose of defining the territory within which a BOC may offer its telecommunications service.

Local Exchange Carrier (LEC)-- A telecommunications service supplier that provides public, local service in a specific geographic area.

Low-Speed Voiceband Data-- Data that is transmitted in voiceband frequencies at a rate less than or equal to 2400 bps.

Maintainability-- The ability to preserve the constant operation of NETS including routine servicing and fault repair.

Message-- A sequence of NETS tones and announcements.

Modem-- Contraction of modulator-demodulator; in referring to a carrier system.

NETS Access Code-- The 7-digit number that allows a user to access NETS.

NETS Maintenance and Administration Center (NMAC)--The NETS element that serves as an operations center which assists in providing the logistic support for NETS.

Off-Hook-- The condition that indicates the active state (closed loop) of a customer line.

On-Hook-- The condition that indicates the idle state (open loop) of a customer line.

Operations, Administration and Maintenance (OA&M)-- A NETS logistics function that provides for the operation, administration and maintenance of the system.

Originating CC (OCC)-- The CC that first receives a request for NETS service and that processes the call following origination procedures.

Originating End Office-- The office that serves the calling party; i.e., that office where a particular call originates.

Originating Station-- The telephone from which a NETS user originates a call.

Precedence and Preemption-- A NETS function that determines whether a NETS call can preempt another NETS call and enables assigned-user call privileges to be used.

Precedence Level--The level assigned to a NETS user that determines the allocation of NETS resources with respect to other NETS users.

Preemption-- The process of disconnecting a NETS call for the purpose of making the NETS resource available to a call of higher precedence level.

Preset Connection-- A single NETS call set up over a preset path.

Preset Path-- A geographical path consisting of specific telecommunications links that connect one set of NETS users with another.

Preset Path Number (PPN)-- A set of numerical digits that uniquely identify a NETS preset path.

Priority Call Treatment-- A NETS function carried out by the PSN in which NETS calls are given priority treatment using network management techniques.

Privilege-- The call rights that are available (e.g., number of concurrent calls allowed, call holding time, probing time).

Probing and Routing-- A NETS function that provides special call routing to get around damage in the PSN.

Public Switched Network (PSN)-- The equipment operated by LECs to provide local public telecommunications service and the equipment operated by ICs to provide public, interexchange telecommunications service.

Reliability-- The capability of sustaining a NETS call once placed.

Remote User Module (RUM)-- A hardware device situated at a NETS user location and designed to provide transmission compensation.

Retry-- A NETS function that allows a user, on completion of one NETS call, to initiate another NETS call without surrendering the connection.

Secure Voice-- Voice signaling that is transmitted after encryption.

Standard Call--A type of NETS call that involves the applications of probing and routing. This excludes preset connections, test calls, and exercise calls.

Station Set--A telephone.

Switch Internal Module (SIM)-- A set of hardware and software that is integrated into a host PSN switch to provide NETS functions.

TEMPEST (-PROTECTED)-- A procedure for shielding electronic equipment to prevent emissions of electromagnetic signals that can be detected at a distance from the equipment.

Terminating CC (TCC)-- The CC that is the final CC in the call setup path and that routes the call to the terminating user.

Terminating Station--The telephone that is the destination of a NETS call.

Test Call-- A type of NETS call designed to test a portion of a NETS connection.

Translation-- The conversion of information received in one form to another form; for example, in switching machines the translation of digits received to those required to complete a call.

Transmission Compensation-- A NETS function designed to provide enhancement of transmission quality over pathways used for NETS calls.

Trunk-- (1) A channel connecting switching centers or exchanges. (2) An interface circuit, primarily for supervisory purposes.

Ubiquitous Access-- A NETS function that allows users to enter the NETS network from any station in the CONUS and to reach any other station.

Via CC (VCC)-- A CC that is in the middle of a call setup path and that routes a call from one CC to another CC.

APPENDIX C

GLOSSARY OF ACRONYMS

ac-- Alternating Current
Ao-- Operational Availability
ASD-- Access Security Device
AT-- Access Tandem
AUTOVON-- Automatic Voice Network
BOC-- Bell Operating Company
bps-- bits per second
CC-- Call Controller
CCM-- Call Control Module
CCS-- Common-Channel Signaling
CIDL-- Compromised Identifier List
CONUS-- Coterminous United States
dB-- Decibel
DCTN-- Defense Commercial Telecommunications Network
DSP-- Digital Signal Processor
DTMF-- Dual Tone Multifrequency
EMI-- Electromagnetic Interference
EMP-- Electromagnetic Pulse
EO-- End Office
EOC-- Extended Operational Capability
FCC-- Federal Communications Commission
FOC-- Full Operational Capability
FTS-- Federal Telecommunications System
GFE-- Government Furnished Equipment
GFI-- Government Furnished Information
GOS-- Grade of ServiceGTOC-- General Telephone Operating Companies
HEMP-- High-Altitude Electromagnetic Pulse
Hz-- Hertz
IC-- Interexchange carrier
ID-- Identifier
IDM-- Identifier Message
IOC-- Initial Operational Capability
ITC--Independent Telephone Company
KP-- Key Pulse
LATA-- Local Access and Transport Area
LEC-- Local Exchange Carrier
LMS-- Least Mean Square

MF-- Multifrequency
MTBF-- Mean Time Between Failure
MTP-- Master Test Plan
MTTF-- Mean Time To Failure
MTTR-- Mean Time To Repair
NCS-- National Communications System
NETS-- Nationwide Emergency Telecommunications Service
NMAC-- NETS Maintenance and Administration Center
NSEP-- National Security Emergency Preparedness
OA&M-- Operations, Administration, and Maintenance
OCC-- Originating CC
OCCM-- Originating CCM
ORUM-- Originating RUM
OU-- Originating User
PBX-- Private Branch Exchange
PDD-- Probe Destination Digits
POP-- Point of Presence
PPN-- Preset Path Number
PSN-- Public Switched Network
RF-- Radio Frequency
RUM-- Remote User Module
S-- Secret
SIM-- Switch Internal Module
TCC-- Terminating CC
TCCM-- Terminating CCM
TLP-- Transmission Level Point
TRUM-- Terminating RUM
TU-- Terminating User
U-- Unclassified
VCC-- Via CC