

Originally Processed With FOIA(s):
2005-0336-F

FOIA Number:
2005-0336-F

FOIA MARKER

**This is not a textual record. This is used as an
administrative marker by the George Bush Presidential
Library Staff.**

Record Group/Collection: George H.W. Bush Presidential Records
Collection/Office of Origin: Science and Technology Policy, Office of (OSTP)
Series: O'Neil, John F., Files
Subseries: Reports and Publications Files

OA/ID Number: 62104
Folder ID Number: 62104-002

Folder Title:
National Research Council

Stack:	Row:	Section:	Shelf:	Position:
	0	0	0	0

Experts Say Phone System Is Vulnerable to Terrorists

By ROBERT D. HERSHEY Jr.

Special to The New York Times

WASHINGTON, Feb. 7 — Top scientific advisers to the Government warned today that the nation's telecommunications system was increasingly vulnerable to large-scale disruption by terrorist attack.

Appearing before a Senate panel, the experts said the risks have risen because of industry fragmentation after the 1984 breakup of the American Telephone and Telegraph Company and because of advances in fiber optics and other technologies that foster heavy concentrations of equipment and data.

As a result, "a few well-placed hand grenades would crash major portions of the domestic long-distance networks," said John C. Mc-

Donald, the head of a 14-member panel of the National Academy of Sciences that is scheduled to publish a major report on telecommunications security this spring.

Appearing before the Senate Governmental Affairs Committee, the specialists agreed that while the United States had been largely free of attacks against its domestic infrastructure, it should be assumed that terrorists would someday move beyond highly symbolic targets, like diplomatic operations and airliners, to take potentially crippling actions against broad sectors of the economy.

Telecommunications networks "present tempting targets," said Charles C. Lane, a Secret Service agent who has spent the last year working as a special investigator for the Senate committee, which is

headed by John Glenn, Democrat of Ohio. "The networks are exposed, they are vulnerable; chances of a successful attack are highly probable, and significant economic damage might be inflicted as a result," Mr. Lane said.

New Impetus for Study

Congress and national security specialists have spent much time studying the protection of industrial and other sensitive operations, and the issue has gained fresh impetus because of recent terrorist activities and assorted non-terrorist episodes, like a fire last May at the central office of the Illinois Bell Telephone Company in Hinsdale, Ill.

The fire, considered to be the most serious ever experienced by the industry, disrupted local and long-distance communications over a wide

area, including many business and emergency services touching tens of thousands of people.

Two of today's witnesses, however, sought to minimize the risk of serious disruption while acknowledging that the threat of successful attack had risen in recent years.

"Major disruptions of the nationwide telecommunication networks during a peacetime emergency or disaster would be highly unlikely," said Benham E. Morriss, the deputy manager of the National Communications System, a Government body established in 1963 because of shortcomings in emergency communications identified during the Cuban missile crisis in 1962.

He was joined by Thomas Norman, the vice president of engineering and operations for United Telecommunications Inc.



Cys to John O'Neil

The Washington Times

WEDNESDAY, FEBRUARY 8, 1989

WASHINGTON, D.C.

PHONE: 636
SUBSCRIBER SERVICE: 636

Message networks at risk

By Peter Copeland
SCRIPPS HOWARD NEWS SERVICE

The U.S. telecommunications system is becoming increasingly vulnerable to terrorist attack or computer hackers, an expert testified yesterday before a Senate committee.

"The public networks are becoming more vulnerable to serious disruption ... because of the introduction of new technologies," said John McDonald, chairman of a telecommunications committee for the National Academy of Sciences.

"Second, because of economic incentives to cut the costs of normal commercial operation, today's networks are being designed without sufficient attention to emergency preparedness," Mr. McDonald told the Senate Committee on Governmental Affairs.

Mr. McDonald, who also is executive vice president of technology for Contel Corp., said more information is passing through fewer and more vulnerable channels because of new technology such as fiber-optic cables and digital switching.

Also, the dependence on computer software to run complicated telecommunications systems means the systems could be disrupted by computer hackers, Mr. McDonald said.

Mr. McDonald's warnings were disputed, however, by a government official in charge of safeguarding government communications.

"Major disruptions of the nationwide telecommunication networks during a peacetime emergency or disaster would be highly unlikely," said Benham Morriss, deputy manager of the National Communications System, an obscure government agency with almost 100 employees and a \$75 million annual budget.

Mr. Morriss maintained that "the nation's telecommunication networks are diverse, robust and redundant — qualities which make the network as a whole very resilient."

But a former director of the NCS testified that he thought the system was more vulnerable than ever.

Lee Paschall, a retired Air Force officer and NCS director from 1974 to 1978, said the government concentrates on protecting its own communications and not those of the general public.

Committee Chairman John Glenn, Ohio Democrat, said the breakup of the AT&T network into seven regional companies makes it harder for the government to know if the telecommunications system is secure.

"I don't want to play Big Brother," Mr. Glenn said, explaining that the government can advise companies to protect their networks against terrorist attacks, but forcing them to build costly new protection systems could drive them out of business.

PAGE A3

Growing Vulnerability of the Public Switched Networks:



Implications for National Security Emergency Preparedness

NATIONAL RESEARCH COUNCIL

John Francis O'Neil

First Lieutenant
United States Marine Corps

Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness

A Report Prepared by the
Committee on Review of Switching,
Synchronization and Network Control
in National Security Telecommunications

Board on Telecommunications and Computer Applications

Commission on Engineering and Technical Systems

National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. 1989

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, DC 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*, CONTEL Corporation,

PAUL BARAN, METRICOM

FLOYD BECKER, University of Colorado

CULLEN M. CRAIN, The Rand Corporation

HOWARD FRANK, Network Management Inc.

LEWIS E. FRANKS, University of Massachusetts

PAUL E. GREEN, JR., International Business Machines
Corporation

ERIK K. GRIMMELMANN, AT&T Bell Laboratories

E. FLETCHER HASELTON, Teknekron Infoswitch Corporation

AMOS E. JOEL, JR., Executive Consultant

DONALD KUYPER, GTE Operating Group*

RICHARD B. MARSTEN, VITRO Corporation

DAVID L. MILLS, University of Delaware

LEE M. PASCHALL, American Satellite Company (retired)

CASIMIR S. SKRZYPCZAK, NYNEX Corporation

Senior Adviser

JOHN C. WOHLSTETTER, CONTEL Corporation

Staff

WAYNE G. KAY, Study Director

KAREN LAUGHLIN, Administrative Coordinator**

LOIS A. LEAK, Administrative Assistant

*Resigned August 1988.

**Until July 1988.

BOARD ON TELECOMMUNICATIONS AND COMPUTER APPLICATIONS

CHARLES W. STEPHENS, *Chairman*, TRW Electronics & Defense Sector (Retired)

JORDAN J. BARUCH, Jordan Baruch Associates, Incorporated

DANIEL BELL, Harvard University

HERBERT D. BENINGTON, UNISYS Defense Systems

CARL J. CONTI, International Business Machines Corporation

DAVID J. FARBER, University of Pennsylvania

JAMES L. FLANAGAN, AT&T Bell Laboratories

ROBERT Y. HUANG, TRW Space Technology Group (Retired)

JOHN C. McDONALD, CONTEL Corporation

WILLIAM F. MILLER, SRI International

ALAN J. PERLIS, Yale University

HENRY M. RIVERA, Dow, Lohnes and Albertson

ERIC E. SUMNER, AT&T Bell Laboratories

GEORGE L. TURIN, University of California at Berkeley

KEITH W. UNCAPHER, Corporation for National Research Initiatives and University of Southern California

ANDREW J. VITERBI, Qualcomm, Incorporated and University of California at San Diego

WILLIS H. WARE, The RAND Corporation

Staff

JOHN M. RICHARDSON, Director*

RICHARD B. MARSTEN, Director**

ANTHONY M. FORTE, Senior Staff Officer

BENJAMIN J. LEON, Senior Staff Officer

BERNARD J. BENNINGTON, Visiting Fellow

CARLITA M. PERRY, Administrative Associate

KAREN LAUGHLIN, Administrative Coordinator

LOIS A. LEAK, Administrative Assistant

LINDA JOYNER, Administrative Secretary

*Director from January 1988.

**Director until January 1988.

Preface

This report concludes a multifaceted study conducted by the National Research Council's (NRC) Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications. The committee, established at the request of the Manager, National Communications System (NCS), had its first meeting in November 1986. Phase I of the committee's work involved evaluating the NCS Nationwide Emergency Telecommunications Service (NETS), which is one of three programs to improve survivability in national security emergency preparedness (NSEP) telecommunications capabilities mandated by presidential order in National Security Decision Directive NSDD-97. NETS, the largest in scope of the programs, is intended to provide survivable switched voice and data communications. The committee worked on an accelerated schedule during this phase, holding meetings every month. They concluded their work with a formal briefing to the NCS Manager and his staff in April 1987. The committee's interim report, *Nationwide Emergency Telecommunications Service for National Security Telecommunications*, was published in August 1987 and fulfilled Task 1 of the NCS study requirements.

The committee reconvened in September 1987 to address the remaining tasks of reviewing and assessing synchronization, switching, and network control of the public switched network (PSN). The committee found that existing synchronization capabilities are likely

to be adequate to support NSEP telecommunications. An in-depth discussion of Issues in Digital Network Time and Frequency Synchronization is included in this report as Appendix B and fulfills Task 2 of the NCS study requirements. For Task 3 the committee was to review the inventory of switching installations for survivability of switching and control functions after nuclear attack, considering redundancy and alternative connectivity (see Appendix A for the complete Task 3 statement). However, for this task it was implicitly necessary to look to the future evolution of the network rather than merely to examine the current status. The future network is likely to be different from that of today because of changes in regulation, technology, competition, and customer demand. Accordingly, with the concurrence of the Deputy Manager of NCS, this report considers how the network may evolve by the year 2000, the drivers influencing its architecture and topology, and the vulnerabilities it may have.

The committee considered the implications of two opposing trends in network development: (1) a trend, driven by competition, toward the provision of many networks and (2) a trend, driven by economic forces, toward decreasing interoperability and restorability in emergencies.

The intended audience for this report is the NCS Manager and those who provide oversight to him. They include policy-level officials of the Office of the Secretary of Defense, the National Security Council, the Office of Science and Technology Policy, the Office of Management and Budget, and the Congress. The report is also addressed to the providers of public and private telecommunications facilities, to the extent that NSEP telecommunications ultimately depends on their systems.

The committee appreciates the strong support and personal involvement of the NCS staff, especially Benham E. Morriss, Deputy Manager. We are also grateful to all who provided information and insights as to where the networks are likely to be in the year 2000. These estimates were highly valuable in helping the committee understand network trends and their NSEP implications.

The committee was ably supported by the NRC staff and the Director of the Board on Telecommunications and Computer Applications, Dr. John M. Richardson. In particular the committee thanks Wayne G. Kay, Consultant and Study Director, for his personal and professional commitment of excellence to the task. We also praise Karen Laughlin, of the staff, for her outstanding administrative effectiveness on our behalf. We also thank Lois A. Leak and Linda

Joyner, also of the staff, for their invaluable assistance. In addition, I want personally to thank my assistant, John Wohlstetter, for his able contributions. Finally, my personal thanks to each member of the committee for his time, perseverance, and dedication to this important study.

John C. McDonald
Chairman

Contents

EXECUTIVE SUMMARY	1
The Emerging Problem, 1	
Recommendations, 2	
1 INTRODUCTION.....	9
Current Programs, 10	
The Committee's Approach, 10	
Some Conclusions, 11	
Structure of the Report, 14	
References, 15	
2 NATIONAL SECURITY EMERGENCY PREPAREDNESS INITIATIVES TO DATE.....	16
Background, 16	
Commercial Satellite Interconnectivity, 18	
Commercial Network Survivability, 19	
Nationwide Emergency Telecommunications Service, 20	
References, 21	
3 PUBLIC SWITCHED NETWORKS IN THE YEAR 2000...	22
Regulation, 23	
Technology, 23	
Competition, 27	

	Customer Demand, 29	
	Summary, 31	
	References, 31	
4	REGULATION.....	33
	Jurisdiction, 34	
	Open Network Architecture, 35	
	Broadband Services, 37	
	Pricing, 38	
	Bypass, 39	
	Local Exchange Carrier Regulation, 40	
	Additional Nationwide Telecommunications Emergency	
	Service and National Security Emergency	
	Preparedness Considerations, 42	
	References, 45	
5	TECHNOLOGY	46
	Transmission, 47	
	Switching, 51	
	Integrated Circuit Technology, 53	
	Network Management, 55	
	Network Synchronization, 59	
	A Summary of Public Switched Network Vulnerability	
	Trends, 60	
	Recommendations, 63	
	References, 65	
6	COMPETITION	67
	Exchange Telephone Services, 67	
	Cellular Mobile Radio, 68	
	Customer-Premises Equipment, 70	
	Value-Added Networks, 71	
	Databases, 72	
	Cable Television, 73	
	Innovative Services, 74	
	Recommendations, 74	
	References, 78	
7	CUSTOMER DEMAND.....	80
	Basic Technological Assumptions About the Environment	
	in the Year 2000, 80	

User Needs, 81
National Security Emergency Preparedness
 Implications, 87
Recommendation, 87
References, 88

APPENDIXES

A. Statement of Task, 89
B. Issues in Digital Network Time and Frequency
 Synchronization, 91

GLOSSARY 117

Executive Summary

Today it is universally acknowledged that the United States is becoming more and more an information society, and that telecommunications and information networks are essential components of an information society's supporting infrastructure. Networks of the future will be increasingly relied on for a remarkable variety of voice, data, and video services. It is thus of considerable concern that, because of powerful trends in the evolution of the nation's telecommunications and information networks, they are becoming more vulnerable to serious interruptions of service.

THE EMERGING PROBLEM

Specifically, because of changes in regulation, technology, and the interaction between competitive market incentives to cut costs and market-specific customer demand, tomorrow's networks are at greater risk than today's. Regulation is opening major portions of the network to customer control; technologies—notably fiber optics, digital switching, and software control—are driving network assets into fewer, but more critical, network nodes; competition is reducing the incentives of providers to build redundancy into their networks; and customer demand is not stimulating deployment of network assets that are sufficiently robust to cover the full range of national security emergency preparedness (NSEP) contingencies.

While the National Communications System (NCS) has sponsored several valuable national-level programs to address the ability of the nation's networks to support NSEP, the committee believes that there is a set of valid NSEP contingencies that fall outside the traditional view of NSEP and that need to be addressed. Because of the growing reliance of our information society on smoothly functioning telecommunications and information networks, NSEP concerns should include provision for reducing network vulnerabilities to broader economic and social dislocations arising from network disruptions.

Just how vulnerable our networks have become is illustrated by the experiences of 1988: There were three major switching center outages, a large fiber optic cable cut, and several widely reported invasions of information databases by so-called computer hackers. As we become more dependent on networks, the consequences of network failure become greater and the need to reduce network vulnerabilities increases commensurately.

RECOMMENDATIONS

The committee makes the following recommendations to reduce growing network vulnerabilities and thus provide adequate assurance that NSEP needs will be fully supported by the nation's public switched networks.

Recommendation No. 1: Assure Sufficient National Level National Security Emergency Preparedness Resources

In light of society's growing reliance on information and telecommunications networks and the resulting increase in risk to national security emergency preparedness, the National Security Council should review whether the resources available to the National Communications System are sufficient to permit it to fulfill its responsibilities for planning, implementing, and administering programs designed to decrease communications vulnerabilities for national security emergency preparedness users in an environment of proliferating public networks. (Chapter 4)

Government must be able to analyze what network features are necessary for national security. Government must also be able to implement plans and procure services pertinent to national security needs.

In its efforts to date to assure the NSEP capabilities of the public networks the federal government has not sufficiently considered how network capabilities might be enhanced to reduce vulnerabilities to broader economic and social disruption. There is a gap in NSEP oversight: Our committee believes that the government should review whether its existing resources are sufficient to adequately perform expanded NSEP oversight of the proliferating public networks and clarify the appropriate agency missions to address these broader NSEP questions.

Recommendation No. 2: Use More Technology Diversity

Because public network evolution is increasingly being driven by economic considerations, the Nationwide Communications System should ask the National Security Telecommunications Advisory Committee to examine how national security emergency preparedness needs can be met; the National Security Telecommunications Advisory Committee should recommend steps to make critical network nodes more secure, reduce concentration of network traffic, and increase alternate route diversity. (Chapter 5)

Trends in telecommunications and computer technology are leading toward increased central switch routing capacity, increased traffic concentration, and reduced route diversity. High-capacity central office digital switches are already concentrating network traffic at key central network nodes. Virtually all the network trunking capacity will be provided by optical fiber, thus greatly increasing traffic concentration. As optical fibers replace dozens of copper wires or microwave links and as fiber becomes increasingly the transmission medium of choice, network route diversity will be greatly diminished.

Worrisome trends in network technology go beyond loss of route diversity. Network control intelligence is migrating from switching systems into common channel signaling systems. This separated signaling network will be very thin, relying on a small number of large databases; traffic on interexchange networks will be switched via a limited number of signal transfer points, greatly increasing network vulnerability, especially to coordinated attacks on critical network nodes.

Recommendation No. 3: The Nationwide Emergency Telecommunications Service Is Needed

Given that there is no assurance that by the year 2000 enhanced routing capabilities will be ubiquitous in the public networks, the Nationwide Emergency Telecommunications Service is needed now, and its functional equivalent will be needed beyond the year 2000 for national security emergency preparedness purposes. (Chapter 5)

Emerging network capabilities will not provide a substitute for NCS's proposed Nationwide Emergency Telecommunications Service (NETS). Among key new network capabilities the committee examined were the integrated services digital networks (ISDN), switching techniques that use the asynchronous transfer mode, Federal Telecommunications System 2000, and the widespread deployment of very small aperture terminals (VSATs). Neither these nor any other foreseeable emerging technology will, by themselves, ensure adequate fulfillment of the requirements for the proposed NETS. The public networks will lack sufficient capability to provide NSEP unless NETS is deployed.

Recommendation No. 4: Provide Priority Service

As emergency services cannot be provided without prepositioning dedicated network equipment, the National Communications System should ask the Federal Communications Commission to require the industry to deploy the network assets needed to provide priority service for selected users during declared emergencies. (Chapter 4)

Major emergency situations cause overload conditions on the telephone system. These overloads will indiscriminately block calls of emergency personnel who need communications access as well as nonessential callers. Thus, priority service provisions for such selected users as police, firemen, hospitals, and government officials are necessary. Service options should include such techniques as priority dial tone and trunk access, for example.

The committee understands that ample authority already exists for the government to require that industry be permitted to deploy network assets that would support priority service under a

wide range of contingencies. However, without emplacement of adequate network assets in advance, it will not be possible to implement priority plans quickly in event of a crisis.

Recommendation No. 5: Provide Additional Redundancy

Because concentration of network traffic and routing nodes is increasing network vulnerability, additional route diversity and network node diversity should be provided for national security emergency preparedness purposes. (Chapter 5)

Implementing priority access procedures cannot alone ensure the availability of emergency communications. If fire destroys the only central switching office that can route emergency traffic from a given area, or if an earthquake uproots critical optical fiber transmission lines, essential communication linkages will be severed. The increased reliance of the public networks upon a single technology for transmission—optical fiber—is thus a source of great risk to NSEP. These measures will cost money. However, whether users, shareholders, or taxpayers should bear the cost is a matter of public policy that goes beyond the scope of the committee's charter.

Recommendation No. 6: Increase Radio Access Capabilities

Since radio technologies can provide a valuable source of alternative routing in emergencies, the National Communications System should consider how terrestrial and satellite radio transmission can be employed to provide route diversity for national security emergency preparedness purposes; in particular, consideration should be given as to how very small aperture terminals can be used to back up the public switched networks. (Chapter 5)

Advances in radio technology offer great promise for augmenting network route diversity. Cellular mobile radio has enormously expanded available capacity for mobile communications interconnected with the landline switched networks; digital microwave technology is making telephone service economical in hitherto inaccessible rural areas; VSATs are making data distribution by satellite economical and efficient and offer possibilities for economical deployment of widely distributed intelligent network signaling architectures.

Recommendation No. 7: Establish Emergency Plans

As crisis management skills are critical in making emergency assets work effectively, the National Communications System should establish additional emergency plans, tailored to the evolving public networks, that use simulated disaster and recovery scenarios to develop fallback strategies for network use during emergencies. (Chapter 4)

Preparedness requires more than availability of adequate facilities. Emergency personnel must be trained to use the equipment with the speed and efficiency needed to enable adequate discharge of NSEP responsibilities. Large organizations must develop procedures and practice their implementation, adjusting plans as experience with actual disasters dictates. In this regard, experience with recent disasters will help provide a blueprint for developing future contingency plans. Finally, as a truly practical endeavor the NCS should commission the analysis of scenarios that postulate the destruction of a megaswitch and enumerate the steps that would be currently undertaken to restore communications along with the problems that would likely be encountered. These should include estimates of costs, time required to restore communication, the level of the restoration, telecommunications service priority adherence, and network management obstacles.

Recommendation No. 8: Establish Software Security Measures

Since the public networks are increasingly driven by software, the National Communications System should consider how to protect the public network from penetration by hostile users, especially with regard to harmful manipulation of any software embedded within the public networks that is open to customer access for purposes of network management and control. (Chapter 7)

Perhaps the most disturbing of the growing network vulnerabilities is that of contemplated open outside access to network executable code and databases. The desire to open access to the public networks must be counterbalanced by a recognition that the integrity of the public networks must be protected. The growing number of mischievous and hostile penetrations of networked computer systems portends

the possibility of similar penetrations of network switching databases, even though the executable code may be thought to be well protected.

Recommendation No. 9: Exploit Value-Added Networks

Because packet switching techniques are well suited for adaptive routing, the National Communications System should devise ways to exploit the capabilities of the commercial packet-switched, value-added data networks for national security emergency preparedness purposes, including message transmission, electronic mail boxes, and more robust signaling. (Chapter 6)

Another potentially valuable source of public network redundancy is value-added networks. Whereas today's circuit-switched networks were designed almost exclusively to carry voice transmission, the network of the future will be increasingly driven by data transmission needs. A class of networks known as value-added networks (VANs), first introduced in the 1970s, is becoming widely deployed for commercial use. These networks are packet switched rather than circuit switched, that is, they do not tie up a circuit end-to-end, but occupy space only when data are actually being transmitted. VANs offer valuable network routing capabilities if interconnected with the public switched networks. Such signaling capability is superbly suited to alternate routing schemes: Packet switching was originally designed to enable adaptive routing through damaged networks. The committee also notes, however, that making use of VANs to strengthen survivability will only succeed if the other recommendations covering attention to greater redundancy are followed.

Recommendation No. 10: Promote Internetwork Gateways

Because interconnection of the proliferating public networks is essential for national security emergency preparedness, the National Communications System should explore how the capabilities of public and private institutional voice and data networks can be used to provide redundancy; particular attention should be given to how network interoperability can be increased through deployment of gateway architectures. (Chapter 6)

Many large government and commercial private networks are not currently fully interoperable with the public switched networks: They operate according to a different set of protocols and standards. These networks, if fully interconnected with the public networks, could augment NSEP resources. Another impediment to end-to-end interconnectivity is the possibility that many terminal devices will not be entirely compatible with network interface standards.

Recommendation No. 11: Retain Existing Synchronization

As existing network synchronization levels already exceed those required for national security emergency preparedness, no action need be taken to increase the robustness of network synchronization beyond existing standards for normal network operation; designers of terminal devices should engineer them to operate satisfactorily under system synchronization standards. (Chapter 5)

In one respect, that of network synchronization, the existing and prospective network capabilities appear more than sufficient to meet present and future NSEP requirements. The committee examined network synchronization in detail and concluded that the present standards ensure an adequate margin of safety. However, because users have full freedom to connect registered terminal devices to the public networks, it is incumbent upon equipment designers to build units that function properly within existing network synchronization standards.

* * * *

In essence, the vulnerabilities stemming from changes in network regulation, technology, competition, and customer demand are not significantly offset by any countertrend. Robust systems such as NETS will be necessary to enable the government to carry out vital NSEP responsibilities. Civil emergencies will also require enhancements and backup to the capabilities of networks whose architectures are being driven primarily by economic incentives rather than by security concerns. Otherwise, serious losses will threaten governmental, commercial, and personal pursuits.

1

Introduction

The economic, architectural, regulatory, and technological trends during the evolution of the public switched networks to and beyond the year 2000 will create a more fragmented (less unified) network of networks, and the National Communications System and other users of the public switched networks will have to factor this fragmentation into their planning for national security emergency preparedness.

Virtually every segment of the nation depends on reliable communications, and no business or institution could perform its normal functions without the smooth operation of its voice and data communications networks. The committee, after careful study, has concluded that a serious threat to communications infrastructure is developing. Public communications networks are becoming increasingly vulnerable to widespread damage from natural, accidental, capricious, or hostile agents.

The government of the United States must be able to control and direct the allocation and use of its critical national resources in the event of national emergency conditions. This ability to control and direct depends on reliable, survivable communications. The rich fabric of transmission facilities, switches, and embedded technology that makes up the nation's public switched network, now a network

of networks, is the communications resource upon which all levels of government and industry will depend to control and direct resources and assets. This network of networks is viewed as the U.S. nationwide telecommunications network, made up of many common carrier, private, institutional, research, and other networks.

CURRENT PROGRAMS

For the federal government, the Manager of the National Communications System (NCS) has the responsibility to plan the architecture for a survivable communications capability to support the nation's reconstitution in the event of a national emergency (Executive Office of the President, 1984). The responsibility for similar planning in the industrial sector does not exist. For the government's part, considerable effort has been devoted to this undertaking. Three interrelated programs are being implemented that address organization, planning, and implementation of national security emergency preparedness (NSEP) telecommunications.

The programs are the Commercial Satellite Interconnectivity program, the Commercial Network Survivability program, and the Nationwide Emergency Telecommunications Service. These programs are cited in Chapter 2 and are described and analyzed fully in the committee's interim report, which documented the first phase of the committee's overall task to assist the NCS Manager (National Research Council, 1987). The committee wishes, at the outset, to commend the NCS for its diligence in carrying out its mission. NCS is addressing the problems posed by network vulnerabilities to the best of its ability, consistent with its current resources and powers. The committee also commends the National Security Telecommunications Advisory Committee (NSTAC) for bringing together industry and government representatives to address NSEP issues.

However, the telecommunications industry as a whole has not sufficiently addressed survivability or other aspects of assuring system availability (Center for Strategic and International Studies, 1984; *Telecommunications Reports*, 1988).

THE COMMITTEE'S APPROACH

The second phase of the committee's work was to assess the vulnerabilities of the public switched networks to a variety of threats and to review the switching, synchronization, and network control aspects of

surviving network elements. Issues of restoration and reconstitution of communications were also addressed. Two full committee meetings and numerous briefings were devoted solely to assessing whether adequate synchronization capabilities are likely to exist to support NSEP telecommunications restoration and reconstitution after a natural disaster or attack on the country. The committee concluded that the current standards of synchronization do ensure an adequate margin of safety. The committee then turned its attention to the subject of the survivability of network switching and control. It was to take into account redundancy, alternative connectivity, and emerging technologies and then assess the adequacy of switching facilities to permit restoration and reconstitution. Given the proliferation of emerging technologies and a rapidly evolving nationwide network, it was considered desirable to explore a somewhat broader NSEP perspective including circuit, burst, and packet switching as well as the control aspects. Network evolution is of significant importance, particularly since new vulnerabilities are introduced by an open network architecture, new embedded technologies, widely distributed software, and the trend toward customer control of software.

The Deputy Manager of NCS agreed that the committee should examine switching and control in the context of a broader review focused on what the public switched networks might look like in the year 2000 and what the NCS planners may be faced with in fulfilling the President's National Security Decision Directive (NSDD-97). The committee heard presentations from industry network planners, systems architects, technologists, and engineers as well as regulators, manufacturers, academics, network management experts, and individuals from the research and development community. The committee's principal conclusions appear in *italics* below, preceded by brief introductory discussions.

SOME CONCLUSIONS

Since public and private organizations depend critically on networks, significant network failures will cause great economic damage to users and providers and also may disrupt the ability of government to provide basic services, such as health care, law enforcement, and fire protection, as well as national defense.

The committee believes that the consequences of network failure are becoming much greater for both customers and network providers than they were a decade ago.

* * * * *

The growing dependence of the United States on its networks is occurring at a time when they are becoming more vulnerable to wide-scale disruption. This unfortunate situation is emerging because of converging trends in technology, economics, and regulatory practice.

It is becoming increasingly easier to make the public switched networks inoperable.

* * * * *

Among the technology trends that are increasing vulnerability are the development and perfection of fiber optic technology and the advances in digital switching. Optical fibers are able to offer great increases in traffic-carrying capacity when compared to earlier transmission schemes. Consequently, new transmission routes are primarily fiber. While a fiber route is not inherently more vulnerable than alternative methods of landline transmission, fewer fiber routes are needed to meet national capacity requirements.

The power of optical fiber technology is diminishing the number of geographic transmission routes, increasing the concentration of traffic within those routes, reducing the use of other transmission technologies, and restricting spatial diversity. All these changes are resulting in an increase in network vulnerability.

* * * * *

Switching technology has advanced in parallel with transmission technology. Today's digital switches are physically smaller but have substantially greater capacity than earlier electronic switches. They also have the ability to control remote unmanned systems. Therefore, a single switching node may support communications for many tens of thousands of subscribers in multiple communities. Furthermore, each major transmission provider is embarked on an evolutionary path toward reducing costs through centralizing control of its network in fewer switching centers and a small number of signal transfer points.

The evolution of switching technology is resulting in fewer switches, a concentration of control, and thus greater vulnerability of the public switched networks.

* * * * *

At the same time that switches have become more powerful and

physically smaller, the cost of investment capital, labor, and real estate has continued upward and has helped motivate communications providers to consolidate operations into fewer geographic facilities. As a result this trend increases the potential for catastrophic disruption that may be caused by damage to even a single location.

There is a progressive concentration of various traffic in and through single buildings resulting in increasing vulnerability. It is common for the following types of equipment to be in one building: signal transfer points; class 3, 4, and 5 switches; packet switches; mobile telephone switching offices; and private line terminations.

* * * * *

During the period of the committee's study, a fire (May 1988) at an Illinois Bell Telephone Company central office in Hinsdale disrupted communications services for tens of thousands of households and businesses (National Communications System, 1988). The fire affected telephone service and data communications in the public switched network as well as in many private communications networks with facilities routed through the Hinsdale office. Initially thousands of user services were disrupted. Although essential government facilities for air traffic control were rapidly restored, many businesses and most residences did not regain service for up to several weeks. The economic consequences of the failure were widely reported. The Hinsdale situation has three separate components that may need to be differentiated. The first is the accidental fire; little can be done to eliminate such accidents. The second component of concern is the extent of damage caused by the evolution of communications to higher and higher levels of concentration. The third is the economic disruption that can occur as society increasingly relies on the public switched networks.

The committee points to the Hinsdale event as an early warning for the need to broaden the scope of national security emergency preparedness in an information society.

* * * * *

Along with developments in transmission and switching, which concentrate network capacity, the public switched networks are centralizing network database intelligence through improvements in software technology. Software is creating new services for which users need

access to previously masked aspects of network control, management, and operations. At the same time, computer "hackers" have become more sophisticated in using telecommunications networks to penetrate remote computer software.

The public switched networks are increasingly controlled by and dependent on software that will offer open public access to executable code and databases for user configuration of features, a situation that creates vulnerability to damage by "hackers," "viruses," "worms," and "time bombs."

* * * * *

The competitive environment of the past decade has caused a proliferation of networks and network vendors. One would think this proliferation should decrease vulnerability because of the added redundancy provided by multiple networks. However, in practice, there is actually less than meets the eye. Some of these networks traverse the same geographic rights-of-way and are thus vulnerable to the same physical attacks. Further, competitive factors and the large array of technical alternatives have increased incompatibilities in public and private networks, so that it will be difficult to use the surviving assets in one network to back up those of another.

STRUCTURE OF THE REPORT

These vulnerabilities, with appropriate recommendations, were summarized in the Executive Summary. Chapter 2 traces the evolution of NSEP policy from 1979 to the present. It also summarizes the NCS programs and initiatives that address the organizational, planning, and implementing structures for NSEP telecommunications. Chapter 3 presents an overview of the probable evolution of the public switched networks through the year 2000. It discusses the probable effects of the regulatory environment, technology advances, competition, and customer demand. Chapter 4 focuses on the regulatory drivers of the public switched network evolution. Six major areas are investigated. They are (1) expected changes in jurisdictional responsibilities, (2) the trends toward Open Network Architecture, (3) the impact of broadband services regulation, (4) the gradual adoption of market-based pricing for services other than basic voice telephone service, (5) the effects of bypass, and (6) the trend toward deregulation of local exchange carriers. Chapter 5 discusses a number

of technological driving forces, notably fiber optics, digital switching, and customer controlled software, seen to be major influences in the evolving network, and relates their effects to network architecture, services, and vulnerabilities. In Chapter 6 the committee analyzes the impact of competition on the public switched network and relates this subject to NSEP issues. It includes a discussion of the providers of local and interexchange services, cellular mobile radio, customer-premises equipment, value-added networks, electronic databases, cable television, and some innovative services. Chapter 7 looks at a number of user needs that derive from what new technology may offer and would be affordable to a wide customer base. The committee discusses integrated voice, data, and image applications that will likely be available to residential, commercial, and institutional subscribers by the year 2000. It also points out how customer demand for more and better services can amplify network vulnerabilities that may result.

REFERENCES

- Center for Strategic and International Studies. 1984. *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks*. R. H. Wilcox and P. J. Garrity, eds. Washington, D.C.: Georgetown University.
- Executive Office of the President. 1984. *Assignment of National Security and Emergency Preparedness Telecommunications Functions*. Executive Order 12472. Washington, D.C.: U.S. Government Printing Office. April 3.
- National Communications System. 1988. *May 8, 1988 Hinsdale, Illinois Telecommunications Outage*. Washington, D.C.: National Communications System.
- National Research Council. 1987. *Nationwide Emergency Telecommunications Service for National Security Telecommunications*. Washington, D.C.: National Academy Press.
- Telecommunications Reports*. 1988. Ameritech's Weiss says telecommunications policy should be a national priority. November 21.

2

National Security Emergency Preparedness Initiatives to Date

BACKGROUND

The Cuban Missile Crisis of October 1962 brought home to policy makers the importance of communications resources during emergency conditions. Problems encountered during that two-week period led President Kennedy to establish what is now known as the National Communications System (NCS). While few national security communications initiatives were undertaken in the first 15 years, there have been numerous national security emergency preparedness (NSEP) initiatives during the past 10 years. The more important ones are described herein to illustrate progress made and to provide a baseline for future work. In 1979 President Carter issued Presidential Directive 53 (PD 53), a national security telecommunications policy directive that stated that survivable communications is a necessary component of national security (Executive Office of the President, 1979). PD 53 placed heavy reliance on the national telecommunications infrastructure supplied by the common carriers to supply communications for NSEP programs.

The divestiture of Bell System components raised genuine concerns in the national security community about the effect of the breakup on NSEP. In 1982, and responding to such concerns, the divestiture court ordered the establishment of a centralized support

organization to serve as a single point of contact for the NSEP activities of the seven regional companies. The organization, known today as Bell Communications Research (Bellcore), provides staff resources and technical assistance, and serves as an interface between the regional companies and the federal government. In March of 1982 NCS officials met with telecommunications industry leaders to consider approaches for joint industry-government planning for NSEP communications. The result was the establishment of the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order (EO) 12382 (Executive Office of the President, 1982). The purpose of the NSTAC is to advise the President and the Secretary of Defense (who is the Executive Agent for the NCS) on NSEP telecommunications matters.

This action was followed in 1983 by the issuance of National Security Decision Directive (NSDD) 97 (Executive Office of the President, 1983), which replaced PD 53. NSDD 97 stated that the nation's domestic and international telecommunications resources are essential elements of U.S. national security policy and strategy, and that a survivable telecommunications infrastructure able to support national security leadership is a crucial element of U.S. deterrence. It went on to establish a steering group to oversee implementation and assigned specific responsibilities to the Manager of NCS, NSTAC, and federal departments and agencies.

In 1984, EO 12472 consolidated the assignment of NSEP telecommunications functions (Executive Office of the President, 1984). It provided a framework for planning, developing, and exercising federal government NSEP communications measures. It also established a means for providing advice and assistance to state and local governments, private industry, and volunteer organizations regarding their NSEP communications needs.

An early recommendation of the NSTAC was to establish a joint industry government coordinating center to assist in the initiation and restoration of NSEP telecommunications. The National Coordinating Center was established in January 1984 and has operated continuously since that time.

A related, and still ongoing, activity is the establishment of the Telecommunications Service Priority system. Recently approved by the Federal Communications Commission, it provides the regulatory, administrative, and operational system for authorizing and providing priority treatment of NSEP telecommunications services.

Finally, in December 1985, NSDD 201 was issued to ensure the

availability of resources necessary to achieve NSEP telecommunications objectives. This was an important step because it established funding responsibilities. Thus, a number of measures have been established to address the organizational, planning, and implementing structure for NSEP telecommunications. From that structure emerged the first NSEP National-Level Programs, which are described below (Bird, 1987).

COMMERCIAL SATELLITE INTERCONNECTIVITY

The Commercial Satellite Interconnectivity (CSI) program uses surviving C-band commercial satellite resources to augment or reconstitute public switched network (PSN) interswitch trunking in a postattack environment (Williams, 1988). The program offers a major improvement in survivability at a relatively low cost.

There are about 19 C-band satellites that are candidates for use in the postattack environment. Even though commercial satellites are generally thought to be vulnerable to enemy attack, either by jamming or nuclear effects, it is assumed that one or more of these satellites will survive. As far as the desirability of further hardening of satellites against radiation is concerned, assessments that take into account threat, the consequences of loss, the additional weight penalty on the spacecraft, and the additional costs involved have indicated that hardening beyond that already employed would not be warranted. Although the destruction of these satellites is possible, the task is not an easy one. In this case the enemy would have to destroy all 19 satellites. If any single satellite or two were to go intermittently quiet, the enemy's targeting would become extremely difficult. Even if the enemy has a 0.9 probability of destroying any single satellite, the probability of destroying all is only 0.135. At this time there are no known antisatellite weapons (ASATs) that have the ability to destroy a geosynchronous satellite. By contrast, ASATs pose a demonstrated threat at low altitudes.

Various attack modes against geosynchronous satellites have been postulated, but evidence of such a development has been lacking. Among conceivable attacks are the following:

- On-orbit mines
- Command-link seizure, followed by a command causing a catastrophic action by the satellite
- Jamming, a temporary interruption unless sufficient power is used to "burn out" the input circuits of a transponder

- Direct physical attack from earth by missile or some other mechanism designed to "burn out" the solar arrays.

Thus, the probability of destruction of a commercial communications satellite (all at geosynchronous altitude) is very low. An illustrative assumption of 0.9 is perhaps excessively conservative. However, the thesis that the probabilities are such that some will survive, and should be considered in the planning process, is valid even with an excessively conservative assumption at the beginning. Thus, the payoff for parallelism here is significant. From this point of view, the survivability of commercial satellites as a whole may be underestimated.

To use this potential capability, the NCS National-Level Program must add whatever missing pieces are necessary to allow any single surviving satellite to constitute the "patch cords" between the surviving islands of communications after a major attack. In the plan, all the reconstituted spans are patched using T-1 links terminating at 4ESS switches. To implement the plan, the NCS provides the circuit under the CSI program from the common carrier's switch location to the selected satellite "up-link" station location.

Phase I of CSI augments only the American Telephone and Telegraph Company's interexchange carrier network. The program leases standby services. The NCS is initially concentrating on C-band coterminous U.S. (CONUS) earth station facilities, of which there are some 1,000 in the United States. C-band is used because it incorporates end-to-end standardization. All CONUS facilities follow the same frequency plan based on T-1 modems. Twenty T-1 channels fit into a 36-MHz transponder with intermodulation requirements met. Only satellites having encrypted telemetry, tracking, and control will be used by the NCS in accordance with national security guidelines. In Phase I, the NCS is planning to add 75 T-1 equivalent links to the system.

Mobile earth stations are feasible and technically viable. They would have much value but are costly; thus they are a "budget-permitting" issue in the federal government. The use of Ku band is also being studied. However, Ku-band satellite channels will be more difficult to implement because of a nonstandard channel allocation among the different satellites.

COMMERCIAL NETWORK SURVIVABILITY

The Commercial Network Survivability (CNS) program provides a

limited number of links to connect user clusters to access points (Martens, 1987). CNS focuses on connecting isolated clusters of users to surviving portions of the PSN. The CNS may be thought of as providing the local connectivity to a user, whereas the CSI is the long distance network transmission patch. There are two program components: carrier interconnection (CI) and mobile transportable telecommunications (MTT).

The carrier interconnection concept is to improve connectivity between carriers so that damaged facilities can be bypassed. In addition, the use of existing government networks can be used for interconnection to improve the robustness of the PSN for NSEP users. The NCS has such a program under the CNS to demonstrate and implement a Federal Aviation Administration (FAA) and PSN interconnect in the Dallas-Fort Worth area, to be followed by further interconnects in Brockton, Massachusetts and Louisville, Kentucky in 1988 and 1989. Potentially, two FAA locations per month could be added to the program. The FAA-PSN interconnects will require modifications to routing tables, or require new routing tables to reflect the availability of these new connections. The FAA network is a "nailed-up," or dedicated, private line arrangement, which it appears will use in-band signaling transmitted over the FAA microwave system. This interface with the PSN requires software and hardware to accommodate network control, but not through the signal transfer points.

The mobile transportable telecommunications capability augments PSN transmission for NSEP traffic. An early demonstration in the Colorado Springs area used older generation military radios as PSN "pipes" that passed voice and low-data-rate data traffic. The purpose was to evaluate and test system interfaces and verify the MTT concept and capability to support diverse users during adverse conditions. A more comprehensive exercise was conducted in California during October 1987, simulating an earthquake disaster. Transmission quality for voice was satisfactory over six tandem links; 2,400-bits/s data transmission was satisfactory over two links; and 1,200-bits/s data transmission was satisfactory over four links.

NATIONWIDE EMERGENCY TELECOMMUNICATIONS SERVICE

The Nationwide Emergency Telecommunications Service (NETS) is the NCS's major National-Level Program. NETS is intended to

provide selected users with a highly survivable, interagency, switched voice and data telephone service based on a distributed system of call controllers and making use of a nonstandard routing scheme designed to find any available route to a destination. NETS is described and analyzed fully in the previously published report of this committee (National Research Council, 1987).

REFERENCES

- Bird, J. 1987. National level national security emergency preparedness telecommunications. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., December 8.
- Executive Office of the President. 1979. *National Security Telecommunications Policy*. Presidential Directive 53. Washington, D.C.: U.S. Government Printing Office.
- Executive Office of the President. 1982. *President's National Security Telecommunications Advisory Committee*. Executive Order 12382. Washington, D.C.: U.S. Government Printing Office.
- Executive Office of the President. 1983. *National Security Telecommunications Policy*. National Security Decision Directive 97. Washington, D.C.: U.S. Government Printing Office.
- Executive Office of the President. 1984. *Assignment of National Security and Emergency Preparedness Telecommunications Functions*. Executive Order 12472. Washington, D.C.: U.S. Government Printing Office.
- Martens, W. 1987. Commercial network survivability. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., December 8.
- National Research Council. 1987. *Nationwide Emergency Telecommunications Service for National Security Telecommunications*. Washington, D.C.: National Academy Press.
- Williams, L. 1988. National Communications System commercial satellite interconnect—sites and capabilities. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., January 20.

3

Public Switched Networks in the Year 2000

The public switched networks (PSN) are rapidly being transformed by the confluence of changing regulation, technology, competition, and customer demand. The committee's earlier report (National Research Council, 1987) defined the public switched networks as a national "network of networks" that are interconnected and provide voice and data transmission throughout the United States. (There are numerous private voice and data networks that are linked to the public networks but are not always interoperable with them.)

The American Telephone and Telegraph Company (AT&T) divestiture and the introduction of competition into discrete equipment and transmission markets coincided with the advent of economically available fiber optic transmission, common channel signaling, and digital switching techniques. Together, these factors have stimulated customer demand for new services that are permissible by regulation and possible through technology. These forces will continue to dominate network evolution. Nowhere on the horizon do there exist comparable counterforces to reverse that evolution; although its specifics are not all predictable, its general direction is evident.

Of course, all these influences interact. Regulation was reduced deliberately to stimulate competition, promote technological innovation, and lower prices so as to increase customer demand. Technology is an important basis of competition, and it creates demand as well by making services both possible and affordable. Competition spurs

new technology and expands demand on the basis of improved product and price. Ideally, revenues from increased demand are fed back into research and development to create new technology.

This chapter presents an overview of the probable evolution of the public networks to the year 2000. Separate sections are devoted to the impacts of regulation, technology, competition, and customer demand. These topics are then addressed separately in greater detail in another chapter, which supports the committee's conclusions and presents associated recommendations.

REGULATION

By the year 2000, most of the existing legal and regulatory barriers to entry, which chiefly restrict exchange carriers, will probably have been removed. Only local exchange basic voice service for the small customer is likely to remain a monopoly service in any significant measure. Competition will reach the large-customer market for local exchange carriage, and open entry will extend into video markets as well as those of voice and data.

Thus, the fundamental regulatory principles governing the public networks through the year 2000 will remain the same as today. Regulators will permit open entry where market conditions appear capable of supporting competition. They will press for timely deployment of an Open Network Architecture (ONA) to afford all competitors equal access to the customer. Carriers will be allowed increasingly flexible tariffs to price competitive services closer to cost. Rate-of-return regulation may largely be phased out. Ultimately, there will be a merging of the regulatory treatment for voice, data, and video carriage as technology permits installation of enough network traffic capacity to accommodate multiple providers on equal terms.

TECHNOLOGY

Trends in technology can broadly be grouped into transmission modes, switching, and network technologies.

Transmission Modes

The dominant force in telecommunications transmission throughout the 1990s will be the widespread deployment of optical fiber. By the mid-1990s virtually all the trunk portions of the public networks will be fiber; but fiber will be introduced only gradually into the local

loop (the feeder and distribution portions of the network). Although competition on trunk routes will add some network route redundancy, the lack of widespread competition on feeder and distribution routes and the limited availability of access tandem switches (see below) will operate to limit the benefits of trunk route diversity.

Historically, transmission technology deployment in the public networks has been diverse, that is, copper pairs, coaxial cable, microwave radio, satellites, and even waveguide. The current trend is toward consolidation of network transmission assets into optical fiber. Fiber routes will "prune" the network by aggregating much greater traffic loads in fewer lines and routes. Another essential factor will encourage concentration of fiber traffic in physically contiguous geographic routes: the high cost of obtaining new rights-of-way.

Thus, the dominance of fiber in long haul network transmission means that the 1990s public switched network transmission will become increasingly reliant on the survivability of a single transmission mode, namely, fiber. Dependence on any single transmission mode tends to increase network vulnerability to damage.

Radio will become the transmission medium of choice in areas where emplacement of fiber is economically prohibitive (Stanley, 1988). If they are deployed widely, digital terrestrial microwave, cellular mobile radio, and portable personal communication systems will become significant alternative transmission modes. However, some number of terrestrial microwave routes track closely the rights-of-way used for coaxial and fiber cable routes. Such close physical proximity of alternate transmission mode routes limits the gain in network survivability that physical route diversity would otherwise provide within the public networks.

Satellites will be supplanted by optical fiber for voice service. However, satellites will remain the medium of choice for broadcasting, at least until fiber reaches most residences, sometime in the twenty-first century. This migration to fiber is largely due to its high quality, exceptional bandwidth potential, and freedom from the delay characteristics of satellite transmission, combined with its economic advantages for high-density communications paths. In addition, the cost per circuit mile favors the optical fiber mode. Other niche applications for satellites will include remote location, mobile access, navigation, and point-to-multipoint data. A potentially significant augmentation of network redundancy is very small aperture satellite (VSAT) technology, which can provide physically separate transmission backup. While cellular radio adds voice redundancy,

VSATs provide data transmission redundancy, with some projected to provide data, voice, and video capabilities by the year 2000.

Switching

Evolution in central switching is being driven by several conflicting trends. Very large capacity wire centers (for example, Hinsdale, Illinois) have been built to house "super switches," which act as massive connectivity nodes and control hubs for remote terminals. These hubs will control switching for substantial amounts of traffic. At the lower network echelons, more and more remote switches are being deployed in rural areas to aggregate traffic from small communities into the hub.

There is a second simultaneous trend and countertrend in switching. Within the public networks, network intelligence is being concentrated into fewer, centralized software databases, connected by signal transfer points (STPs). Distributed customer-premises switching will also grow. The public networks in the year 2000 will rely on both central-office and premises-based network architectures. To the extent that premises-based switching prevails, alternating current (AC) power generation will become the responsibility of the customer rather than the network provider. As a result, network reliability will no longer be based only on physical redundancy and diversity, but will also depend on the reliability of the electric utilities as the major source of electric power.

Switching technology will be more service specific by the year 2000. For voice transmission, electromechanical switching will be almost completely removed from the local and tandem portions of the public networks with digital time division (DTD) switching taking its place. About 50 percent of the local offices will also be on DTD. Dynamic nonhierarchical routing (DNHR) will be common. For data, switching will be by virtual circuits or packet networks. As broadband services are introduced, a new era of space division switching will be opened. Eventually, though not likely by 2000, optical or photonic switching may be employed with video capabilities.

Network Technologies

Nationwide internetworking will be complicated by the proliferation of private networks. Software-defined virtual private networks will interconnect fully with the public networks. However, physically

separate private links, especially those dedicated to data carriage, will not always prove fully interoperable with the PSN. With appropriate National Communications System planning those packet networks that are interoperable with the public networks could provide robust signaling and routing augmentation.

Signaling

By the mid-1990s, most interswitch signaling will be by common channel signaling (CCS) with Signaling System No. 7 (SS7) as the method of choice. SS7 is fundamental to the integrated services digital network (ISDN) concept, and SS7 software will be programmed to facilitate customer control of network services and to enhance network flexibility via more dynamic nonhierarchical routing.

Network Control

Software is already driving the evolution of network control. The replacement of hardware-based network control with software-driven network intelligence has opened the network and given the user more service options. Coupled with control intelligence owned by the customer and located on the customer's premises, network software will permit the transfer of effective control over many network service-oriented functions from the network provider to the customer. Remote databases will be accessible to customers who wish to reconfigure their networks. Software-defined virtual networks, already introduced for large customers, will be available for many medium and small customers.

Network Standards

Competition in terminal equipment, the AT&T divestiture, and regulatory rules mandating equal network access to providers of information services have led to a new need for effective network standards. While standards issues are being addressed today in government-industry forums, the trends at this writing augur for less ubiquity. There is a growing proliferation of options within given standards, and standards are less likely in today's environment to win industry adoption during the market lifetime of a product or service.

Prior to divestiture, the Bell System, for all practical purposes, set industry standards. Today, network standards are more a product of negotiation among competitors, both large and small, in industry

forums. As a result, telephone network standards could more and more come to resemble the computer industry's "protocol zoo," that is, a plethora of piecemeal network configurations.

Further, the abundance of options produced by individual manufacturers suggests that there is less guarantee, within a given standard, that their products will interface with other products designed to the same standards. The committee notes that multiple options within standards have contributed to nullifying interoperability goals. While this could be true to some extent, more recent standards, as, for example, for ISDNs, are meant to be fully implemented or designed to allow automatic adaption to a variety of switches or subsets. The options allow them to be tailored, on the user side, for various applications and equipment, thereby increasing their acceptability. The objective of newer standards is to be applicable to hundreds of millions of terminals so that large-scale integrated circuits, incorporating all options, are practical.

Although industry forums have made progress in setting standards, the process of developing them has become so lengthy that, as indicated above, adoption of a final standard has sometimes occurred only after the product is no longer state of the art in the marketplace.

COMPETITION

By the mid-1980s, most domestic telecommunications markets had been opened to competition. Competition drives suppliers of equipment and services to meet customer demand as efficiently (that is, as economically) as possible. The driving forces behind the evolution of competitive telecommunications markets have been business and government demand for data transmission and data processing services. While data transmission represents roughly 20 percent of the total demand for telecommunications service, revenues from data are expected to increase more than for basic voice transmission. Hence market evolution will be determined largely by data demand.

The effects of competition are visible in many areas of telecommunications. Local exchange carriers compete with interexchange carriers from business and government networks that partially or totally bypass the public networks. Customized tariffs are becoming a major tool for attracting business customers. Bypass "overbuild" networks give customers the means to manage their network services (Jackson, 1988). Exchange carrier network services lagged in the early 1980s because of regulatory constraints on the manner in which

carriers could employ centralized network intelligence to offer both competitive and basic services, but these regulatory constraints have been relaxed.

Competition in cellular mobile radio has stimulated the growth of cellular "super systems" centered in metropolitan hubs and ringed by smaller satellite communities. Vigorous demand for cellular service, coupled with limited spectrum availability, is driving cellular systems toward digital cellular technology, which will substantially increase channel capacity. Cellular providers are dominated by larger entities, as economies of scale enable larger companies to build cellular mobile switching nodes more efficiently.

Video services competition is increasing. Already, video service is more ubiquitous than basic telephone service: About 98 percent of U.S. households have broadcast television, while only 93 percent have telephone service (Solomon, 1988). Cable television is now the principal agent of video signal distribution into the U.S. home: Over 50 percent of domestic households receive their television signals via coaxial cable, and over 80 percent have access to cable service. Another potential major pipeline for video transmission into the home is via telephone line; currently, federal law limits telephone companies to offering cable service outside their franchise service areas (except for narrow exceptions applicable to sparsely populated areas).

Already, the Federal Communications Commission is weighing whether to recommend to Congress that telephone companies be allowed to provide video service inside their serving areas. By the year 2000 it is likely that telephone companies will be permitted to offer video dial tone; whether they will also be allowed to offer program content is unclear at this writing. A major factor in making telephone company entry into video likely is that telephone companies are leaders in the installation of optical fiber, a medium whose unmatched signal quality makes it superbly suited to transmission of improved definition and high-definition television formats.

The impact of competition has been most evident in the extraordinary proliferation of different brands of customer-premises equipment (CPE). The great variety of equipment available has spurred customizing of business services. Also, premises-based signaling has driven value-added data network applications.

Today's network is also a repository for hundreds of information services, accessible via telephone line linkage to remote databases. Such services require that the customer possess intelligent CPE or a

personal computer in order to engage in an interactive data dialogue with the databases.

Competition will spur deployment of new innovative customized services. Favored applications will include network control and management, business database management, and customized consumer services, for example, custom local area signaling services, which allow residential customers to obtain centrally delivered network services hitherto economically available only to business customers (Wallace, 1988).

On balance, it appears that competition will have a detrimental impact on national security emergency preparedness (NSEP). While service offerings have proliferated, network interoperability has been diminished by widespread deployment of customized nonstandard network architectures. Many private data networks, both circuit and packet switched, are not fully interoperable with the public switched networks. Thus, as sources of potential network redundancy they are extremely limited, unless linked to the public networks by gateway architectures. Further, reliance on centralized databases to provide network services economically makes the network vulnerable to users who access them to damage or destroy them (Atkinson, 1988). Such harmful access capability is especially worrisome because the network is becoming increasingly dependent on software-based services. Cellular mobile radio, however, has potentially significant capabilities for public network redundancy as cellular systems are deployed in smaller metropolitan and rural markets.

CUSTOMER DEMAND

Numerous publicly available sources have exhaustively documented the variety of service offerings that are expected to become widely available by the year 2000—indeed, many of these services have already been introduced into small market segments (Huber, 1987). In addition to basic voice service, customers will have economic access to hundreds of data services and enhanced voice storage and retrieval services. The data services will include both transport and access to information sources. Advanced video services, such as improved and high-definition television and high-resolution facsimile, will also be used by market leaders by the year 2000.

The customer demand driving the introduction of these services is influencing the public networks in several critical ways. First, the nature of user reliance on the network is undergoing fundamental

change. Historically, users viewed the public networks almost exclusively as a means of voice communication, but business users rely increasingly on the public networks as links to connect a wide variety of computers that are becoming vital to their business operations.

Thus, while today's network usage is still predominantly voice service, in the year 2000 usage will be driven primarily by the data services required to function in the information age. Among the data services that businesses rely on are remote database access, real-time links between facilities, and financial transaction capability. For such users, loss of transmission links means serious economic loss from the disruption of their business affairs.

Video usage will be greater than today. Eventually telephone companies will enter the video marketplace, but residential penetration will be modest at best by the year 2000. (Ultimately, when video is ubiquitous, its revenues may dominate the home marketplace, and residential demand will become video driven as well as voice driven.)

A second feature of the evolving public networks is that more of the intelligence that delivers network services to the customer will reside in equipment located on the customer's premises. This is particularly true for business users. Residential users, unless they have personal computers, will continue to rely on centralized network intelligence. Premises-based intelligence will add flexibility to network usage. However, distributed intelligence is encouraging a proliferation of private networks bypassing the public ones. This tends to siphon off revenues from the public network exchange carriers and to impair their ability to provide economical services. Business users will not wait to obtain needed services from the public networks: If they cannot obtain necessary services there, they will build their own private networks.

From the standpoint of NSEP, private bypass networks, if physically separate from the public networks like VSATs, would add to network redundancy. Private networks configured from public networks resources would not do so. For example, virtual networks merely allocate public network capacity dynamically to guarantee bandwidth to the customer. Some links dedicated to private users may simply share space in a physical cable that also carries circuits dedicated to the public network.

SUMMARY

The public networks are evolving rapidly under the pressures of regulatory and technological change and pursuant to the economics of competition and commercial customer demand. By the year 2000, the public networks will be a repository of flexible, powerful technologies. Lightwave (fiber) will be the transmission medium of choice. Digital techniques will dominate both transmission and switching architectures. Radio technologies will offer route diversity. Signaling within the public networks—and in private ones as well—will be software driven and subject to customer control for many functions. Data services, as prime business revenue sources, will drive network evolution. Video services ultimately will offer, via residential revenues, an avenue for deployment of broadband architectures, but these will not be widespread prior to the twenty-first century.

But, while customers will have a diversity of customized services from which to choose, and while technological innovation will continue, network evolution will not be well matched to NSEP needs unless changes are made. Proliferating architectures and interfaces, limited redundancy, and the absence of entities with full end-to-end responsibility for network design and maintenance make it highly desirable that planners with NSEP responsibility take steps to require augmentation of the assets of the public networks. Without augmentation of public network assets the government cannot be confident that its vital NSEP needs will be fully available from the public networks.

Chapters 4 through 7 describe in greater detail how regulation, technology, competition, and customer demand will drive the evolution of the public switched networks through the year 2000.

REFERENCES

- Atkinson, R. 1988. Where in blazes is security. *Communications Week* (August 8).
- Huber, P. W. 1987. *The Geodesic Network: 1987 Report on Competition in the Telephone Industry*. Washington, D.C.: U.S. Government Printing Office.
- Jackson, C. 1988. Telecommunications—an industry watcher's perspective. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., January 19.
- National Research Council. 1987. *Nationwide Emergency Telecommunications Service for National Security Telecommunications*. Washington, D.C.: National Academy Press.

- Solomon, R. J. 1988. Planning for uncertain futures: The utility of a general purpose broadband network. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., March 15.
- Stanley, T. 1988. Technical and spectrum developments for future telecommunications. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., January 19.
- Wallace, L. 1988. Perspectives on testing, restoration, and network management. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., March 16.

4

Regulation

As indicated earlier, regulation is one of several forces that will drive the evolution of the public switched networks for the remainder of the twentieth century. The impact of regulation on network evolution has already been dramatic (Huber, 1988). The divestiture of elements of the American Telephone and Telegraph Company (AT&T) and the introduction of competition into segmented telecommunications markets have transformed what was originally a single integrated nationwide network into a "network of networks." While specific forecasts are hazardous, enough has transpired in the past two decades to allow a reasonable projection of the general direction of telecommunications regulation. Landmark rulings already made, although subject to modifications as circumstances may dictate, will not be completely or even substantially reversed.

In particular, divestiture is irreversible. The integrated Bell System no longer exists, and its component parts have undergone organizational transformations that preclude reassembly of the original entity, even assuming that such a policy decision were made and could lawfully be implemented. Corporate goals have changed: Companies that formerly perceived themselves as passive providers of common carriage now regard themselves as active marketers of telecommunications and information services. In the predivestiture environment, the Bell System supplied end-to-end monopoly service and offered non-Bell companies liberal access to the research of Bell

Laboratories. In the evolving competitive marketplace, and with the expiration on 1 January 1989 of the 1956 consent decree's mandatory licensing of Bell patents, some of AT&T's research is expected to shift toward applied rather than basic areas. While the laboratories will no doubt seek to address security needs, applied research leads to greater emphasis on commercial products, and those products needed for national security emergency preparedness (NSEP) that are not commercially viable might receive less attention. The research support organization for the divested operating companies, Bell Communications Research (Bellcore), is also expected to emphasize applied research. The products and services developed will be increasingly market oriented.

In the remainder of the twentieth century, the chief regulatory drivers of public network evolution will be (1) expected changes in jurisdictional responsibilities; (2) the evolution of Open Network Architecture (ONA); (3) the nature of broadband services regulation, that is, of cable television and advanced video services; (4) the gradual adoption of market-based pricing for services other than basic voice telephone service; (5) the incentive for bypass of the public switched networks; and (6) the evolution of regulation of local exchange carriers. Each of these is discussed in turn, with observations concerning their impact on NSEP planning and requirements.

JURISDICTION

Background

Today, authority for making the rules governing the providers of telecommunications is divided among the Federal Communications Commission (FCC), the AT&T divestiture court, the Congress, and the state public utility commissions (PUCs). The main jurisdictional uncertainty is what authority, if any, will be retained by the divestiture court in the year 2000. The court has established as a prerequisite to ending its superintendence over the Regional Bell Operating Companies (RBOCs) the introduction of genuine competition in the local loop, that is, competition sufficient to make available to residential subscribers meaningful alternatives to obtaining basic telephone service from their local exchange carrier. Potential candidates for providing local loop alternatives are cellular mobile radio and the introduction of optical fiber into the local loop.

In terms of federal-state jurisdictional prerogatives, the past decade has seen the growth of a partnership—not without sharp

disputes—between the FCC and the state PUCs, via increasing FCC reliance on Federal-State Joint Boards to resolve issues with significant interjurisdictional ramifications. Initial blanket state PUC resistance to federal deregulatory initiatives has been replaced by a search for compromises that will preserve the integrity of state regulation over the reasonableness of rates and conditions of service while permitting a gradual shift toward pricing policies more closely related to the actual cost of providing each specific service.

Congressional supervision of the FCC's policies will influence the nature and timing of deregulation, but no legislative reversal of the overall direction of domestic telecommunications policy is likely.

In sum, by the year 2000 jurisdictional responsibilities will be less fragmented than at present, especially with regard to regulation of the RBOCs.

National Security Emergency Preparedness Implications

Because jurisdictional responsibility will remain substantially fragmented, NSEP needs may not be adequately met. As NSEP planning requires nationwide integration, the division of jurisdiction underscores the need to implement, in some form, the committee's recommendation to strengthen the existing national-level NSEP resources to oversee planning for public network emergencies.

OPEN NETWORK ARCHITECTURE

Background

The principle of ONA is an accomplished fact. AT&T and the RBOCs have already filed preliminary ONA plans and received tentative approval from the FCC. The goal of ONA is accepted by all: that is, equal, user-transparent access via the public networks to network services provided by network-based and nonnetwork enhanced-service providers. But the specifics of ONA implementation are complex, and any solution must prove acceptable to many competing industry groups. While ultimate agreement on some form of ONA is highly likely, operational definition of the detailed elements of ONA will continue for years, with gradual, element-by-element introduction rather than wholesale implementation, and continual modification as new services become available.

National Security Emergency Preparedness Implications

The focus of governmental inquiry into the deployment of ONA has been to ensure the widest possible user access to network software, in order to afford true equality of interconnection for nonnetwork enhanced-service competitors. Deployment of ONA will have significant impact on the public networks' NSEP capabilities. A positive aspect is that ONA should provide the flexible network intelligence needed to meet NSEP requirements—notably, out-of-band signaling. But ONA could have a serious adverse impact on NSEP:

As network software becomes increasingly accessible, the potential increases for hostile users to disrupt the public switched networks.

Computer hackers might scramble network data. Instead of using hardware-oriented schemes such as "blue box" billing bypass, thieves might access network software databases to alter customer records, such as billing information. Finally, saboteurs might also implant "computer viruses" or "worms" in accessible network software, causing serious damage to network databases and operations (*Communications Week*, 1988; *New York Times*, 1988; *Telephone Engineer and Management*, 1988).

ONA can increase network vulnerability to such disruptions in two ways. First, ONA increases greatly the number of users who have access to network software. In any given universe of users, some will be hostile. By giving more users access to network software, ONA will open the network to additional hostile users. Second, as more levels of network software are made visible to users for purposes of affording parity of network access, users will learn more about the inner workings of the network software, and those with hostile intent will learn more about how to misuse the network.

Network security is the other side of the coin of network access: ease of access makes security difficult; tight security makes access difficult. Somewhere along a continuum, between perfect access with no security and perfect security with no access, an appropriate trade-off must be made. How much security is desirable depends on the value of the assets to be protected, the cost of protecting them, and the importance of affording ease of access.

Ease of access to network software is the essential for ONA, but ease of access for legitimate users means equal ease of access for hostile ones. Given that the nationwide telephone network and associated databases are a vital national asset, government policy

makers should take care to ensure that security concerns are reflected in the evolution of ONA. Cost constraints and the need for user-friendly access may preclude maximum protection, but some level of security is clearly needed: It is hard to overstate the dependence of the U.S. economy on a fully functioning telecommunications network infrastructure.

The vulnerability of network software raises an important regulatory issue: What level of network software should be masked against access by users in order to safeguard network integrity? For example, outside users should not have access to executable source code, which drives network operations. Access to databases could be subject to verification of user identification, and other safeguards such as partitioning might be useful. At minimum, the evolution of ONA should reflect security considerations as well as the desire to provide open, equal access for users.

BROADBAND SERVICES

Background

The 1990s will see the convergence of broadband and telecommunications technologies made possible by progress in digital switching and transmission, that is, the "arbitrarily large bandwidth" capacity afforded by the use of fiber's extremely broadband capabilities. At this writing, the FCC is considering modifying the rules that limit telephone company participation in cable television franchises. The existing rules are premised upon the limited bandwidth available to telephone users; the introduction of optical fiber into the local loop will eventually obviate the need to retain the current restrictive rules. Thus, even if the cable rules are not revised in the next year or two, eventual revision is probable. With the bandwidth deliverable via optical fiber access lines, multiple service providers will be able to compete for customers. Telephone company entry would be conditional on their willingness to provide nondiscriminatory access to competitors. At this writing, as indicated earlier, it is not clear if telephone companies would be allowed to provide more than video dial tone.

With the advent of high-definition television (HDTV) sometime in the 1990s, demand for broadband capacity will be stimulated. Regulation will focus on ensuring multiple-provider access to local subscribers. If implemented in conjunction with a broadband ISDN architecture, network connectivity for voice, data, and video will

be significantly enhanced. But broadband penetration of the local loop is not anticipated before the mid-1990s. Even by the year 2000 broadband connectivity will probably be limited to "islands"—selected exchange areas.

National Security Emergency Preparedness Implications

If, eventually, television signals are deliverable to a nationwide majority of the customers via landline networks, some portion of the radio frequency spectrum currently allocated for television broadcast could conceivably be reallocated to other technologies such as cellular, domestic mobile, and paging. Those channels could then become available for radio access for NSEP purposes.

PRICING

Background

Traditional telephone pricing was designed to foster "universal service": basic voice telephone service at rates that virtually all potential subscribers could afford. Telephone service was priced according to "value of service": Each customer paid the same flat rate for the right to access the same universe of subscribers. Because high-volume users such as business or urban subscribers received no volume discounts, the value-of-service pricing model incorporated subsidies for residential and rural users.

With the abandonment of the traditional monopoly environment, its centerpiece, value-of-service pricing, will ultimately be largely supplanted by market pricing. Competition is premised upon the ability to price services at or near actual cost per customer. Because advanced network services will be open to competition, and because policing competition will require identification of costs associated with provision of specific services, price disaggregation will prove necessary for most services available in the marketplace. Transitional mechanisms will be required, but some form of postmonopoly price structure, whether it is the FCC's current "price cap" proposal or some other form, will likely be introduced over the next decade.

Prices will not, however, be precisely matched to costs even by the year 2000. The subsidy to maintain universal access for basic voice telephone service will continue to skew the price of access below its true economic cost for low-volume users. Also, the absence of any universally accepted definitive yardstick for separating joint

and common plant costs of providing inter- and intrastate service will continue to preclude pure cost-based pricing of basic service.

An evolving pricing concept developed by the state PUCs is the "social contract" tariff: In return for guaranteeing low-cost universal basic telephone service, exchange carriers are permitted flexible pricing for other, nonuniversal services. The FCC's "price cap" proposal has similar objectives. While some subsidies will remain in effect where the cost of service is well beyond any price that could reasonably be charged, by the year 2000 price disaggregation should be almost complete and public network services will mostly be offered via usage-sensitive, strategically priced tariffs.

National Security Emergency Preparedness Implications

The redundancy afforded in a monopoly environment, such as duplication of databases, though vitally important for NSEP, is less likely to be available in a cost-disaggregated environment. The cost of carrying excess inventory can impede the ability of a firm to price competitively, and thus carriers have an incentive to avoid excess investment in backup resources.

The Hinsdale, Illinois, disaster illustrates the consequences of inadequate redundancy: to thousands of users, services were disrupted, in some cases for up to several weeks. The prospect of future occurrences is real, and the harm done could be worse next time. In addition to the loss of residential connectivity and injury to businesses dependent on network access, a future occurrence could cause loss of life, if, for example, 911 emergency service is disrupted and medical or police assistance is unavailable.

While full-scale network redundancy is not economically feasible, modest, strategically located redundancy is affordable. Because non-service specific network enhancements are no longer automatically includible in the carrier rate base, an alternative method of financing emergency backup is needed.

BYPASS

Background

There are, as defined by the FCC, two types of bypass: "facilities bypass" and "service bypass." Facilities bypass is the use of facilities that are physically separate from the embedded public network. Examples of such bypass include earth station to satellite to earth

station and point-to-point microwave. Service bypass refers to price-discounted services delivered via the public network, for example, virtual private networks.

The rate and extent of customer migration from the public network will be dictated by the pace of transition to cost-based pricing on that network, and the timing of the introduction of ubiquitous "arbitrarily large bandwidth" at rates that would render bypass uneconomical for those who remain public network users for most of their traffic. If price reformation lags, large users would use the public network primarily as a "carrier of last resort."

The principal deterrent to bypass will be regulatory approval of market-priced virtual private networks. By the year 2000 there will be substantial data traffic carried on private networks, but the bulk of voice traffic will remain on the public network; the impact on carriers will be primarily reflected in carrier revenues. Because most bypassers are expected to retain links to the public network, network connectivity should not be seriously impaired—*provided that the private networks employ protocols and interface gateways that are compatible with public network standards.*

Whether service quality will also be maintained is unclear, as the proliferation of networks and network interface standards may preclude attainment of optimal network service quality. For NSEP purposes, however, connectivity at a threshold level of adequacy is more important than whether service quality meets commercially acceptable standards.

National Security Emergency Preparedness Implications

As private networks proliferate, many with robust packet switching capabilities, they will constitute a resource for augmenting network redundancy. The committee recommends that efforts be made to exploit the capabilities of private networks for message transmission, mail-box storage, and more robust signaling.

LOCAL EXCHANGE CARRIER REGULATION

Background

Market pricing and ubiquitous access to information services will drive competition into the local exchange for most services. Two regulatory issues will be paramount: (1) the extent of the de facto

exclusive local exchange franchise and (2) the definition of what constitutes "universal service."

For market-priced services, carriers will not possess an exclusive franchise. Regulation predicated upon the traditional monopoly service model will gradually be supplanted by more flexible regulation, designed to promote open entry and competition. While "last resort" provider service will remain closely regulated, the remainder of local loop traffic will not be regulated under monopoly rules.

Regarding universal service, many federal and state policy makers feel that in the Information Age the traditional concept of universal service—access to basic voice telephone service—should be expanded to include information services. Such expansion is intended to prevent the social segmentation of society into "information rich" and "information poor" classes. It is unlikely that at the federal level a specific new definition of universal service will be adopted. At the state level, there is likely to be considerable experimentation, with many states adopting, in cooperation with exchange telephone companies, Information Age definitions of universal service. Already, inquiries on advanced network services are under way in New York and Florida, and the California PUC has also expressed interest in the subject.

Another problem in local exchange carrier regulation is ensuring that NSEP personnel have access to the public networks. For example, in June 1988 a power failure at a New England Telephone central office blocked incoming calls for some 35,000 local business and residential customers. A number of area banks closed because of lack of business. Their business operations were so intertwined with the telephone system that when it failed the banks' daily business largely evaporated. Even though the telephone company blocked incoming calls from outside the region, it was reported that local calls were almost impossible to make until late in the day. This led local authorities to scatter police and fire resources strategically throughout the affected area.

As is evident from the above situation, an emergency creates telephone overloads that can block access to whatever remaining capacity exists within the communications system. This in turn can prevent authorities from providing local or even regional emergency services. The committee believes that situations will occur where local authorities are unable to maintain essential services because of the failure of communications services. One solution would be to give

priority communications service to selected users during emergencies that cause massive overloads on the public switched networks.

Several options to accomplish priority service could be made available. For example, access to dial tone is considered critical, because if enough nonessential users are connected to a damaged network, higher priority users can be blocked from access. Also, techniques of "line load control" and "directionalization" have been used in the past to control access to a limited telephone capacity. It appears that such controls are no longer actively maintained. In some states, local laws may prohibit telephone companies from providing priority communications services to designated users.

National Security Emergency Preparedness Implications

Because the mainstay of Nationwide Emergency Telecommunications Service (NETS) and NSEP needs will be voice communications, regulation, by conditioning deregulation on retention of "last-resort" voice, will serve NSEP purposes by maximizing network connectivity. The deployment of information services as universal service adjuncts of basic voice service would enhance the capabilities of the public network and serve NSEP goals. The committee believes that roadblocks to such services must be removed and that facilities should be installed to support priority service where appropriate. Well-meaning laws seeking equal access and treatment may inadvertently be counterproductive in the case of damage to public network assets. It is the committee's understanding that at least one state has a specific prohibition against priority treatment, therefore preventing implementation of line load control.

ADDITIONAL NATIONWIDE EMERGENCY TELECOMMUNICATIONS SERVICE AND NATIONAL SECURITY EMERGENCY PREPAREDNESS CONSIDERATIONS

Changes in regulation have had significant impact on the proposed NETS program. The organizational changes wrought by divestiture and the cost-cutting incentives created by competition make NETS planning more difficult. The existence of multiple-service providers competing in segmented markets will also complicate procurement creativity and flexibility if the assets of a network of networks are to be used to serve NETS purposes effectively.

NSEP concerns are less service-specific, but must cover a broader range of contingencies than the war-oriented scenarios to which the NETS program is addressed. NSEP concerns include network reconstitution in the wake of sabotage, natural disasters, and accidents attributable to human error. As with NETS, the regulatory changes of the past two decades make NSEP management more complicated and NSEP capabilities more problematical. The ultimate NSEP challenge for regulatory policy is to meet nonservice-specific NSEP needs in a service-specific regulatory and marketing environment.

For regulation to serve adequately NSEP purposes, network redundancy and security considerations must be given greater weight in government policymaking. Sound regulatory policy must reflect a multitude of factors. Critical factors include (1) a sensitivity to the vulnerability of software-driven networks, (2) an awareness of diminishing network route diversity and the concomitant need for nonservice-specific redundancy, (3) encouraging the exploitation of advanced technologies, and (4) managing the spectrum in ways that promote network redundancy and survivability (Stanley, 1988).

Based on the foregoing discussion and analysis, the committee makes the following recommendations.

Recommendation: Assure Sufficient National Level National Security Emergency Preparedness Resources

In light of society's growing reliance on information and telecommunications networks and the resulting increase in risk to national security emergency preparedness, the National Security Council should review whether the resources available to the National Communications System are sufficient to permit it to fulfill its responsibilities for planning, implementing, and administering programs designed to decrease communications vulnerabilities for national security emergency preparedness users in an environment of proliferating public networks.

Government must be able to analyze what network features are necessary for national security. Government must also be able to implement plans and procure services pertinent to national security needs. In its efforts to date to evaluate the NSEP capabilities of the public networks, the federal government has not considered how network capabilities might be enhanced to reduce vulnerabilities to

broader economic and social disruption. There is a gap in NSEP oversight: The committee believes that the government should review whether its existing resources are sufficient to adequately perform expanded NSEP oversight of the proliferating public networks and clarify the appropriate agency missions to enable them to address these broader NSEP questions.

Recommendation: Provide Priority Service

As emergency services cannot be provided without prepositioning dedicated network equipment, the National Communications System should ask the Federal Communications Commission to require the industry to deploy the network assets needed to provide priority service for selected users during declared emergencies.

Major emergency situations tend to cause overload conditions on the telephone system. These overloads are nondiscriminatory to telephone users and will equally prevent authorities from accessing the system as they will block nonessential callers. Thus, priority service provisions for selected users as police, firemen, hospitals, and government officials are necessary. Priority service options should include such techniques as guaranteed dial tone, line load control, and directionalization, to name a few. The committee understands that ample authority already exists for the government to require that industry be permitted to deploy network assets that would support NSEP under a wide range of contingencies (*Telecommunications Reports*, 1988). Without emplacement of adequate network assets in advance, it will not be possible to implement NSEP plans in event of a crisis.

Recommendation: Establish Emergency Plans

As crisis management skills are critical in making emergency assets work effectively, the National Communications System should establish additional emergency plans, tailored to the evolving public networks, that use simulated disaster and recovery scenarios to develop fallback strategies for network use during emergencies.

Preparedness requires more than availability of adequate facilities. Emergency personnel must be trained to use the equipment with the speed and efficiency needed to enable adequate discharge of NSEP

responsibilities. Large organizations must develop procedures and practice their implementation, adjusting plans as experience with actual disasters dictates. In this regard, experience with recent disasters will help provide a blueprint for developing future contingency plans. Finally, as a truly practical endeavor the NCS should commission the analysis of scenarios that postulate the destruction of a megaswitch and enumerate the steps that would be currently undertaken to restore communications along with the problems that would likely be encountered, including estimates of costs, time required to restore communications, the level of the restoration, telecommunications service priority adherence, and network management obstacles.

REFERENCES

- Communications Week*. 1988. Virus alters networking. November 14.
- Huber, P. W. 1988. Regulatory and other pressures on network architecture. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., May 19.
- New York Times*. 1988. Breach reported in United States computers. April 18.
- Stanley, T. 1988. Technical and spectrum developments for future telecommunications. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., January 19.
- Telecommunications Reports*. 1988. FCC adopts new telecommunications priority system for national security emergency use. October 31.
- Telephone Engineer and Management*. 1988. Computer virus. December 15.

5

Technology

Historically, the evolution of the public switched networks has, to a significant extent, been driven by the development and deployment of new technologies. Terrestrial transmission has evolved from copper wire pair to coaxial cable to optical fiber cable; radio has evolved from terrestrial microwave to satellite microwave to cellular mobile radio; switching began with mechanical technology, followed by electromechanical, electronic analog, and electronic digital, and optical modes are on the horizon; and computing power was first supplied by vacuum tubes, then transistors, and then successive generations of integrated circuit technology.

The evolution of the public networks to the year 2000 will be marked by further advances in network technology. Optical fiber is becoming the transmission medium of choice; digital switching is becoming the dominant switching technique; and software-based processing, linked to very large scale integrated (VLSI) circuitry, is becoming the preferred technology for network management and control.

The incorporation of these new technologies is making available to network users an economically viable host of new telecommunications and information services, which will give customers more channel capacity, more processing power, and more control over the mix of services they draw from both public switched and private networks. The new technologies make possible the first significant

deployment of broadband networks. Widespread use of real-time, high-speed data networks will develop, whose performance will offer economic advantages to high-volume users (Dvorak, 1987; Langseth, 1987).

But the changes in network architecture and operation brought about by these powerful new technologies will have unintended side effects which, if no adjustments are made, could seriously impair the ability of the public networks to provide the mix of services required to meet national security emergency preparedness (NSEP) goals. The sections that follow present a more detailed picture of how transmission, switching, integrated circuit technology, and network technologies are being deployed in the public networks and will briefly assess the implications of each of these technological trends for NSEP.

TRANSMISSION

Optical Fiber

Background

As copper-based systems become obsolete, the media that will provide transmission in the public networks will be optical fiber, satellite radio, and terrestrial radio. Increasingly, the dominant domestic transmission medium will be optical fiber (Henry, 1988; Solomon, 1988).

Optical fibers, first tested less than 20 years ago, are strands of ultrapure "glass," usually fabricated from a silica-based compound, which guide lightwaves along a transmission path. Transmission is accomplished by modulating the light from a light source (either a light-emitting diode or a laser) and coupling the resulting optical beam into the fiber. At the receiving end, a photo-detector typically performs the first level of demodulation to provide multiplexed electrical output signals. Lasers are the preferred light source, since their narrower light beam and purer spectrum couples more efficiently into the fiber and results in higher overall transmission efficiency.

Fiber transmission provides unequalled channel capacity (bandwidth) and signal quality. Already, commercially available fiber systems can transmit at 1.7 Gbit/s rates, thus supporting over 24,000 voice conversations; systems with twice that capacity are forecast to be operational soon. Fiber has an inherent transmission capacity estimated at 20 THz, or more than 10,000 times existing systems; roughly the capacity of all the voice traffic in the United States at

the busiest hour on the busiest day of the year. Actual transmission capacity on fiber systems is limited not by the carrying capacity of the medium, but by limits on the ability to modulate the transmitting lasers. In this regard, fiber is unlike most other transmission media, whose inherent carrying capacity is less than the modulation capability of the source. Increases in capacity have recently come from wavelength division multiplexing techniques, which combine multiple bit streams on different wavelengths inside the fiber.

Fiber produces superior signal quality because the purity of the glass greatly reduces the attenuation and distortion of the signal as it travels from point to point. A common figure-of-merit is the rate-distance product. Digital fiber research systems have achieved 1,000 (Gbit/s)(km); commercial systems, 1 (Gbit/s)(km). Future advances in reducing attenuation, by development of purer glass compounds made of exotic fluoride-based materials, could enable transoceanic transmission without use of repeaters to amplify the signal.

Fiber is also, in some respects, cheaper to maintain than other transmission media. In addition to its high capacity, the economic attractiveness of fiber transmission is driving its deployment in the public networks. But fiber deployment has complicated the task of powering telecommunications networks. Historically, the telephone company supplied power from a centralized source, not tied to electric utility power. With fiber deployment, and coupled with the widespread deployment of private branch exchange (PBX) and key systems powered on the premises, electrical power is increasingly being provided from the customer's premises, often from the electric utility company.

By 1995, fiber will be the most common mode of transmission in network interoffice trunking systems (that is, the long distance portion of the public switched networks). Additionally, it is becoming cost-effective for deployment in the feeder portions of the network (from the access tandem switch gateways to the local central office). By the mid-1990s it may well become cheaper to install fiber in the "last mile" from the local exchange central switching office to the customer's premises. The prevalence of metropolitan area networks by the year 2000 will mean a much richer fabric of interconnectivity on the scale of 100-km distance or less. In high-density areas, such as the Northeast Corridor, the possibility of improvising new interconnections between many such networks in the case of failure of the long-haul backbones could provide a promising backup capability.

National Security Emergency Preparedness Implications

The increased reliance on optical fiber has led to greater concentration of network traffic in a limited number of trunks and, by supplanting other transmission media, has increased network reliance on a single technology. Simply put, there are fewer transmission lines and fewer alternative transmission routes to act as backup in event of failure. The accidental cut of a single fiber cable in New Jersey in November 1988 took down network capacity by 200,000 conversations per hour. By the year 2000, with higher capacity fiber links, a single cable cut could lose many times that number of calls per hour. The increased dependence of the public networks on power supplied by electric utility adds a new source of network vulnerability: electric power outages (Samuelson, 1988).

Satellite Radio

Background

The principal alternative transmission medium for long distance service has been satellite radio. Transmission is accomplished by sending line-of-sight, microwave radio signals from earth-station antennas to the satellite. Satellites provide highly economical transmission, especially for broadcasting and point to multipoint data transmission, because the cost of transmission does not vary with distance within the footprint (geographic coverage) of a given satellite (Lowndes, 1988). Also, the cost of right-of-way procurements is avoided. Satellites are not considered as desirable as terrestrial links for voice transmission, since the round-trip signal propagation delays of over 250 milliseconds to and from the satellite disturbs some users, even with high-quality echo-suppression processors. On a two-satellite path, user frustration is high, and thus a typical transoceanic call goes by satellite in one direction and via undersea cable on the second path.

Communication satellites can provide significant transmission capacity: The INTELSAT VI satellites will have a capacity of 100,000 voice circuits (compared to 240 circuits for the first INTELSAT satellites of the 1960s). Satellite technology continues to evolve: Earth station antennas only 2 meters in diameter (very small aperture terminals, or VSATs) are being deployed for business data transmission; satellites are using "spot beams" to pinpoint small geographic areas,

enabling frequency re-use within the satellite's coverage area; on-board signal processing permits multibeam control; and power supply enhancements such as nickel-hydrogen batteries have extended the useful life of commercial satellites beyond 10 years. Fiber proliferation notwithstanding, satellites will remain important into the twenty-first century for several applications: broadcasting, remote location, point-to-multipoint data, and a "restoration" backup for transoceanic and terrestrial cable routes.

National Security Emergency Preparedness Implications

Satellites can provide enormously valuable backup for terrestrial systems. Their NSEP value is underscored by the decisions of the National Communications System (NCS) to implement the Commercial Satellite Interconnectivity and Commercial Network Survivability programs. The dominance of fiber as a terrestrial transmission mode makes satellites an especially important source of route diversity.

Terrestrial Radio

Background

Terrestrial radio access is the third major area in which network transmission technology is advancing. The principal types of terrestrial radio are line-of-sight microwave and cellular mobile radio. Other systems, such as tropospheric scatter and meteor burst, perform highly specialized communications functions for the military.

Terrestrial microwave signals are transmitted using radio relay equipment (towers) spaced approximately 30 miles apart. Transmission frequencies range from 400 to 500 MHz up to 23 GHz for digital microwave systems.

Cellular mobile radio systems divide service areas into "cells," which have low-power microwave antennas at their center, with each antenna linked terrestrially to a centralized switching center (mobile telephone switching office, or MTSO), which, in turn, is interconnected with the landline telephone network. Substantial frequency re-use can be achieved in these systems. As mobile users travel from cell to cell, their calls are "handed off" to the next cell they enter, thus freeing the channel in the previous cell. Cellular systems serve hundreds of the country's largest metropolitan areas. Digital

transmission techniques will significantly increase system capacity, perhaps by a factor of four or five.

National Security Emergency Preparedness Implications

Radio access offers potentially significant enhancements to network redundancy. Radio transmission can, in some cases, be considered more robust than terrestrial links because, whereas terrestrial links are vulnerable along the entire length of the transmission line, radio links are vulnerable principally at the transmitting and receiving points. In the aftermath of the recent Hinsdale fire, some users were able to re-establish valuable communications links via radio links—notably via cellular radio and the use of VSATs (National Communications System, 1988).

SWITCHING

Background

Switching technology is marked by two divergent trends: advances in microprocessing technology are driving switching capabilities toward the customer's premises; but the economics of digital switching is driving telephone companies to build large-hub switching centers with huge capacities. The technologies that are providing the impetus for these trends are very-high-performance integrated circuits and highly sophisticated distributed processing technologies.

Integrated circuit technology has progressed at a dizzying pace. As recently as 10 years ago a random access memory chip could store 16 kilobits of data; the current generation of chips can handle 1 million bits. With VLSI chips being supplanted by ultra-large-scale integrated (ULSI) circuit chips, by the year 2000, a 100-million bit chip is expected to be available. Processing memory is becoming considerably less constraining for the system designers. Multimegabit chips with self-healing capabilities, in the form of redundancy on a single chip, have been demonstrated in the laboratories of the chip designers. Semiconductors are now largely fabricated from silicon; eventually gallium arsenide will assume an increasing role because of its inherent speed advantage for digital signal processing applications.

Software and firmware technology has introduced stored-program control into switching systems, for both central and distributed

nodes. Software programs are becoming increasingly complex: central nodes now incorporate up to 10 million lines of code; by the year 2000 as many as 100 million lines of code may be needed to run central megaswitch hubs. Software-driven switching gives great flexibility to network operations and enables customer control of network configuration and operation. It does, however, introduce enormous design and maintenance complexity.

Distributed intelligence is significantly altering the physical topology of the public networks. Megaswitches are being linked to multiple remote switches. Distributed nodes serve as routing points for network control, linking the central node with remote databases. Central nodes perform specified functions for the distributed nodes, thus permitting economical deployment of the remote nodes.

The dependence of remote nodes on central hubs is analogous to that of computer workstations "slaved" to a central mainframe processor: Without stand-alone capability, the remote switches will fail if the host does. Fortunately, the remote switches at Hinsdale had some stand-alone capability, so some connectivity was retained after the fire. One example of a total dependence of remote nodes on a central processor is that of cellular "super systems," in which the centralized MTSSO supplies essential network functions.

Both the megacentralization and dispersal trends in switching will almost certainly continue in the networks of the year 2000, with neither trend having emerged as dominant.

Another way in which the dominance of digital switching techniques will influence the evolution of both public and private networks is in the increasing use of packet-switched networks. Whereas the traditional circuit-switched call occupies a specific transmission link for the duration of the call, packet switching techniques permit multiple calls to alternate in using the same communication channel; thus, channel usage is more efficient, especially for data calls. Packet networks will provide signaling capabilities needed for implementation of advanced digital networks, such as the integrated services digital networks (ISDN). Packet networks also enhance adaptive routing capabilities, which are predicated upon sophisticated signaling capabilities for which packet switching techniques are well suited.

Digital switches also provide self-diagnostic capabilities, enabling more rapid repair of damaged digital nodes. Operators at remote data terminals can examine distant switching nodes and determine which switch module needs to be replaced.

National Security Emergency Preparedness Implications

Enhanced distributed switching capabilities potentially give the networks of the future substantial augmentation in adaptive routing capabilities, which are essential for restoring network connectivity after major damage. But megaswitch nodes will create points of potentially catastrophic failure, and, as a later section of the chapter indicates, the increasing accessibility of network software will provide hackers and saboteurs with opportunities to damage the routing databases. As noted earlier, the vulnerability of large wire centers was graphically illustrated at Hinsdale. Recently a hacker penetrated university databases and even some computers at the National Security Agency.

Furthermore, the validation of software design, for systems of the complexity of the year 2000, is sufficiently difficult so that confirmation of software performance in all network modes and conditions may prove unattainable. This consideration introduces additional uncertainty, particularly under conditions of high network stress.

INTEGRATED CIRCUIT TECHNOLOGY

Background

Very large scale integration continues to stretch the imagination. The realization of 1-million-bit chips today has brought memory costs to the point where software developers consider memory to be free. Additional advantages are realized from VLSI chips that reduce power, increase speed, and reduce the size of the packaged system. The trend of VLSI will certainly be superseded by ultra large scale integration (ULSI), and the 4-million-bit chips now in early development will, as indicated above, reach the 100-million threshold by the year 2000. In the future, memory will undoubtedly be treated as no obstacle, as well as being of minimal cost.

Not only have the semiconductor technologists projected 100-million-bit chips but also other memory technology continues with significant jumps in speed and reduction in size. Both in optics and in magnetics, the densities continue to increase. At the moment, the projections point to no limitations that will hinder a system developed for deployment in the year 2000.

VLSI technology has made possible the super-microprocessor chip. Not only do the advanced micros affect data processing, but they also bring today's central office control into the single-chip

distributed switch control of tomorrow. The speed, power, and size factors completely change the concept of telecommunications system architectures for the year 2000.

A by-product of 100-Mbit chips will be multi-microprocessors with voting or automatic switchover between processors upon failure. In addition, the multi-megabit memory chip also allows multiredundancy in memories themselves. Thus, the concept of self-healing systems, talked about for the past 20 years, will certainly prove realizable in 2000. With such completely self-recoverable, robust systems, the concerns for unduly short mean times between failure can disappear. The system availability (the ultimate goal) will reach the levels necessary to hold maintenance costs down while providing uninterrupted service.

Digital signal processing (DSP) in a chip has been realized because of VLSI. Previously, filters and other processing of analog signals could only be achieved through relatively large physical components (resistors, capacitors, and inductors). Suddenly, the microprocessor as signal processor places in a chip the speed, power, and size that knows almost no bounds. ULSI will only push DSP still further. Therefore, merging of the analog world with the digital world folds together one of the most natural integrations achieved since the beginning of electronics.

The advent of integrated circuits has brought a true revolution in electronics, which has reached no limitation today that will not be surpassed tomorrow. The future, into the year 2000, holds exactly the same promise. Not only will the merging of analog signal processing and digital signal processing continue but, at the system level, the advanced microprocessors will allow switching and transmission to merge as well. By the year 2000, the trend of today to bring switching and transmission multiplexors together will only weld the switching multiplexor into a practically indistinguishable system element within a fiber network. Lastly, every time that silicon seems to reach a limiting threshold and gallium arsenide will have to take over, silicon again breaks another speed barrier. Whatever the final silicon limitation may be, the integrated circuit will continue to break the necessary barriers for the future.

National Security Emergency Preparedness Implications

Without hesitation it can be said that the semiconductor technology will meet any system requirement for the year 2000.

NETWORK MANAGEMENT

Background

Software Control

Computer control (stored-program control) is the dominant control technique for all electronic switching systems, including PBXs, in the U.S. networks. Furthermore, most terminal devices, from computers to feature telephones, use microprocessors. Whether large switching systems or small chips, software constitutes the breath that brings the equipment (hardware) to life. Unlike biological systems, the memory may be reloaded to make the equipment perform differently. The different sequences of instructions form programs that must be written and processed before the equipment may be activated. This process is time consuming and costly. While one may always hope that an invention or creative stroke of genius will alter this process, there is none currently on the technology horizon.

The variety of stored program devices and systems is ever increasing. They are programmed in at least a dozen different high- and low-level languages. There is no unanimity among designers as to the best language or operating system. One cannot predict what one is to encounter in a given installation. This means that making universal changes in programmed devices is ever increasing in difficulty.

The greatly increased reliance of the network on software to control network operations is a worrisome trend. As indicated above, large switches have software programs of up to 10 million lines of code, and massive databases used for network control result in concentration of network software assets. Further, the Federal Communications Commission has mandated that the Regional Bell Operating Companies provide Open Network Architecture (ONA) to enable nonnetwork-based providers to compete with the Bell Companies on an equal footing in competitive telecommunications markets. As noted in Chapter 4, while that purpose is laudable, the practical consequence of opening network software to outside access is a reduction in network security. Here again it is a mistake to view network assets solely in terms of their economic role and value; our public networks also have security and emergency capabilities that are critical to our national welfare and, indeed, to our very survival.

ONA will, to be sure, confer real benefits: Providers and users

can control their networks by reprogramming network software. Network structures can be dynamically reconfigured, reducing communications costs and providing a valuable tool for businesses with high data transmission requirements.

But as with fiber and digital switches there is a downside: viruses, Trojan horses, worms, and the like.

Signaling

Sophisticated software is also a source of vulnerability in modern network signaling. The purposes of signaling are to route a call through the network and to report on its status—busy, ringing, connected, or terminated. Network signaling today is moving toward what is called “common channel signaling.” Older technology employed multifrequency signaling, such as the tone one hears in touch-tone telephones when dialing. In the old system, signaling was “in-band”—the network signals were carried in the same channel as the communications; the new system is “out-of-band”—signals are software-created and then carried in a common signaling channel, physically separate from the communications channels. This consolidation of the signaling function creates additional vulnerability.

In a typical call with in-band signaling, the calling party signaled to his originating central office by dialing a number. This number was then sent to the next office over a voice channel, which would later be used for the actual conversation. Signaling then proceeded from office to office until the final destination was reached. If the called party's line was busy, a busy signal would be returned over the circuit path of the call to the originating party. Thus, signaling was distributed throughout all the trunks in the network.

Common channel signaling will change that: All signaling takes place over separate data links, which connect the switching systems of the network. In a typical application, the calling party signals his or her central office by using multifrequency touch tone. The central office, employing common signaling, receives the dialed number and the central processor creates a message, which is sent over a separate packet-switched network to the destination central office. If the called party is busy, a busy message is returned over the packet network to the originating central office.

This new signaling technology provides much flexibility in processing and routing calls. However, the concentration of the signaling software and hardware into a subnetwork means greater vulnerability

than if the signaling function were spread throughout entire networks. Without signaling, networks cannot function, so this added vulnerability is a serious matter. For example, the signaling networks of domestic interexchange carriers depend on a very limited number of critical packet switching nodes. While those systems can function under failures at single points, they cannot do so under multiple failures.

Another source of software vulnerability arises from a concept called the "intelligent network." These networks employ the packet signaling networks to provide access to remote databases used for offering such services as the national 800 number. Some of the intelligence that would normally reside in a local switching office is now removed and concentrated at a distant point reached by the packet-switched network. There are only a few of these databases, and they are another source of major vulnerability (from accidental or intentional destruction of software data stored in the databases).

Another worrisome prospect for networks increasingly driven by system software is the possibility that a disgruntled employee might invade and damage or destroy executable network source code. This danger will exist even if executable code is masked from outside access. Partitioning or physically separate backup software may be needed to reduce this risk; otherwise, a knowledgeable insider might disable more than one network node by sending (via transmission links) software program alterations from one network node to other nodes.

The enormous proliferation of private networks will not alleviate these problems. Such networks employ the same technologies, and unless they are interconnected and interoperable with the public networks they do not provide much redundancy. Indeed, many of these network lines interconnect with the public networks through hubs like Hinsdale, and often their lines are laid along the same bridges and highways as the public network lines. In any event, private lines between business offices will not help a resident who needs immediate access to 911 service after a central office burns down.

Standards

The public networks have traditionally placed much reliance on the development, implementation, and adherence to standards to ensure interoperability and uniformity of performance. Prior to divestiture,

network standards were generally developed by the Bell System, implemented within the Bell System, and also made available to other telephone companies, which also embraced these de facto standards for the public networks.

In the postdivestiture environment, the telephone industry has embraced a voluntary standards setting mechanism that adheres to and follows the American National Standards Institute (ANSI) due-process principles. The T-1 Committee, sponsored by the Exchange Carrier Standards Association (ECSA), has become the primary standards setting instrument for the public networks. These forums are attended by a broad spectrum of industry participants, but the existence of conflicting interests can make consensus difficult to reach and can result in delay even where consensus is reached.

The computer industry is also putting more effort into the voluntary standards process through ANSI. The X-3 Committee, sponsored by the Computer and Business Equipment Manufacturers Association (CBEMA), along with the Institute of Electrical and Electronics Engineers (IEEE) and the Electronic Industries Association (EIA), all develop voluntary standards for data communications.

Two major trends affecting the entire telecommunications industry can be expected to have a major impact on the traditional role of standards in the evolution and operation for the public networks and for the private networks that may be used in an emergency to bridge breaks in the public network. These two trends are: (1) rapidly evolving, increasingly complex technologies and services and (2) increased competition, which will tax the ability of the existing standards.

In addition, because of the complexity of the technologies and services, the standards that are established may not have sufficient specificity to ensure full interoperability at the actual application level. Although individual public network providers may adhere to a standard, that alone will not guarantee interoperability. In order to alleviate this problem, groups are now being formed to establish conformance tests and provide testing services.

These trends, when coupled with the pressures of the competitive environment, may cause network providers to introduce technologies and services prior to the availability of a fully defined standard. Thus, the delay in setting narrow-band ISDN standards has retarded ISDN deployment and stimulated deployment of T-1 and other digital architectures (Buckley, 1989). However, the conformance testing

programs should make these problems short lived once they are detected.

National Security Emergency Preparedness Implications

As indicated above, the evolution of network management from circuit- to packet-switched architectures has the potential of significantly enhancing adaptation capabilities, but customer access to network software, the concentration of network databases, and the thinness of packet networks will create additional system vulnerabilities in the public networks. The deterioration of network interoperability resulting from standards degradation is, additionally, a matter of serious concern from a NSEP standpoint.

NETWORK SYNCHRONIZATION

Background

With an increasing number of carriers deploying digital networks, the public network configuration is evolving toward a set of separate islands, each having their own means for accessing and distributing a primary frequency reference. The islands will typically use a navigational system, such as Long-Range Navigation System-C (LORAN-C), for a timing source. As a backup facility, most islands will be equipped with cesium clocks having a 0.5×10^{-11} accuracy. The LORAN-C system coverage is expected to be expanded and will remain operational until well after the year 2000, at which time other navigational systems, such as the Global Positioning System (GPS), will be available to provide equal or better frequency references for network synchronization.

National Security Emergency Preparedness Implications

The trend of partitioning into separate timing islands has a beneficial effect on NSEP goals. Each island distributes timing over redundant paths, and each path has a limited number of nodes so that buildup of timing error is minimized.

It is expected that network timing parameters, such as number of slips per day, probability of reframe events, and so on, will tend to become standardized. Applications with especially stringent timing requirements, such as encrypted voice or video messages, will

bear the burden of design to accommodate the standardized network timing-error characteristics. If certain future applications are developed that must operate with higher precision timing references, there is the possibility that network timing recovery and distribution equipment could gradually be enhanced by adding more redundant timing sources and by increasing buffer sizes so that the rate of timing slips is reduced to required values. An in-depth discussion of this subject is given in Appendix B.

As a result of this analysis, the committee reaches the following conclusion.

No significant synchronization timing issues for national security emergency preparedness appear to exist, because timing is set by the connected surviving access tandem.

A SUMMARY OF PUBLIC SWITCHED NETWORK VULNERABILITY TRENDS

Among the technology trends that are increasing network vulnerability are the development and perfection of fiber optic technology, the advances in digital switching, and the reliance on software for network control. Optical fibers are able to offer great increases in traffic carrying capacity when compared to earlier transmission schemes. Consequently, new transmission routes are primarily fiber and, while a fiber route is not inherently more vulnerable than alternative land-line transmission methods, fewer fiber routes are needed to meet capacity requirements.

The power of optical fiber technology is diminishing the number of geographic transmission routes, increasing the concentration of traffic within those routes, reducing the use of other transmission technologies, and restricting spatial diversity. All these changes are resulting in an increase in network vulnerability.

Switching technology has advanced in parallel with transmission technology. Today's digital switches are physically smaller but have substantially greater capacity than earlier electronic switches. They also have the ability to control remote unmanned systems. Therefore, a single switching node may support communications for many tens of thousands of subscribers. Furthermore, each major transmission provider is embarked on an evolutionary path toward centralizing

control of its network in fewer switching centers and a small number of signal transfer points (STPs).

The evolution of switching technology is resulting in fewer switches, a concentration of control, and thus greater vulnerability of the public switched networks.

While switches have become more powerful and physically smaller, the cost of manpower and real estate have continued their upward climb. Consequently, communications providers are consolidating operations into fewer geographic facilities. This trend is also increasing the potential for catastrophic disruption that may be caused by damage to even a single location. Thus, access to critical nodes must be sufficiently restricted so that penetration by either casual or determined saboteurs is made virtually impossible.

There is a progressive concentration of various traffic in and through single buildings resulting in increasing vulnerability. It is common for the following types of equipment to be in one building: signal transfer points; class 3, 4, and 5 switches; packet switches; mobile telephone switching offices; and private line terminations.

Along with developments in transmission and switching that result in greater capacity, the public switched network is gaining greater "intelligence" through improvements in its software technology. This is leading to new services where users have access to previously prohibited aspects of network management and operations. At the same time, computer hackers have become more sophisticated and are more able to penetrate computer software.

The public switched networks are increasingly controlled by and dependent on software that will offer open public access to executable code and databases for user configuration of features, a situation that creates vulnerability to damage by "hackers," "viruses," "worms," and "time bombs."

A significant aspect of the increasing vulnerability of the public networks is the trend toward centralization of network control by each of the major public communications carriers. The American Telephone and Telegraph Company (AT&T) network contains a limited number of STPs (deployed in pairs with each pair consisting of a primary STP and a backup). Other carriers will have even fewer

STPs. The committee notes that destruction of a pair of points will disrupt a carrier's network in an entire geographic region.

The competitive environment will provide backup for some threats, but not for correlated events in which damage is inflicted at several points by an intelligent adversary or by a widespread natural disaster.

This vulnerability to correlated events is a natural product of common channel signaling (CCS). Communications suppliers are moving toward centralization, common control, and consolidation because of the economic realities of the competitive communications world. It is unlikely that companies will act independently in the national interest to increase redundancy (and hence their operating cost) without financial incentives, legislative imperatives, or the ability to recover their additional costs.

Earlier committees of the National Research Council that examined NSEP communications noted the trend in the public networks toward CCS. These committee reports cautioned the NCS that too few signal transfer points would represent an increased potential for vulnerability in the network.

The committee's review of this matter clearly indicates that the trend toward common channel signaling is continuing and is irreversible in the timeframe of concern. Moreover, economics is clearly driving the number of signal transfer points and associated database facilities downward. Thus, the network vulnerability is increasing.

Divestiture and competition have greatly increased the number of separate networks that make up the public networks. AT&T, MCI Communications Corporation, US Sprint Communications Company, and all the Regional Bell Operating Companies (RBOCs) are implementing CCS with STPs and related databases in order to provide new services to more efficiently use their network facilities. If the total can be made interoperable to provide mutual support and backup in an emergency, the public networks will be much more robust and the STP vulnerability somewhat ameliorated.

At present, however, these separate sets of STPs are not fully interoperable and do not provide mutual support. It is not clear if

they can be made to do so. The NCS should examine this possibility very carefully and, if feasible, funds should be appropriated to increase interoperability.

RECOMMENDATIONS

Based on the foregoing discussion and analysis the committee makes the following recommendations.

Recommendation: Use More Technology Diversity

Because public network evolution is increasingly being driven by economic considerations, the National Communications System should ask the National Security Telecommunications Advisory Committee to examine how national security emergency preparedness needs can be met; the National Security Telecommunications Advisory Committee should recommend steps to make critical network nodes more secure, reduce concentration of network traffic, and increase alternate route diversity.

Trends in technology are increasingly concentrating public network assets in a few dominant technologies: fiber, digital switching, and software. The committee finds that these trends could adversely affect NSEP and recommends action to make critical network nodes more secure, reduce the concentration of network traffic, and examine ways to provide more diversity in transmission facilities.

Recommendation: The Nationwide Emergency Telecommunications Service Is Needed

Given that there is no assurance that by the year 2000 enhanced routing capabilities will be ubiquitous in the public networks, the Nationwide Emergency Telecommunications Service is needed now, and its functional equivalent will be needed beyond the year 2000 for national security emergency preparedness purposes.

Emerging network intelligence technologies will not, without remedial intervention, provide a suitable infrastructure for NCS's proposed Nationwide Emergency Telecommunications Service (NETS).

Among the key new network capabilities the committee examined were the ISDN, switching techniques that use the asynchronous transfer mode, and the widespread deployment of VSATs. Neither these nor any other foreseeable emerging technology will, by themselves, ensure adequate fulfillment of the requirements for the proposed NETS. Due to concentration of network intelligence in large switches and databases, the public networks will lack sufficient critical-node redundancy to implement NETS if disaster strikes.

Recommendation: Provide Additional Redundancy

Because concentration of network traffic and routing nodes is increasing network vulnerability, additional route diversity and network node diversity should be provided for national security emergency preparedness purposes.

Implementing priority access procedures cannot alone ensure the availability of emergency communications. If fire destroys the only central switching office that can route emergency traffic from a given area, or if an earthquake uproots critical optical fiber transmission lines, essential communications linkages will be severed. The increased reliance of the public networks upon a single technology for transmission—optical fiber—is thus a source of great risk to NSEP.

These measures will cost money. However, whether users, shareholders, or taxpayers should bear the cost is a matter of public policy that goes beyond the scope of the committee's charter.

Recommendation: Increase Radio Access Capabilities

Since radio technologies can provide a valuable source of alternative routing in emergencies, the National Communications System should consider how terrestrial and satellite radio transmission can be employed to provide route diversity for national security emergency preparedness purposes; in particular, consideration should be given as to how very small aperture terminals can be used to back up the public switched networks.

Advances in radio technology offer great promise for augmenting network route diversity. Cellular mobile radio has enormously expanded available capacity for mobile communications interconnected with the landline switched networks; digital microwave technology is

making telephone service economical in hitherto inaccessible rural areas; VSATs are making satellite distribution economical and efficient for smaller business users and present possibilities for economical deployment of widely distributed intelligent network signaling architectures.

Recommendation: Retain Existing Synchronization

As existing network synchronization levels already exceed those required for national security emergency preparedness, no action need be taken to increase the robustness of network synchronization beyond existing standards for normal network operation; designers of terminal devices should engineer them to operate satisfactorily under system synchronization standards.

In one respect, that of network synchronization, the existing and prospective network capabilities appear more than sufficient to meet present and future NSEP requirements. The committee examined network synchronization in detail and concluded that the present standards ensure an adequate margin of safety. However, because users have full freedom to connect registered terminal devices to the public networks, it is incumbent upon equipment designers to provide units that function properly within existing network synchronization standards.

REFERENCES

- Buckley, W. 1989. T1 standards and regulations: Conflict and ambiguity. *Telecommunications* (March).
- Dvorak, C. 1987. A framework for defining service quality and its applications to voice telephony. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., December 8.
- Henry, P. 1988. Lightwave communications: Looking ahead. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., May 18.
- Langseth, R. 1987. Data communications overview: Network performance and customer impacts. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., December 8.
- Lowndes, J. 1988. Corporate use of transponders could turn glut to shortage. *Aviation Week & Space Technology* (March 9).
- National Communications System. 1988. *May 8, 1988 Hinsdale, Illinois Telecommunications Outage*. Washington, D.C.: National Communications System.

Samuelson, R. 1988. The coming blackouts. *Newsweek*. December 26.

Solomon, R. J. 1988. Planning for uncertain futures: The utility of a general purpose broadband network. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., March 15.

6

Competition

The opening of most major telecommunications markets to competition increases concerns about network vulnerability. Competition has stimulated product and service diversity, but it has also led to proliferation of discrete network architectures (Huber, 1987). Further, because competition is more mature in some markets than in others and because the economics of market segments differ, competition's impact on national security emergency preparedness (NSEP) varies from market to market.

For purposes of the committee's analysis of the impact of competition on public network NSEP, it is useful to distinguish between seven categories of telecommunications and information services. This chapter discusses providers of exchange service (local and interexchange), cellular mobile radio, customer-premises equipment (CPE), value-added networks (VANs), electronic databases, cable television, and innovative services.

EXCHANGE TELEPHONE SERVICES

Background

Divestiture segmented the local and long-distance exchange service markets. Competition is an established fact in interexchange markets. Local-loop competition already exists in private local exchange

bypass services; metropolitan area networks (MANs), wide area networks (WANs), and premises-based local area networks (LANs) are becoming ubiquitous features of business telecommunications. Teleports use satellites to establish long distance links connecting to public and private local landline networks via optical fiber links. Business data traffic can bypass local gateways to interexchange networks. Fiber MANs and WANs link business firms within the same urban area and can also bypass public network facilities. Already, according to documents filed with the Federal Communications Commission (FCC), bypass is siphoning billions of dollars in revenues from the local exchange carriers (although carriers are eligible to compete for bypass business).

National Security Emergency Preparedness Implications

Bypass stimulates duplication of network facilities, and can lead to deployment of substantial excess network transmission capacity. Intense competition for limited customer demand can drive providers to offer prestandard or nonstandard offerings in an effort to get the jump on competitors. Manual or automatic network reconstitution mechanisms can ameliorate somewhat the NSEP problems posed by networks not configured to prevailing general standards. When telecommunications is opened to competition by many carriers, some initial incompatibilities will arise. Work in the Exchange Carriers Standards Association Telecommunications Committee (T-1) indicates that user demands for open system access in the marketplace are motivating vendors to standardize interfaces.

CELLULAR MOBILE RADIO

Background

Since its commercial introduction in 1983, cellular mobile radio has greatly increased mobile channel capacity in major urban markets and brought high-capacity mobile service to many smaller areas. Cellular is a mature technology initially tested in 1970: Vehicles with cellular phones communicate with a centrally located fixed transceiver site, which is linked via terrestrial lines to a computerized mobile telephone switching office (MTSO) which, in turn, interconnects the landline telephone networks to the cellular system. Cellular systems are subdivided into "cells"; as a user passes from one cell to the next the call is "handed off" to the next cell. This

"frequency re-use" allows system capacities far greater than offered by fixed mobile radio systems.

The FCC has divided each cellular market into two blocks: one "wireline" block allocated to telephone companies, and a nonwireline block reserved for mobile radio providers. The FCC's bidding process for cellular licenses and the large capital investment required to construct a cellular system, particularly in prime metropolitan areas, has led to ownership by consortia. As of the fall of 1988, in 12 of the 30 top cellular markets, wireline carriers have purchased the nonwireline franchise, creating competition between two wireline providers.

Cellular expansion has reached into hundreds of smaller markets. In many of these, smaller markets are linked as satellites to hub metropolitan systems, with remote switching in these "super systems" directed by the hub MTSO. Such arrangements make cellular economical for many rural markets that could not support stand-alone cellular systems.

Eventually, analog cellular systems will be replaced by digital cellular in the 1990s, which will increase system capacity, thus obviating the need to allocate additional scarce radio spectrum for cellular use. The economics of cellular systems makes conversion of analog facilities cheaper than constructing digital facilities from the ground up. By the year 2000 advanced signal processing will augment the sophistication of cellular systems. Spread spectrum transmission might also be employed.

National Security Emergency Preparedness Implications

From an NSEP standpoint the redundancy that cellular radio may provide to other systems is generally limited in two ways. First, cellular will not replicate in full—or even nearly in full—the capacity of the landline telephone networks. Second, cellular "super systems" are, in the context of NSEP, pseudoredundant: The remote switches serving the satellite areas depend on the capabilities of the hub metropolitan MTSOs, and thus if the hub MTSO goes down, the remotes will follow suit. This point is not intended to denigrate the value of super systems; they do provide valuable service to small areas that would otherwise lack cellular service.

Despite these limitations, cellular radio can significantly augment public network NSEP capabilities by offering some level of redundancy in the local loop. Cellular and other mobile systems

were used effectively by businesses affected by the Hinsdale switching facility fire. Business losses were prevented and, in some cases, alternative routing facilities were made available to serve their customers. Also, conversion from analog to digital cellular will improve cellular transmission security—digital systems are more difficult to intercept, as they are more easily encrypted.

CUSTOMER-PREMISES EQUIPMENT

Background

The most visible evidence of the impact of competition on the telecommunications industry is the proliferation of hundreds of types of CPE: Handsets, key sets, and private branch exchanges (PBXs) have brought distributed intelligence capabilities to the premises of many individual users—especially to business users (Handler, 1988). Premises-based intelligence gives users network management and control capabilities, a strategic asset in an information-based economy.

The introduction of myriad types of CPE stimulated regulatory relocation of network interfaces to facilitate customer control of network functions and ease interconnection (Sugrue and Cimko, 1988). As basic transport of the integrated services digital network (ISDN) is made available, independent protocols are likely to be developed in order to link diverse CPE to the public and private networks.

Premises-based switching intelligence will drive new forms of switching before they appear in the public, centrally switched networks: Wideband packet and voice/data LANs will likely appear first in premises-based applications.

Already, several generations of CPE have been produced and deployed in the domestic networks. This equipment diversification coupled with growth in variety of internal protocols should, by the year 2000, lead to almost completely heterogeneous configurations on the customer's premises. Competitive pressures will spur customizing of individual CPE network packages.

National Security Emergency Preparedness Implications

The bewildering diversity of available CPE can seriously complicate NSEP management. When Western Electric was the sole CPE manufacturer for the integrated Bell System, Bell System managers were fully acquainted with the characteristics of the CPE connected by

wire to the network. By contrast, today, and even more so tomorrow, no network-based company is likely to have knowledge of more than a few major CPE systems. Customers are free to interconnect the equipment of their choice to the network, without even notifying the telephone companies. Further, the proliferation of interfaces between the customer's premises and the public and private networks will complicate loop testing and billing verification. Other future uncertainties could include CPE configured to be voice activated by specific users only.

Thus, although deployment of highly diverse CPE has enhanced customer choice, it has hindered development of ubiquitous network-premises interface standards that would guarantee universal interoperability. Again, as with other areas open to competition, there are clear benefits to users in having greater freedom of choice, but the resulting product diversity has compounded the problems NSEP planners must face.

VALUE-ADDED NETWORKS

Background

A class of networks known as VANs, first deployed in the 1970s, is becoming widely available for commercial use. These networks are packet switched rather than circuit switched. That is, they do not tie up a circuit end-to-end, but only occupy space when data are actually being transmitted. The past decade has seen establishment of numerous VANs, primarily to supply business data services, but also to provide information services to residences. Businesses have an overriding incentive to migrate data traffic to private VANs: the desire for absolute control over the management and operation of their telecommunications and information networks. Customer control affords business users with strategic assets to manage system costs and match them to system capabilities.

VANs are also leading to another form of network "overbuild": buying or leasing fiber routes operated by entrepreneurs, separate from the public networks. These "transmission condominiums" use pipeline, rail, and highway rights-of-way. Also, some entrepreneurs are entering joint ventures with established carriers, forming "owner associations." Interexchange carriers have constructed large VANs, priced via special tariffs, to provide users with bypass alternatives to local exchange access to interexchange gateways. But as with other competitive markets, value-added services competition is stimulating

deployment of nonstandard architectures in the public and private networks.

National Security Emergency Preparedness Implications

VANs provide valuable signaling capabilities that may be used to supplement centrally located network signaling; packet networks were designed to enable rapid reconstitution of damaged networks. But if a proliferation of nonstandard architectures prevails, for want of interoperability their overall value may be minimal for NSEP redundancy, and thus private operators of VANs may will only be able to provide limited backup to public users in emergencies.

DATABASES

Background

Electronic software databases now represent a voluminous repository of information service database access. Among the principal market applications are call answering (800) service, financial services (such as electronic funds transfer and credit card verification), specialty news services, home shopping, and network management. Business use predominates, with residential applications limited by the penetration of intelligent CPE or personal computers needed to access databases and maintain interactive data dialogues with them.

National Security Emergency Preparedness Implications

Electronic databases offer significant potential NSEP benefits. As one example, medical assistance might be augmented by database information. Operating instructions for vital equipment could be stored for access by inexperienced personnel. But databases also have major vulnerabilities. Being software driven, and given that they are oriented toward ease of customer access to facilitate marketing database services, they are vulnerable to hostile penetration.

Protecting databases while ensuring adequate public access is difficult. Recently, the Lawrence Livermore National Laboratory—a vital national research facility—experienced multiple penetrations by a hostile user. Unable to locate the user, the laboratory posted a public query on its damaged data network, asking the intruder to disclose his grievance and discuss ways of resolving it. Many

public research databases depend critically on open public access—certainly, any electronic database intended to supplement NSEP capabilities must be readily accessible to the public networks, yet such accessibility contains the seeds of their potential destruction.

CABLE TELEVISION

Background

In the video marketplace of the 1980s cable television has become a widely available alternative to traditional network (broadcast) television. According to the National Telecommunications and Information Administration, in 1975 cable served 13 percent of the nation's households; it now serves more than 53 percent. Cable has now "passed" over 80 percent of the nation's households, that is, cable service can be provided to these households without installation of additional distribution plant. Whereas in the late 1970s the three major television networks could count on reaching 90 percent of the prime-time audience, today that figure stands at 70 percent. During the daytime, cable has earned the allegiance of as much as 50 percent of the viewing audience.

Cable television today uses a tree and branch distribution architecture, in which homes are tapped off long feeder cables. Its systems architecture is optimized for one-way transmission of 30 to 50 channels at a minimum cost. (Minimal two-way cable carriage provision was imposed on cable carriers by the FCC in 1972, but the requirement was abolished by Congress in 1984.) Signals are delivered in analog form via coaxial cable.

In the future the distribution medium of choice for cable television may become fiber optics, if fiber is deployed in the local exchange loop, that is, to the customer's home. Fiber provides enormous bandwidth and high signal quality and could become a formidable competitor for coaxial cable transmission. How quickly and ubiquitously fiber is deployed depends on both regulation and economics. One regulatory issue is whether telephone companies will be allowed to provide video service to their exchange subscribers, and whether if allowed to do so they will be permitted to offer video programming as well as dial tone. Today, there is only a little fiber in the cable television plant, and that is used for long trunk routes using analog modulation.

At present, given the underlying economics of fiber, the desirability of fiber in the future, and the large and growing differences

in the price of a cable subscriber over the capital investment in the physical connection, it appears that overbuilding bypass will eventually occur, that the content control prohibition on the telephone operating companies may well be relaxed, and that the new video transmission medium of choice will most likely be fiber. It is unlikely that all this will occur in large scale by the year 2000. Ultimately, if broadband switching is deployed by exchange carriers, they will be able to offer switched video services that cable television companies cannot offer with their tree and branch architecture.

National Security Emergency Preparedness Implications

Cable television, if delivered via optical fiber, could eventually largely supplant traditional methods of television transmission, though probably not until some point in the twenty-first century. Accelerating the migration of television signal transmission to fiber could conceivably free up limited spectrum for re-allocation to other radio applications, for example, public safety channels.

INNOVATIVE SERVICES

Background

Future service applications will undoubtedly emerge via the deployment of customizing service packages of individual customers. As digital architectures become the norm in the public networks, and as fiber makes "arbitrarily large bandwidth" available, potentially valuable NSEP applications could be developed, provided that standardized interoperable equipment and architecture are employed.

National Security Emergency Preparedness Implications

At this time, the potential benefits of innovative services are highly problematical, as specific new services are only now beginning to be deployed and many possibilities have yet to be explored.

RECOMMENDATIONS

While competition brings to the public networks its handmaiden, greater diversity for individual users, it does so in part at the expense of collective user needs like NSEP, the satisfaction of which

is not typically the object of commercial marketing efforts. Network disaster planners focus on adding redundancy to ward off the effects of contingencies whose severity may be extreme, but whose occurrence may be improbable. By contrast, competition induces competing companies to trim costs, especially in businesses with the narrow profit margins typical of many competitive telecommunications markets.

In some regards, the multiple competitive networks that have come into existence will provide backup for one another. This is true for isolated damage situations in which damage in one area or geographic region is totally unrelated to damage in another. However, destruction of only a few signal transfer points (STPs) in each of the major carrier networks can disable the associated network. Since some number of carrier transmission routes follow the same rights-of-way, certain damage situations could cause simultaneous failures in the facilities of several network providers. The competitive environment will provide backup for some threats, but not for correlated events in which damage is inflicted at several points by an intelligent adversary or widespread natural disaster.

The committee believes that, unless corrective actions are taken, the cost of network failures caused by natural disasters or covert activities (terrorists) could create an unacceptable burden to society. A small group of individuals could create economic damage and social disruption by attack or sabotage at critical switching and transmission facilities (Center for Strategic and International Studies, 1984). The immediate damage could potentially be in the many millions of dollars with the longer range consequences impossible to quantify. It may be difficult to reconstitute communications services, including ordinary telephone service, if significant damage is done to the communications infrastructure.

The difficulty of reconstitution results from the need to find and re-establish complex centralized databases, to reinstitute centralized control through damaged STPs, and to manufacture and install massive switches. It is further complicated by the higher skill levels needed among personnel who operate advanced networks: Fewer people will be available to assist in reconstitution. Also many remote switches that depend on core central complexes will, as indicated earlier, fail if the host node fails.

This report recommends that the National Communications System explore how the capabilities of private institution voice and data

networks can be used to provide NSEP redundancy. Particular attention should be given to how private network interoperability can be increased via deployment of gateway architecture. The committee recognizes that, while this approach may provide additional resources, it also presents some nontrivial problems with implementation and readiness. For the government to have high confidence that such gateway arrangements will operate as anticipated would require extensive network tests, regular exercising, and long-term coordination of network planning. Both the public networks and most private networks are in constant states of change, with database updates constantly occurring. Unless live traffic is routinely being sent over such gateways, the confidence factor that a standby capability is available will not be high.

From an NSEP standpoint some measure of standardized system interfaces and universal access via gateways are desirable network enhancements. However, while from a simple availability of facilities standpoint this is certainly true, from a security standpoint there is a potential increase in risk if this move toward standardization and interconnection occurs before the trusted software to support it evolves. Were all private and public networks to be fully interconnected and employ common software, the entire network could be at risk if a hostile user were to find an exploitable flaw in the system software (a "back door" for example). This again amplifies the importance and need for trusted software in applications such as network management and Open Network Architectures. This problem reveals a potential, albeit unintended, benefit of the current separation of networks: Today more than one software system would have to be successfully penetrated to cause a system-wide outage. On balance, the committee feels that separation of networks does not best serve the NSEP community; emergency response may fail because officials cannot readily access surviving facilities. While proliferating networks are a current fact of life, some form of preplanned interoperability cutover mechanisms should be designed and put in place. The other critical point to note is that the pace of standardization and interconnection will have to be tied to the pace at which trusted software can be developed in order to maintain network security through the transition.

It would be an exaggeration to assert that the NSEP capabilities of the public networks are near collapse. It would, however, be reasonable to state that competition has made NSEP planning more

difficult and that, if no remedial action is taken, the integrity of U.S. information highways will be put at unacceptable risk.

The committee therefore makes the following recommendations.

Recommendation: Exploit Value-Added Networks

Because packet switching techniques are well suited for adaptive routing, the National Communications System should devise ways to exploit the capabilities of the commercial packet-switched, value-added data networks for national security emergency preparedness purposes, including message transmission, electronic mail boxes, and more robust signaling.

A potentially valuable source of public network redundancy is private networks. Whereas today's networks were designed almost exclusively to carry voice transmission, the network of the future will be increasingly driven by data transmission needs. VANs are often driven by premises-based network control intelligence, and thus offer valuable network routing capabilities if interconnected with the public switched networks. Such signaling capability is superbly suited to alternate routing schemes: Packet switching was originally designed to enable adaptive routing through damaged networks. The committee also notes, however, that making use of VANs to strengthen survivability will only succeed if the other recommendations concerning attention to greater redundancy are followed.

Recommendation: Promote Internetwork Gateways

Because interconnection of the proliferating public networks is essential for national security emergency preparedness, the National Communications System should explore how the capabilities of public and private institutional voice and data networks can be used to provide redundancy; particular attention should be given to how network interoperability can be increased through deployment of gateway architectures.

Many large government and commercial private networks are not currently fully interoperable with the public switched networks: They operate according to a different set of protocols and standards. These

networks, if fully interconnected with the public networks, could augment NSEP resources. Another impediment to end-to-end interconnectivity is that more terminal devices are not entirely compatible with network interface standards.

All parties, for example, customers, service providers, and manufacturers, have been inconvenienced by this trend. There is a growing understanding that signaling and transmission standards are needed to recognize the convergence of "customer" and "service-provider" networks. With the adoption of adequate standards, private network nodes can have stature similar to public network nodes. The national resource will then become communications network standards, rather than any particular set of facilities. For national security purposes, the rapid development of these standards is paramount.

In recognition of this change in the perception of the national telecommunications resource, several communications intensive standards bodies are working to create the necessary recommendations. Efforts have concentrated on access and interoperability standards in association with the next wave of technology implementations—the Open System Interconnection of the International Organization for Standardization for data networking access and interconnections, ISDN for digital network access, Synchronous Optical Network (SONET) for internodal transmission, Signaling System 7 for internodal signaling, and Institute of Electrical and Electronics Engineers metropolitan area networks for broadband network access and interoperability.

Standards, properly enough, take time to develop. The exigencies of the marketplace force other, interim steps from competitors. Gateways, offering limited conversion from one network to another, are means by which prestandard technology implementations can provide a degree of near-term interoperability. Today's network interconnections are predominantly characterized by this technology. Premises-network interconnections, private network to public network connection, and private network interconnection all have gateway offerings that provide limited conversion capabilities. This appears to be an acceptable migratory step in the standards development process.

REFERENCES

- Center for Strategic and International Studies. 1984. *America's Hidden Vulnerabilities: Crisis Management in a Society of Networks*. R. H. Wilcox and P. J. Garrity, eds. Washington, D.C.: Georgetown University.

- Handler, G. 1988. The emerging intelligent network. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., May 18.
- Huber, P. W. 1987. *The Geodesic Network: 1987 Report on Competition in the Telephone Industry*. Washington, D.C.: U.S. Government Printing Office.
- Sugrue, T., and J. Cimko. 1988. Open network architecture and the price cap vs. the rate of return. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., March 15.

Customer Demand

Most efforts to predict future user telecommunications needs are too optimistic about near-term growth in requirements and too conservative about long-term growth. One source of variance between expectations and reality is that forecasters are unable to take into account the effects of technology on user behavior and thus simply extrapolate current trends. User needs, as articulated by users and served by vendors, are a consequence of what technology allows and what can be made affordable. Therefore, until the possibilities of a new technology are evident, users and forecasters have a difficult time in seeing how the new technology will be applied.

Using this principle (that articulated user needs are a consequence of what the technology allows and can be made affordable), the committee based its projections of user needs on its assumptions about the environment in the year 2000. After examining the environment, this chapter discusses user needs in general, presenting specific user profiles and assessing national security emergency preparedness (NSEP) implications.

BASIC TECHNOLOGICAL ASSUMPTIONS ABOUT THE ENVIRONMENT IN THE YEAR 2000

The committee made the following basic technological assumptions about the telecommunications environment in the year 2000:

- Terminal equipment will handle voice, data, and images with equal ease.
- Most telephones will tie into digital devices.
- Most computers will be connected into networks.
- Integrated voice, data, and image (such as facsimile) work stations capable of handling all three transmissions will be widespread.
- Some (as yet unquantified) number of residences in the United States will have remotely addressable, intelligent computing devices—many in telephones or television sets.
- Huge databases of primarily alphanumeric content will be everywhere.
- Image databases (of photographs, catalogs, libraries, and so forth) will be propagating rapidly.
- A combination of high-capacity transmission with terminal equipment of low cost and high compression will allow full-motion, interactive video transmission in many areas.
- Long-haul fiber transmission will be pervasive.
- The public network will be a multivendor, multidevice, multi-application interconnection of networks.

As discussed earlier, the “intelligent network” and “open architecture” concepts will spur the delivery of customized services to government and commercial users. To provide these services, future networks will store pertinent information associated with a wide variety of calls—for example, call priority—in remote, centralized databases. Thus, a call’s unique line circuit and address information will no longer be stored in the central-office switch. In the event that database access is cut off, call information will be unobtainable, and circuits dedicated to emergency use would thus be unavailable. To remedy this defect, future network architectures will have to incorporate a feature which, after database failure, defaults line circuits to general-purpose use.

USER NEEDS

Integrated voice, data, and image applications will be in use by the majority of residential, small and large business, and institutional subscribers. The U.S. information infrastructure in the year 2000 will include most of the following characteristics.

Residences

Most residences will have several competing suppliers for what will then be considered upscale basic communications services:

- Telephone
- Television
- Mail and facsimile (electronic and physical delivery of text, voice mail)
- Catalog services (shopping, reservation, brokerage).

The trend to substitute communications for travel and related activities (one example, home shopping) will continue, albeit at a relatively slow rate. Electronic mail (E-mail) of all forms (voice mail, text mail, and facsimile) will make substantial inroads in penetrating the residential market.

Small Business Users

Small businesses will have the same needs as the upscale residence plus a few others, as follows:

- Telephone
- Television (for example, in-store promotion)
- Mail (electronic and voice)
- Facsimile (manual and automatic)
- Catalog services (ordering, reservations, brokerage)
- Electronic authorization and money transfer.

While not suffering the same immediate degree of paralysis from a network failure that would be felt by a large business, the small company will be affected by network failures in many ways. And, because small businesses depend on communications with larger companies for many of their vital services (credit checking, banking, reservations, and so forth), a widespread network failure would quickly move from causing mere disruption to inflicting serious economic harm.

Large Business Users

Medium and large businesses will employ integrated information systems to connect the various stages of their operational processes together. The typical company will be electronically linked to the order-entry and logistics systems of its business customers and to its suppliers. In manufacturing businesses, networked systems that

handle incoming orders will be tied to material requirements planning (MRP) systems and to those that schedule the delivery of raw materials. In turn, manufacturing scheduling systems will be connected with the MRP systems and with the systems needed to plan the delivery of finished products. Similar integration will take place in large service organizations of all kinds (such as banking, finance, brokerage, and insurance).

Sophisticated users will use very high capacity applications that combine full-motion interactive video with today's more conventional technologies. Advanced users will use interactive video for computer-aided design (CAD), medical diagnostics, image analysis, parts manuals, artwork, documentation, and other high-bandwidth applications. These applications will depend crucially on effective communications and will be disabled if their supporting communications system fails.

The typical large organization will utilize many overlapping, interconnected networks supplied by a variety of sources including local area networks (LANs), very small aperture terminal (VSAT) networks, and private and public wide area networks (WANs). Nearly all businesses will use intelligent terminals interconnected by LANs for routine business functions. These LANs, in turn, will be connected through WANs. The public switched networks will be of enormous importance to businesses of all sizes, since not only will they represent the universal interconnecting vehicle but also the many private networks will share facilities and capacity with public networks.

As companies link the various stages of their business processes together, they will increase their dependence on the proper functioning of the supporting networks. For example, the failure of an order-entry network or a logistics system will disable the business functions associated with taking orders from customers, receiving materials from suppliers, and delivering products to customers.

In this environment, the economic damage caused by network failures of even a few hours will be great.

Government Users

To a great extent, government at all levels can be considered from a communications perspective to be affected in the same way as large businesses. State and local government communications systems will be collections of connected public and private networks.

The functioning of all municipal public services, such as police, fire, and 911 emergency calling, will depend crucially on telecommunications. Routine government functions, such as utilities billing, driver's licenses, and motor vehicle registration, now depend on communications and will continue to do so in the coming years.

Many government services, such as social security and tax administration, depend on access to data stored in large, centralized databases. Such dependencies are increasing as terminals and database systems become more popular and pervasive. Network failures will prevent access and hence prevent the delivery of the service. Many local governments will have their own dedicated emergency communications systems, some utilizing cellular radio. However, these systems will be tied into the public switched networks for citizen access and call routing.

The federal government, while having special requirements for military communications, has needs that parallel those of a collection of giant corporations. The government uses public networks to communicate with the outside world. It employs a collection of private networks for communications among government employees within a particular department or agency or between such agencies. These private networks, in turn, depend on public networks for most of their transmission and switching facilities.

The same technological advances that are propelling the commercial sector toward integration of business functions will allow elements of the federal government to make sophisticated use of voice, data, and image transmission to streamline operations (Reudnik, 1988).

Federal government communications needs can be separated into two general categories: national security and civil functions.

National Security Users

National security functions can be thought of largely as the needs of the president, the U.S. Department of Defense (DoD), Department of State, and national intelligence agencies. The fundamental forms of communications required by the national security community are not expected to change in ways that would drive significant public switched network changes. The national security community will continue to use a combination of private networks and services from the public switched networks.

Secure voice will dominate telephone service needs with a growing demand for specialized services (also in a secure mode), such as voice mail, call forwarding, and preset and ad-hoc conference calls. Satisfaction of the demand for these specialized services by the public switched networks would require communications security features not currently planned. It seems more likely that the voice needs of the national security component of government will be met by government provided (leased or owned) customer-premises equipment (CPE) interconnected by transmission derived from the public networks, together with significant off-net calling capability.

Data traffic needs will range from relatively low speed data circuits to very high speed circuits. Networking very large numbers of remote terminals will become commonplace. Needs will vary to such a degree that both private line networks and packet-switched networks will be employed. Communications and computer security needs will receive growing attention; government users will rely on encryption of government terminal and computer facilities rather than public network security. One can expect that voice and data traffic will be integrated through government-provided CPE and the interconnecting transmission obtained from the public networks. Greater reliance on networking will make restoral much more difficult for worst-case national security emergency preparedness situations.

There will be a continuing need for worldwide narrative message capabilities of a formal nature and a growing demand for narrative messages of an informal nature (E-mail). Both forms of narrative traffic will require cryptographic protection, although the level of protection provided for the informal traffic may be less than that required for formal traffic.

Although fundamental communications needs will be essentially unchanged over the timeframe under consideration, there are some major drivers that will influence the national security community's decision to use the public networks, to acquire its own system, or to use some combination thereof. The critical nature of national security communications needs will cause the customer to demand a very high degree of customer control of those assets used to provide part or all of the service. Thus, transmission provided on a variable basis to interconnect government CPE must allow the government maximum flexibility to reconfigure its network on a minute-by-minute basis.

Greater emphasis will be placed on information security—both communications and computer security. Increasing use of databases and automation in the public networks will generate concern about

unauthorized penetration or manipulation. Hence, the national security community can be expected to avoid the use of service features of the public networks that depend on databases with inadequate computer security safeguards.

Cost of service will continue as a major, but not an overriding, determinant in national security community decisions about use of public network services.

Reliability, survivability, and flexibility will continue to be major performance criteria (Wallace, 1988). The multivendor supplier telecommunications environment will require national security managers to exert greater efforts to assure that the services being acquired from the public networks meet these criteria. It is no longer possible to rely on the single service provider as was the case in the past.

Civil Users

The needs of the civil sector of government for communications for the period under consideration have been defined rather precisely in the Federal Telecommunications System (FTS) 2000 specifications. Numerous dedicated data networks (initially outside of FTS 2000) will be gradually integrated into the FTS 2000 packet-switched component.

FTS 2000 possesses certain NSEP capabilities, but these are limited to capabilities to handle major localized disasters. FTS 2000 is neither designed nor intended to cope with a nuclear attack scenario.

As discussed earlier, software problems are expected to lead to additional network vulnerabilities. Steps should therefore be taken to minimize the damage caused by software disruptions. The combination of the "openness" of future network services to external personnel along with the sophistication of the new generation of "software invaders," can lead to threats not contemplated by conventional analyses of network vulnerability. In particular, planners of new network architectural strategies should consider this issue.

A large-scale failure of the public networks would paralyze the federal government. A few examples of critical functions delivered via government networks will illustrate this point: The U.S. Customs Service serves agents at points of entry into the country, and the many agencies that deliver vital social services, such as Social Security, Medicare, and Aid to Families with Dependent Children, cannot operate without support from voluminous remote databases. Thus, failures of vital public network nodes could bring many civil

governmental functions to a standstill. It is not necessary to enumerate the many individual crises that would result to be convinced that such a failure would truly be a national disaster.

NATIONAL SECURITY EMERGENCY PREPAREDNESS IMPLICATIONS

Customer demand is driving network services toward customized services, customer-directed network software (which requires open access), and information-intensive applications of the public networks. As the services that society relies on become more open and information-oriented, network vulnerability increases. The consequences of accidental damage, while significant, are perhaps less worrisome than the exposure of an information society to nonrandom threats. Those who would intentionally inflict damage on the public networks have more opportunity to do so as networks evolve in the manner described in this report. The nation's increasing economic, social, and political dependence on the information infrastructure means that both the opportunities to inflict damage and the payoff for doing so are growing exponentially.

The NSEP implications of these trends are obvious. Customer control, while highly desirable in many ways, greatly complicates NSEP management by surrendering control over large parts of the public networks to those whose actions are not easily controllable by agencies charged with NSEP responsibility. Whereas organizations such as exchange carriers can be brought into the NSEP planning process and are directly, on a daily basis, accountable to federal, state, and local authorities for the manner in which they conduct their business affairs, individual users are outside the NSEP process. Even user groups cannot coerce individual users to join their organizational efforts. If it is not feasible to bring the universe of customers into the NSEP planning process, then consideration must be given to taking steps that insulate the public networks from certain potentially serious harmful acts that customers can engage in via open access to network software.

RECOMMENDATION

Based on the foregoing discussion and analysis the committee makes the following recommendation.

Recommendation: Establish Software Security Measures

Since the public networks are increasingly driven by software, the National Communications System should consider how to protect the public network from penetration by hostile users, especially with regard to harmful manipulation of any software embedded within the public networks that is open to customer access for purposes of network management and control.

Perhaps the most disturbing of the growing network vulnerabilities described in this report is that of increasingly open outside access to network databases. The desire to open access to the public networks must be counterbalanced by a recognition that the integrity of the public networks must be protected. The National Security Telecommunications Advisory Committee (NSTAC) has already addressed two network software issues: automated information processing (AIP) and industry information security (IIS). With the advent of Open Network Architecture, the work done by the NSTAC must be built on, to meet the challenges posed by the emerging public network environment.

REFERENCES

- Reudnik, D. 1988. Views on telecommunications technology. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., March 16.
- Wallace, L. 1988. Perspective on testing, restoration, and network management. Presentation to the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, Washington, D.C., March 16.

Appendix A

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 objective 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

*This was the original statement of the study task. Midway through the NETS study the National Communications System 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.

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 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 recommend technical approaches to developing cost-effective, survivable synchronization and will suggest technical program 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.

*Fulfilled by the committee's interim report, *Nationwide Emergency Telecommunications Service for National Security Telecommunications* (1987).

Appendix B

Issues in Digital Network Time and Frequency Synchronization

1. INTRODUCTION

This appendix explores issues in the synchronization of digital communications networks used for telephony and data transmission. It is based on briefings presented to the National Research Council's Committee on Review of Switching, Synchronization and Network Control by several organizations, including the American Telephone and Telegraph Company (AT&T), Bell Communications Research, MCI Communications Corporation, US Sprint, CONTEL/ASC, and the U.S. Coast Guard,¹ together with material provided by the committee members themselves. In addition to this information, the appendix includes background material gathered from many sources, as documented in the notes at the end of this appendix.

The most important area of network synchronization for the committee's purposes has to do with how various digital telephone networks interoperate using synchronous data streams at the T-1 rate (1.544 Mbits/s) with DS-1 frames (193 bits). The electrical interfaces between such networks use a double-buffered technique to compensate for the different framing relationship ordinarily encountered between them. If the networks use timing sources not exactly synchronized in frequency (phase locked), the frames sent by one network will precess slowly with respect to another, and frames must

occasionally either be discarded or replicated in order to maintain overall synchronization.

The appendix consists of nine sections, including this one. The following two sections describe the means for generating and distributing the national standards of time and frequency in the United States. In particular, Section 2 discusses general aspects of standard time and frequency scales used for navigation and space science, while Section 3 describes the primary services operated by the National Institute of Standards and Technology (NIST), formerly the National Bureau of Standards (NBS), for the dissemination of standard time and frequency.

The next three sections describe how synchronizing information is distributed throughout the United States and utilized as timing sources by various switches and transmission systems in the U.S. telephone networks. In particular, in Section 4 several time and frequency distribution systems are presented, with special emphasis on LORAN-C, which is fast becoming the system of choice used by U.S. exchange and interexchange carriers. Section 5 discusses issues important for the understanding of synchronization errors and how they may affect the operation of the various switches and other components of the telephone network. Section 6 describes the synchronization networks operated by the various exchange and interexchange carriers in the United States, including AT&T, the Bell Operating Companies (BOCs), and selected independents.

The final three sections contain the committee assessment of the impact of synchronization impairments on the National-Level Program/National Security Emergency Preparedness (NLP/NSEP) programs. In particular, Section 7 analyzes the effects of these impairments on transmission, switching, and user applications, while Section 8 discusses the impact on the NLP/NSEP programs. Section 9 states the committee's conclusion and recommendation.

2. DETERMINING STANDARD TIME AND FREQUENCY²

For many years the most important use of time information was for worldwide navigation and space science, which depend on astronomical observations of the moon and stars. Ephemeris time is based on the revolution of the earth about the sun with respect to the vernal equinox on the celestial sphere. In 1956 the tropical year, or one complete revolution, was standardized at its value at the beginning of this century, when it had a period of 31,556,925.9747 seconds, or

365 days, 5 hours, 48 minutes, 46 seconds; however, the actual year has been increasing by about 5.3 milliseconds (ms) per year since that time. Sidereal time is based on the rotation of the earth about its axis with respect to the vernal equinox point. The mean sidereal day is about 23 hours, 56 minutes and 4.09 seconds of the tropical year, but is not uniform due to variations in earth rotation.

In 1967 the Thirteenth General Conference of Weights and Measures decided that

the unit of time of the International System of Units is the second defined as follows:

"The second is the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium 133 atom."*

The transition referred to had been declared in 1964 by the International Committee of Weights and Measures to be that

between the hyperfine levels $F = 4, M = 0$ and $F = 3, M = 0$ of the ground state $^2S_{1/2}$ of the cesium-133 atom, unperturbed by external fields. . . .

Here, F is the total angular momentum quantum number and M is the magnetic quantum number associated with F .

The International Atomic Time (TAI) scale, used for astronomy and physics, is based on the standard second. On the other hand, the Coordinated Universal Time (UTC) scale, used for other purposes, is based on the rotation of the earth about its axis with respect to the sun, indexed to the prime meridian, which passes through Greenwich, England. In recent times UTC has been slow relative to TAI by a fraction of a second per year.

UTC is coordinated throughout the world by the Bureau International de l'Heure (BIH) at Paris, which issues various corrections to TAI on a regular basis. On 1 January 1972 the TAI and UTC time scales were made coincident and have been diverging slowly ever since. The UT-0 day of 24 hours is defined as the mean sidereal day converted to mean solar day by ephemeris tables. The UT-1 day is determined from the UT-0 day by including regular corrections on the order of 30 ms due to seasonal changes in winds and tides. The UT-2 day is determined from the UT-1 day by including irregular

*Source: National Bureau of Standards. 1977. *The International System of Units (SI)*. NBS Special Publication 330. Washington, D.C.: U.S. Government Printing Office.

TABLE B-1 Characteristics of Primary Standards

Type	Stability	Drift
Hydrogen maser	$< 2 \times 10^{-14}/\text{day}$	$< 1 \times 10^{-12}/\text{yr}$
Cesium beam	$< 3 \times 10^{-13}/\text{day}$	$< 3 \times 10^{-12}/\text{yr}$
Rubidium gas cell	$< 5 \times 10^{-12}/\text{day}$	$< 3 \times 10^{-11}/\text{mo}$

corrections as reported by various observatories to the BIH. UTC is derived from UT-1 as described later.

Primary Frequency Standards

In order that both atomic and civil time can be coordinated throughout the world, it is expected that national administrations will operate publicly available primary time and frequency standards and maintain UTC cooperatively by observing various radio transmissions and through occasional use of portable atomic clocks.

A primary frequency standard is an oscillator that can maintain extremely precise frequency relative to a physical phenomenon, such as a transition in the states of an orbital electron. Presently available standards are based on the transitions of the hydrogen, cesium, and rubidium atoms. Table B-1 shows performance data for typical units.

For reasons of cost and robustness, frequency standards based on cesium are used worldwide for national standards. In principle then, the frequency standards of the world should not drift apart by more than 43 nanoseconds (ns) per day or 95 microseconds (μs) per year. For instance, The NIST Primary Time and Frequency Standard, which consists of multiple cesium beam clocks and computer-controlled measurement and computation methods, is held to within 10^{-12} with daily variations even less.

Primary Time Standards

Since 1972 the various national time scales have been based on UTC, as determined by the BIH using astronomical observations provided by the U.S. Naval Observatory and other observatories. However, it is desirable that the UTC oscillator run in synchronism with the TAI oscillator. Thus, when the magnitude of correction approaches 0.7 s, a leap second is inserted or deleted in the UTC time scale on the last day of June or December.

TABLE B-2 Months of Leap-Second Insertion

Occasion	Month of Insertion
1	June 1972
2	December 1972
3	December 1973
4	December 1974
5	December 1975
6	December 1976
7	December 1977
8	December 1978
9	December 1979
10	June 1981
11	June 1982
12	June 1983
13	June 1985
14	December 1987

For the most precise coordination and time stamping of events since 1972 it is necessary to know when leap seconds were inserted or deleted in UTC and how the seconds are numbered. A leap second is inserted following second 23:59:59 on the last day of June or December and becomes second 23:59:60 of that day. A leap second would be deleted by omitting second 23:59:59 on one of these days, although this has never happened. Leap seconds were inserted on the following 14 occasions prior to January 1988, as shown in Table B-2.¹¹

BIH corrections consist not only of leap seconds, which result in step discontinuities in UTC, but 100-ms adjustments, which provide increased accuracy for navigation and space science. The current time-scale formats used by NIST radio broadcast services do not include provisions for advance notice of leap seconds, so this information must be determined from other sources.

Various specification and standards documents stipulate that the primary timing sources used by digital networks must be verifiable with respect to UTC; however, for digital network synchronization, only the frequency information is used—the time information is not used. This distinction is a minor one, since the U.S. standard frequencies distributed by NIST are based on atomic time, while the standard times distributed are based on UTC.

3. PRIMARY TIME AND FREQUENCY DISTRIBUTION²

Most seafaring nations of the world operate some sort of broadcast time service for the purpose of calibrating chronographs, which are used in conjunction with ephemeris data to determine navigational position. In many countries the service is primitive and limited to seconds-pips broadcast by marine communication stations at certain hours. For instance, a chronograph error of 1 s represents a longitudinal position error of about 0.23 nautical mile at the equator.

The National Institute of Standards and Technology operates three radio services for the distribution of primary time and frequency standard information. One of these uses high-frequency (decametric) transmissions on various frequencies from Fort Collins, Colorado (WWV) and Kauai, Hawaii (WWVH). Propagation of these signals is usually by reflection from the ionosphere F layer, which varies in height and composition throughout the day and season and results in large phase fluctuations at the receiver. The time code is transmitted over a 60-s interval at a data rate of 1 bit/s using a 100-Hz subcarrier on the broadcast signal. While these transmissions and those of Canada (CHU) and other countries can be received over large areas in the Western Hemisphere, the accuracies attainable are considered insufficient for telephone network synchronization.

A second service operated by NIST uses low-frequency (kilometric) transmissions on 60 kHz from Boulder, Colorado (WWVB), which can be received over the continental United States and adjacent coastal areas. Propagation of these signals is between the earth and the ionosphere D layer, which is relatively stable over time. The time code is transmitted over a 60-s interval at a rate of 1 pulse per second using periodic reductions in carrier power. With appropriate receiving and averaging techniques and corrections for diurnal and seasonal propagation effects, frequency comparisons to within 10^{-11} are possible. However, there is only one station and it operates at modest power levels.

The third service operated by NIST uses ultra-high-frequency (decimetric) transmissions on 468 MHz from the Geosynchronous Orbiting Environmental Satellite (GOES). The time code is interleaved with messages used to interrogate remote sensors and consists of 60 4-bit binary coded decimal (BCD) words transmitted over an interval of 30 s. The time code information includes the UTC time of year, satellite position, and UT-1 correction. There is some speculation on the continued operation of GOES (one of the two satellites has

failed), especially if the Global Positioning System (GPS) continues to evolve as expected.

4. SECONDARY TIME AND FREQUENCY DISTRIBUTION

Present time and frequency dissemination services operated by NIST are not sufficiently ubiquitous and reliable as the basis of digital network synchronization in the United States. Accordingly, a high-power, widely distributed and replicated secondary means of distribution would be highly desirable. Among the various means possible to do this are the Long-Range Navigation System-C, or LORAN-C, operated by the U.S. Coast Guard (USCG), the OMEGA system operated by the U.S. Navy, and various satellite services now in operation or planned for the future. These services are described in following sections, with specific attention to LORAN-C, which is particularly suitable for use by U.S. digital networks.

LORAN-C^{1,6}

LORAN-C is a wide-area radionavigation system intended for maritime, aeronautical, and land navigation and positioning. It was first used about 1962 and has been operated since then by the USCG in North America and several overseas areas. Coverage is determined by geometry, range, time of day, and receiver characteristics, and presently includes U.S. coastal areas and large portions of the continent, with the exception of a midcontinent gap that is to be plugged by two new chains with four new stations and linked to existing chains.

While originally intended for ships and aircraft on intercontinental routes, LORAN-C has domestic applications in aviation for non-precision approaches, area navigation, and direct instrument flight rules (IFR) routing, as well as automatic vehicle monitoring, electronic maps, and resource management. The USCG estimates there are 40,000 users in the aviation services alone. However, LORAN-C can also be used for the distribution by radio of precise time and frequency, which is the topic of this section.

The LORAN-C system operates in the low-frequency (kilometric) band of 90 to 110 kHz using pulse-coded modulation. For navigation purposes a LORAN-C chain consists of a master and three or more slave stations, all operating at a designated repetition rate in the 100-ms range. A chain provides differential time-of-arrival measurements that establish position in a hyperbolic coordinate system

to within 500 m under most conditions and to within 30 m (100 ns) under the best conditions.

During its designated repetition interval, each LORAN-C master and slave station emits a group of eight phase-coded 100-kHz pulses transmitted at 1-ms intervals, with different phase codes used for the master and slaves and for even and odd repetition intervals. Accurate time measurement to the order of 100 ns requires precise envelope and zero-crossing determination to provide adequate signal-to-noise ratio and to discriminate against multipath due to sky waves (ionospheric reflections), especially at night. A precisely controlled pulse shape is used to maximize accuracy with achievable transmitter power and bandwidth constraints.

To retain precise timing, each LORAN-C master station is equipped with three cesium clocks and two sets of timing equipment, which are continuously displayed and compared with each other. Slave stations synchronize to the master transmissions. The signals transmitted by the master and slave stations of a chain are monitored by antenna sensors and by remote receivers at various locations in the service area and along the base lines. Monitor updates including time differentials and received power and noise levels are sent via landline to the stations, which compute phase adjustments in 20-ns increments.

Station timekeeping within a chain is usually better than 50 ns relative to the master cesium clock; however, monitored deviations of 100 ns or more are indicated in the transmitted signals by "blinking" certain pulses. The master cesium clocks may drift 60 ns on a day-to-day basis, but are maintained within $2.5\ \mu\text{s}$ of NIST standard time using corrections determined manually and published weekly. With automatic means it is estimated that this accuracy can be improved to 500 ns.

The design of the present generation of LORAN-C stations uses solid-state devices extensively, but includes no specific protection against the electromagnetic pulse (EMP) phenomenon from high-altitude nuclear explosions. However, these stations are usually located in remote areas and if necessary can operate from independent power sources for weeks without onsite operators or coordination. Since for timekeeping purposes only one station of a chain is necessary and most areas of the country are within the service area of multiple stations, a considerable degree of redundancy is available.

According to U.S. Department of Defense (DoD) and U.S. Department of Transportation (DoT) policy and plans for future radionavigation systems, use of LORAN-C by the government may be phased out over the next 10 years in favor of GPS, which is satellite based.

The following quotations¹³ are relevant:

LORAN-C provides navigation, location and timing services for both civil and military air and surface users. It is the Federally provided navigation system for the United States Coastal Confluence Zone (CCZ). LORAN-C is approved as a supplemental air navigation system. Signal monitors necessary for LORAN-C guided nonprecision approaches will be installed and become operational in 1989. By 1990, additional transmitting stations will be installed to complete signal coverage over the 48 conterminous states. The LORAN-C system serving the continental United States (including Alaska) and the coastal areas will remain a part of the navigation mix into the next century. DoD will phase out military use of overseas LORAN-C transmitting stations established for military use that do not serve the North American continent.

GPS is a DoD developed, worldwide, satellite-based radionavigation system that is scheduled to provide three-dimensional coverage by 1991. The GPS Precise Positioning Service (PPS) will be restricted, due to national security considerations, primarily to the military. However, under certain circumstances, PPS will be available to qualified civil users.

OMEGA⁶

OMEGA is a worldwide very-low-frequency (myriametric) radionavigation system for maritime and aeronautical enroute navigation. The system comprises eight high-power transmitting stations operating on frequencies in the range 10.2 to 13.6 kHz. Navigational position is determined by comparing the relative phase differences of received signals; however, this results in lane ambiguities that must be resolved by other means. The accuracy of these comparisons is limited by propagation corrections, which depend on location and time, and result in a navigational accuracy of 2 to 4 nautical miles.

In principle, the worldwide coverage and relatively stable propagation conditions possible at OMEGA frequencies would make this system highly useful for worldwide dissemination of time and frequency. Unfortunately, as mentioned in the section on LORAN-C, future operation of the OMEGA system is in doubt and may be discontinued if GPS proves reliable and economically viable.

Global Positioning System⁶

The Global Positioning System is a worldwide satellite-based radio-navigation system developed by the DoD and operating on two L-band (decimetric) microwave frequencies at 1227.6 MHz and 1575.42 MHz. When completely deployed as planned over the next few years, the system will consist of a constellation of 18 satellites in near-earth orbit, with at least four satellites necessary to provide accurate horizontal and vertical position information.

The key to accurate position determination with GPS lies in accurate determination of satellite position, which is aided by an on-board ephemeris table in each satellite. The tables are continuously updated by information transmitted to the satellite by the system control station and relayed to the users via the L-band transmissions. These transmissions are also modulated in quadrature by two pseudorandom sequences for range determination from the satellite to the user. One of these sequences provides accuracy to within 500 m and is intended for civil use. The other provides accuracy to within 20 m horizontally and 30 m vertically, but is currently classified and available only for U.S. military use.

There remain considerable uncertainties about the accuracy, reliability, and availability of satellite-based secondary time-distribution systems such as GPS, especially in areas where LORAN-C is available. Satellite-based systems such as GPS can provide differential time measurements to an extraordinary precision; however, with current DoD policy the accuracy achievable with GPS for civil users is in the same range as LORAN-C.

Portable Clocks and Transfer Standards⁶

Portable cesium clocks have been constructed for the purpose of calibrating local time and frequency standards when other means are not available and as a backup for these means when available. These clocks are intended for equipment calibration only and not as a substitute for the regular, in-service methods based on LORAN-C and other systems discussed in previous sections.

At one time NIST advocated calibrating local time and frequency standards using the 3.579545-MHz color-burst signal transmitted by the television networks and, indeed, the New York studios of all three networks were equipped with precision oscillators for this purpose. Assuming the offset of these oscillators was known (published periodically, for example), then it would be a simple matter to calibrate a

local standard, as long as the signal available locally was synchronous relative to the oscillator.

Unfortunately, the advent of frame buffers, in which the television frame is buffered locally and made synchronous with the local-station timing generator, destroyed the accuracy of this method and it is no longer viable in most areas.

Disciplined Frequency Standards¹

Quartz crystal oscillators have been used as frequency references for many years, since they are compact, relatively inexpensive, and stable. A suitably designed and temperature-stabilized crystal oscillator should be stable within a few parts in 10^{10} per day and be adjustable to a precise reference, such as a cesium clock. However, typical crystal oscillators will show a gradual departure from nominal frequency with time, known as the aging rate. Thus, an uncorrected crystal oscillator may not satisfy the requirements for telephone network synchronization. A disciplined frequency standard (DFS) incorporates a precision quartz crystal oscillator together with a mechanism to measure its departure from a primary reference source and generate corrections accordingly. In the form used by several digital networks the corrections are generated by a LORAN-C receiver and implemented in the form of a digital phase-locked loop. The loop can include provisions to estimate the particular crystal aging rate, as well as ensure stable operation during intervals when the primary reference signal is not available (holdover).

The design of typical stratum-2 and stratum-3 clocks (see definitions below) is based on the same principles of DFS, except that in these cases the primary reference signal is not a LORAN-C receiver, but the chosen timing reference signal at either the same or lower stratum. A typical clock design for the DMS-100 family of telephone switches has been described.⁸

5. GENERAL SYNCHRONIZATION ISSUES^{1,3,5}

The primary reason for worrying about synchronization is to avoid frame slips due to mismatched clocks at the ends of a digital transmission link. General issues on the design and stabilization of clock-distribution networks are discussed in publications cited in notes 3, 4, and 5. In the case of a 1.544-Mbits/s DS-1 link and mismatched

TABLE B-3 Slip Probability

Syntonzation Error	Time Between Slips	Probability of at Least One Slip per Day	Probability of at Least One Slip per Week
0^{-11}	Infinity	0.0	0.0
10^{-10}	145.0 days	0.007	0.05
10^{-9}	14.5 days	0.07	0.5
10^{-8}	1.5 days	0.7	1.0
10^{-7}	3.5 hours	1.0	1.0

TABLE B-4 Clock Stratum Assignments

Stratum	Minimum Accuracy	Minimum Drift	Interval Between Slips	Switch Assignments by AT&T
1	1×10^{-11}	NA	72 days	BSRF
2	1.6×10^{-8}	1×10^{-10}	14 days	4ESS
3	4.6×10^{-6}	3.7×10^{-7}	5.6 min	5ESS
4	3.2×10^{-5}	NA	3.9 s	POP

clocks of given syntonization error, for example, the expected number of slips involving the loss or duplication of a 125 μ s frame is given by Table B-3.

Clock Stratum Assignments

Given the accuracy of frequency distribution, as evident from the foregoing discussion, the question is not whether slips will occur, but how often. The industry has agreed on a classification of clocks as a function of minimum accuracy, robustness, and other issues. This classification is based on what is called the stratum level, with more accurate clocks assigned the lower-numbered strata and less accurate clocks the higher-numbered strata. Table B-4 summarizes the stratum assignments.

By industry agreement through the American National Standards Institute (ANSI T-1 Committee), all digital synchronization networks must be controlled by a primary reference standard (PRS). The PRS must maintain a long-term accuracy of 10^{-11} or better

with verification to UTC using a portable clock and is, by definition, a stratum-1 clock. Such a device is expected to be monitored continuously to precisions in the order of 100 picoseconds (ps).

The AT&T Basic Synchronization Reference Frequency (BSRF) of 2.048 MHz, which is derived from three cesium clocks at Hillsboro, Missouri, meets these requirements. Other clocks, including disciplined oscillators controlled by LORAN-C or GPS, are not considered stratum 1, since they are not directly traceable to UTC; however, this distinction may not be significant for practical purposes.

Stratum-2 clocks represent the stability required for interexchange toll switches such as the No. 4 Electronic Switching System (4ESS) and interexchange digital cross-connect systems, while stratum-3 clocks represent the stability required for exchange switches such as the No. 5 Electronic Switching System (5ESS) and local cross-connect systems. Stratum-4 clocks represent the stability required for digital channel banks and private branch exchange (PBX) systems.

Additional rules required for digital synchronizing networks require that, for each stratum, timing comes from equal or lower-numbered stratum levels (that is, higher accuracy), and that no timing loops exist. Besides requiring a minimum accuracy at each stratum level, the rules require that the pull-in range of a clock be adequate to lock onto another clock of equal or lower-numbered stratum when both clocks are started at the limits of their tolerances.

It is assumed that satellite links are not used to carry timing and that the best facilities (most error free) are used. Stratum-2 and stratum-3 clocks must have diverse primary and secondary timing sources, show little effect of source switching, and have accurate holdover in case of complete loss. Stratum-3 and stratum-4 clocks must switch sources if the current timing signal source is defective (for example, out-of-frame synchronization).

Error Discussion and Analysis

The performance of a slave clock synchronized to a master clock of specified accuracy can be described as follows. Let $X(t)$ be the slave clock timing error relative to an absolute reference.

$$X(t) = y_0 t + (1/2) D t^2 + e_{pm} + \int e_{fm}(t) dt,$$

where

t	=	time
y_o	=	frequency offset due to reference error
D	=	drift during loss of signal (holdover)
e_{pm}	=	white PM (phase noise) due to jitter and short-term oscillator instability
$e_{fm}(t)$	=	white FM (frequency noise) due to long-term oscillator instability under stress.

The noise terms are due to digital implementation quantization effects, which affect the phase-detector resolution and the ability to set precise frequency, as well as random phase walk and biased phase walk resulting from short disruptions. For instance, a four-link system model with exponential arrivals of outages (mean 5 hours) and uniform outages (0 to 1 s) shows about 1- μ s daily phase variation and 2.7 μ s weekly.

The accuracy achieved by the slave clock also depends on the synchronization path to the master. This path may be disturbed by any one or more of several mechanisms, including facility error bursts and short outages, frame-jitter, phase hits (sudden phase changes), protection switching, and equipment diagnostics. Most of these effects can be minimized with proper system design, including phase memory (build-out), which avoids phase hits when resynchronizing after a short outage or when the synchronization path is changed. Unfortunately, not all telephone equipment includes these features.

The performance of a clock synchronized via a facility can be expected to degrade as the result of temperature changes and other environmental effects. Table B-5 shows the expected daily and yearly variation (wander) for various facilities.

As a specific example, a 30-mile round trip between two typical exchanges showed a diurnal variation due to temperature variations of 200 ns and a pulse-stuffing wander of 75 ns root mean square (RMS).

6. SYNCHRONIZATION NETWORKS¹

The public communication network evolved using a hierarchical configuration. The longer the distances covered by the telecommunications channels, the greater was the chance for some of the synchronization problems discussed above.

As a result a top-down hierarchical approach was used for the synchronization network of the United States prior to the breakup of

TABLE B-5 Facility Delay Variation

Facility and Length	Daily Variation (ns)	Yearly Variation (ns)
Radio link, 1,000 km	210	420-580
Coaxial cable, 1,000 km	57	860
Fiber optic, 1,000 km	110-160	1,690-2,440
Twisted pair		
Polyethene, 100 km buried	100	1,500
Polyethene, 50 km aerial	830	2,080
Paper, 50 km buried	160	2,360
Paper, 250 km aerial	14,000	36,000

the Bell System. This called for four levels or strata with successively less accuracy required from the first level downward. The first level or stratum is the primary reference standard.

As the technology and services of the nationwide network have changed, the AT&T network has been divided into three varieties: one for analog facilities, one for digital facilities, and one for the Digital Data System (DDS).

The following sections contain a brief outline of the plans and present status of synchronization networks used by various U.S. carriers today.

American Telephone and Telegraph Company

The existing AT&T synchronization network is based on the AT&T Basic Synchronization Reference Frequency PRS of 2.048 MHz, which consists of three cesium atomic clocks that maintain stratum-1 accuracy of 10^{-11} . It originates at Hillsboro, Missouri, and is distributed via analog facilities without intermediate multiplexing to subscribing BOCs and other users. The distribution network covers most of the country, including areas now served by BOCs, which are charged a fee for use. The network uses analog facilities and is intricately engineered to avoid loops.

The BSRF was the original source of synchronization that linked all the stratum-2 digital switches. It is distributed to all AT&T switches by analog or digital carrier. These switches provide the stratum-2 level reference to all local exchange carriers (LECs) via digital facilities, generally DS-1, 1.544-Mbits/s lines.

AT&T specifications for local timing supplies allow a maximum

daily wander of 18 μ s, which has been adopted as an American National Standard. Equipment normally operating at stratum 2, including the 4ESS switch, is engineered to this specification. Equipment normally operating at stratum 3, including the 5ESS switch and digital automatic cross-connect systems (DACs), is engineered to a looser standard of 90 μ s. The long-term equipment accuracy is expected to be in the range of 10^{-11} with 4 to 10 transmission links.

AT&T does not intend to operate this network indefinitely. The BOCs (see below) are planning their own synchronization networks and to discontinue use of the BSRF when these become operational. Over the next 10 years, AT&T intends to replace the existing analog network with 12 timing islands, each with a PRS consisting of two rubidium-controlled timing generators, a GPS receiver, and a monitor and control computer to provide performance verification. The stratum-1 accuracy is in concurrence with the International Consultative Committee on Telegraphy and Telephony (CCITT) standards and will be better than 10^{-11} over the long term (that is, 20 years).

The new AT&T sources should not introduce any impairments into the local exchange networks, since the stratum-1 accuracy will be maintained and there are no direct connections to this network.

The choice of clock sources, a local stratum-1 clock or acceptance of BSRF, is basically a business decision of the LECs, since both alternatives are technically suitable. Accepting synchronism from the BSRF network requires no additional equipment, no specialized installation, and no specialized maintenance. A stratum-1 clock requires special surveillance and maintenance, as well as trained personnel to operate the system.

From now to the year 2000 there should be little change in synchronism strategy among the BOC LECs. Some might implement stratum-1 clocks as test beds should any major problems arise. As switches, the key for trouble-free synchronization will be accurate maps and records of transmission facilities utilized for synchronization purposes so that loops will be avoided. Each BOC LEC has one or more synchronization coordinators whose function it is to keep the maps current and provide technical help as required.

Bell Communications Research, Incorporated

Prior to divestiture the RBOC facilities were an integral part of the AT&T synchronization network. There were two digital synchronization networks under AT&T control, one for switched digital services

(4ESS) and the other for the DDS. Following divestiture the BOCs are responsible for synchronizing their own local access transport areas (LATA), which now number over 160. Some of the BOCs make use of AT&T facilities, while others maintain a PRS using cesium clocks or a DFS slaved to LORAN-C.

In 1986 Bell Communications Research, Incorporated (Bellcore) published a plan for network synchronization⁹ that was later incorporated as an ANSI standard.¹⁰ The standard establishes tolerances in frequency, jitter, and wander for each clock stratum, as well as service objectives, impairment allocations, and strategies for interconnecting clocks in a network. It also specifies strategies for deployment and evolution, as well as protection strategies and use of nonstratified clocks.

The Bellcore plan includes an extensive discussion of synchronizing principles for use within a physical facility or building. Each such facility uses a single building integrated timing supply (BITS) clock, which obtains timing from a clock of equal or lower-numbered stratum and has duplicated circuitry and provisions for backup timing via diverse routes. The BITS clock is distributed to all equipment in the facility in such a way that no timing loops will occur, either in normal operation or under abnormal operation involving any combination of backup links. A timing loop occurs when a timed clock receives timing from itself via a chain of timed clocks. Timing loops are undesirable for two reasons. First, all the clocks in the timing loop are isolated from the timing source (that is, a timing path does not exist from a timed clock to the timing source). Second, frequency instabilities may arise because of the timing reference feedback.

MCI Communications Corporation

MCI Communications Corporation (MCI) currently has six major switching centers operating in 12 plesiochronous islands. Each of these islands has a PRS consisting of a DFS with a disciplined oscillator, LORAN-C receiver, and antenna. The DFS operates as a stratum-1 clock and generates 308 kHz for analog equipment and 2,048 kHz for digital equipment to an accuracy of 10^{-11} . The synchronizing tree is organized as master-slave with backup and has an expected service life beyond the year 2000.

The MCI design pays careful attention to the multiple-station LORAN-C deployment. The LORAN-C receiver locks to the strongest station available, but needs only one station (master or slave)

in a chain. If this station is lost, the receiver automatically searches for and locks to one of the remaining stations. If no station can be found after 2.5 hours, the system enters holdover mode and switches to the disciplined oscillator.

The disciplined oscillator uses a temperature-stabilized high-precision crystal oscillator normally locked to the LORAN-C receiver. Its control circuitry memorizes the intrinsic crystal drift and aging rate and corrects for these quantities during periods when the LORAN-C signal is lost. The DFS normally stays within 10^{-10} of the initial frequency during these periods for up to 10 days.

Timing distribution within the island uses a pre-engineered spanning tree. The design avoids long synchronizing paths and allows few clock nodes on each path. Although each island operates with its own DFS and would ordinarily be considered plesiochronous, different islands may be synchronized to the same LORAN-C chain and thus be considered synchronous. Obviously, this would not be possible in all failure scenarios.

MCI plans in the future to use BITS principles. The BITS design imposes a master-slave hierarchy for timing distribution within a physical facility or building. The design of the clock distribution equipment (CDE) includes provisions to smooth and "deglitch" the received timing signal, usually in the form of one or more DS-1 signals, and distribute it within the facility over a loop-free synchronization tree with backup. The CDE is also expected to provide higher-order synchronization for DS-3, Synchronous Optical Network (SONET), and so forth.

CONTEL/ASC

The CONTEL/ASC network includes extensive use of satellite and microwave facilities, in addition to digital fiber. Because of the Doppler shift inherent in satellite systems, special consideration must be given to buffering and timing issues. CONTEL/ASC uses a single dual-redundant DFS slaved to a LORAN-C receiver as the PRS for the national network. Each major central office is synchronized directly to the PRS with claimed minimum stability of 6×10^{-12} per day.

US Sprint Communications Company

The network of the US Sprint Communications Company (US Sprint) includes 45 switches at 28 locations interconnected by over 23,000

TABLE B-6 Synchronizing Failure Estimates

Cause of Failure	Master/Slave	PAMS	
		No Diversity	Diversity
MTBF ^a	10 months	3 years	94 years
MTTR ^b	2-8 hours	8 hours	2 hours
Common failures	Cable cuts, repeater failure	Cable cuts, circuit failure, interface failure	Change-over

^aMTBF: mean time between failure.

^bMTTR: maximum time to repair.

route miles of digital transmission facilities, mostly fiber operating at up to 565 Mbits/s. In comparison with other carriers, US Sprint has many long spans and few diversity routes. After study of several alternatives, US Sprint decided on an approach using a dual-redundant PRS at every switch location. The PRS plan is similar to MCI and involves the eventual deployment of duplexed LORAN-C receivers at all 28 switch locations.

7. IMPACT OF SYNCHRONIZATION IMPAIRMENTS^{1,12}

An analysis of network reliability, based on various considerations of topology and route diversity, is shown in Table B-6. The master/slave column presumes a synchronizing tree with no diversity or alternate routing. PAMS is a distribution system that provides alternate routing with and without route diversity. A failure assumes the loss of all primary and secondary synchronization paths to clocks of lower strata and implies the use of local clocks operating at the stratum level of the equipment itself.

The effects of synchronization impairments (disruption or failure) depend strongly on the type and severity of the underlying cause and on the particular user application. In the following subsections, the effects of synchronization impairments will be assessed on transmission, network elements, and user applications. Subsequent sections will address the implications on NSEP survivability.

Effects on Transmission

Imperfect digital network synchronization can cause two principal types of transmission impairments: controlled slips and burst errors.

Controlled Slips

A controlled slip, which is the deletion or repetition of one frame (193 bits) of a DS-1 bit stream, occurs if the timing source of the transmitting network equipment at the sending end of a digital link is not synchronized with the timing source of the network equipment at the receiving end of that link. The interval between controlled slips is inversely proportional to the frequency offset between the two timing sources. The typical end-to-end performance objective for digital transmission under normal network conditions is one slip every 5 hours.

Burst Errors

A burst error, which is the transmission of a stream of errored bits, can be due to faulty transmission equipment (for example, broken line cards), protection switching, lightning strikes, and maintenance operations. Burst errors, while not caused by synchronization impairments, can be magnified and propagated by certain synchronization configurations. If a burst error of sufficient severity occurs on the incoming line that is providing timing to transmission equipment with a stratum-4 clock, then all of the output lines from that equipment may suffer magnified burst errors. (Channel banks, T-1 multiplexors, and digital PBXs typically have stratum-4 clocks.) This magnification and propagation of burst errors typically do not provide phase continuity when switching from one timing source (primary input, secondary input, or internal oscillator) to another.

Reframes

A reframe is the operation of recovering or initially finding the reference bit in a 125- μ s DS-1, DS-2, and so on, frame. Reframes can occur when equipment is first turned on, when a protection switch occurs, and when the maintenance operations are performed.

As a practical matter, reframes are fairly rare on today's telephone network and are of brief duration from a few milliseconds to several seconds. However, reframes may be expected to arise in

TABLE B-7 Dual-Tone Multifrequency Signaling Survivability

System	Stratum	Days to Exceed Frequency Offset
L5E	2	170
TD radio	3	120
TD radio	4	12

NSEP scenarios when the damage level is high enough to produce any of the above situations and may last longer than several seconds in extreme cases.

Effects on Network Elements

Synchronization impairments can affect any frequency-sensitive network element, including both digital and analog systems. The following analog systems are most frequency sensitive, in decreasing order of sensitivity:

- Dual-tone multifrequency signaling (DTMF)
- Multifrequency signaling (MF)
- Single-frequency signaling (SF)
- Voice.

DTMF, when used to address the local switching office, almost never undergoes frequency translation and, hence, is dependent only on the telephone set from which it originates. When DTMF is used for end-to-end signaling, such as in a Nationwide Emergency Telecommunications Service (NETS) application, then the frequency offsets must be controlled within ± 10.5 Hz. Assuming worst-case scenarios for selected transmission systems, the estimated interval this requirement can be met, following loss of outside timing source, is shown in Table B-7.

Synchronization impairments due to controlled slips result in a loss or replication of a 125- μ s frame. The impact on DTMF signaling could be a missed digit if a minimum 50-ms DTMF signal was being transmitted. Speech is virtually unaffected. The maximum worst-case slip rate in digital systems is about 265 slips/hour. This is an order of magnitude better than the bit error rate (BER) limit of 10^{-4} on a T-1 trunk. There may be some equipment operating with

TABLE B-8 Impairments Due to Controlled Slips

Application	Effect on Transmission Quality
Voice	None
Voiceband data	$\leq 1,200$ bits/s, none; $> 1,200$ bits/s, errors
Secure voice	Loss of secure connection, session rekey required
Digital data	Single-byte dropped or repeated
Facsimile	Small, illegible areas
Video	Mild picture breakup and freezing, garbled audio

TABLE B-9 Impairments Due to Isolated Burst Errors

Application	Effect on Transmission Quality
Voice	Mild noise
Voiceband data	Data errors
Secure voice	Loss of secure connection, session rekey required
Digital data	Severe data loss
Facsimile	Large, illegible areas
Video	Severe picture breakup and freezing, severely garbled audio

2,400-bits/s modems that may well be affected by 265 slips/hour, but new designs planned will eliminate the known problems.

Effects on User Applications

It is not possible, in general, to specify with certainty the effects of particular transmission impairments on user applications, because these effects often depend on the exact timing of the impairment and on the exact contents of the user information being transmitted. It is possible, however, to specify what effects on user applications are typical for different types and severity of transmission impairments. Tables B-8 and B-9 summarize these effects for three levels of transmission impairment for typical user applications.

The three transmission impairments considered in the table are isolated controlled slips, isolated burst errors (for example, a 100-ms period with a BER of 10^{-2} every 4 s), and consecutive burst errors

TABLE B-10 Impairments Due to Reframes

Application	SES ≤ 1 s	CSES > 5 to 7 s
Channel bank, cross-connect	Audible but inoffensive	Disconnect after 5 s
Data transmission		Re-login required
Analog facsimile	Some unreadability in patches	Unreadable
Video codec	Detectable effect	Still usable

(for example, a 250-ms period with a BER of 10^{-2} each second for eight consecutive seconds).

The six user applications considered are voice 64 kbits/s pulse code modulation (PCM) or 32 kbits/s Adaptive Delta PCM (AD-PCM), voiceband data (with modem), secure voice (STU III with 2,400-bits/s-modem), digital data (64 kbits/s), facsimile (group 3), and video (1.544-Mbits/s) coder-decoder (codec). Table B-8 shows the effects of controlled slips on these applications.

While users might notice these effects, most would probably elect to continue the present connection, especially if error-detection and correction procedures were incorporated in the protocol design. Table B-9 shows the effects of isolated burst errors on the applications. Users would certainly notice these effects and may choose to abandon the connection and retry.

In the case of consecutive burst errors the user most likely would find the connection unusable and abandon it. In fact, the transmission equipment, noting the severely degraded state of the link, usually declares it inoperable and drops the connection itself. The effects of reframes are summarized in Table B-10. The kind of application is listed in the first column and the second and third columns list two successively more severe disruption classes. SES means severely errored (more than 10^{-3} BER) seconds and CSES means consecutive occurrences of SES seconds.

8. SENSITIVITY OF NATIONAL SECURITY EMERGENCY PREPAREDNESS TO SYNCHRONIZATION IMPAIRMENTS¹²

The preceding discussion has emphasized the mechanism and effects of synchronization impairments within the telephone network itself

and the resulting impact to the various user applications. This section assesses the impact of these impairments to the programs of the NLP/NSEP. These programs include NETS, Commercial Satellite Interconnectivity (CSI), and Commercial Network Survivability (CNS).

The main motivation in this paper is to determine whether there may be problems due to synchronization impairments in the public switched networks that could lead to unacceptable performance or loss of useful NSEP capabilities of any of the various services required by the National Communications System (NCS). This is to be contrasted with the question of whether there may be perceptible degradation under natural or man-made abnormal stresses—for example, measurable increase in bit error or message delivery time which, of course, may be most important items under normal conditions for public network users.

Degradation or loss of services due to natural effects such as storms and earthquakes will be of limited geographical extent. Probably the worst case that one can consider is a complete loss of the primary synchronization of stratum-1 digital switches. However, such loss would have negligible effect on NSEP services because the system architecture and other strata in the system would be adequate for very long time periods. Synchronization degradation from man-made events includes vandalism, sabotage, direct attack with nuclear weapons, and so forth.

Reflection on the attractiveness of attacking synchronization elements compared to other system components such as common channel signaling (CCS), large switches, and so forth, led to a consensus that synchronization was not a major player in such postulated events and will not be through the year 2000.

Nationwide Emergency Telecommunications Service

In general, there are two potential synchronization and timing concerns in NETS: (1) frame slips, when the divided network must be used in a plesiochronous mode and (2) resynchronization.

Overall, neither concern is of major consequence if network issues are separated from terminal device (or customer-premises equipment) issues. The network will hold up quite well under frame slips. Even under severe conditions, slips appear to cause little network impact. Resynchronization is the more catastrophic event. Here links

are interrupted, circuits are lost, and surviving islands may be forced to operate with relatively unstable timing.

Commercial Satellite Interconnectivity

The only new issue the CSI plan raises relative to synchronization are the effects of the satellite transmission characteristics of the connected T-1 link. The timing hierarchy algorithms used on the public switched networks takes synchronization from the highest surviving stratum. A connection between two main islands by satellite will encompass two more switches. This means that it is highly likely that there will be a stratum-2 clock, or better, in one of the two islands. As synchronization timing is taken from the better of the two sources, synchronization does not appear to be an issue other than through the jitter corruption of the timing through the T-1 link and through the satellite channel delay. This does not appear to be a significant issue.

Commercial Network Survivability

Since the CNS program essentially offers only a skinny analog bandwidth voiceband connection, the usual concerns about timing and synchronization are not applicable. (It is noted that in the older single sideband [SSB] radios used, crystal frequency setting was marginal. Human operator tweaking was required to keep the links going. Parenthetically, this is standard operating practice for these older radio units. More important than the results of the early make-do type experiments was the concept itself.) Better technology radio equipment would permit less manual interaction in setting up connections. As the evolution to T-1 is moving along rapidly, digital multiplexed carriers may be the more likely long-term direction of evolution. The analog connection may be an interim step along the way, but one not to be overlooked.

9. CONCLUSION AND RECOMMENDATION

From the foregoing analysis the committee reaches the following conclusion and recommendation:

No significant synchronization timing issues for national security emergency preparedness appear to exist, because timing is set by the connected surviving access tandem.

As existing network synchronization levels already exceed those required for national security emergency preparedness, no action need be taken to increase the robustness of network synchronization beyond existing standards for normal network operation; designers of terminal devices should engineer them to operate satisfactorily under system synchronization standards.

NOTES

1. Briefing material on file with the Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications.
2. *Time and Frequency Dissemination Services*. 1979. NBS Special Publication 432. Washington, D.C.: U.S. Department of Commerce.
3. Lindsay, W. C., and A. V. Kantak. 1980. Network synchronization of random signals. *IEEE Transactions on Communications COM-28* (8 August):1260-1266.
4. Braun, W. B. 1980. Short-term frequency effects in networks of coupled oscillators. *IEEE Transactions on Communications COM-28* (8 August):1269-1275.
5. Mitra, D. 1980. Network synchronization: Analysis of a hybrid of master-slave and mutual synchronization. *IEEE Transactions on Communications COM-28* (8 August):1245-1259.
6. Jordan, E. C., ed. 1985. *Reference Data for Engineers*, 7th ed. New York: H. W. Sams & Co.
7. Davies, K. 1966. *Ionospheric Radio Propagation*. NBS Monograph 80. Washington, D.C.: National Bureau of Standards.
8. Munter, E. A. 1980. Synchronized clock for the DMS-100 family. *IEEE Transactions on Communications COM-28* (8 August):1276-1284.
9. Bell Communications Research, Incorporated. 1986. *Digital Synchronization Network Plan*. Technical Advisory TA-NPL-000436. Livingston, N.J.: Bell Communications Research, Incorporated.
10. American National Standards Institute. 1987. *ANSI T1.101-1987: Synchronous Interfaces for Digital Networks*. New York: American National Standards Institute.
11. U.S. Naval Observatory (private communication). 1988.
12. Information provided by expert committee members.
13. Beser, J., and B. W. Parkinson. 1982. The application of NAVSTAR differential GPS in the civilian community. *Navigation* 29(Summer).

Glossary

AC	alternating current
ADPCM	adaptive delta pulse code modulation
ANSI	American National Standards Institute
AT&T	American Telephone and Telegraph Company
BCD	binary-coded decimal
BER	bit error rate
BITS	building integrated timing supply
BOC	Bell Operating Company
BSRF	Basic Synchronization Reference Frequency
CATV	cable television
CCITT	International Consultative Committee on Telegraphy and Telephony
CCS	common channel signaling
CCZ	Coastal Confluence Zone
CDE	clock distribution equipment
CENTREX	central exchange
CI	carrier interconnection
CMTS	Cellular Mobile Telephone Services
CNS	Commercial Network Survivability
CONUS	coterminous United States
CPE	customer-premises equipment
CSI	Commercial Satellite Interconnectivity
DACS	digital automatic cross-connect system
DDS	Digital Data System

DFS	disciplined frequency standard
DNHR	dynamic nonhierarchical routing
DoD	U.S. Department of Defense
DoT	U.S. Department of Transportation
DSP	digital signal processing
DTD	digital time division
DTMF	dual-tone multifrequency signaling
ECSA	Exchange Carrier Standards Association
EO	Executive Order
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FDDI	fiber digital distribution interface
5ESS	No. 5 Electronic Switching System
4ESS	No. 4 Electronic Switching System
GOES	Geosynchronous Orbiting Environmental Satellite
GPS	Global Positioning System
HDTV	high-definition television
IDTV	improved definition television
IEC	interexchange carrier
INTELSAT	International Telecommunications Satellite Organization
ISDN	integrated services digital network
LAN	local area network
LATA	local access transport area
LEC	local exchange carrier
LED	light-emitting diode
LMSS	land mobile satellite systems
LORAN-C	Long-Range Navigation System-C
MAN	metropolitan area network
MCI	MCI Communications Corporation
MF	multifrequency signaling
ms	milliseconds
μ s	microseconds
MTBF	mean time between failure
MTSO	mobile telephone switching office
MTT	mobile transportable telecommunications
MTTR	maximum time to repair
NASA	National Aeronautics and Space Administration
NBS	National Bureau of Standards
NCC	National Coordination Center
NCS	National Communications System

NETS	Nationwide Emergency Telecommunications Service
NIST	National Institute of Standards and Technology
NLP/NSEP	National-Level Program/National Security Emergency Preparedness
NRC	National Research Council
ns	nanoseconds
NSDD	National Security Decision Directive
NSEP	national security emergency preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTSC	National Television Standards Committee
ONA	Open Network Architecture
OSI	open system interconnection
PBX	private branch exchange
PPS	Precise Positioning Service
PRS	primary reference standard
ps	picoseconds
PSN	public switched networks
PUC	public utility commission
RBOC	Regional Bell Operating Company
RMS	root mean square
SF	single-frequency signaling
SLC-96	Subscriber Loop Carrier-96
SNA	System Network Architecture
SONET	Synchronous Optical Network
SSB	single sideband
STP	signal transfer point
TAI	International Atomic Time (Temps Atomique International)
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	time division multiple access
TSP	Telecommunications Service Priority
ULSI	ultra large scale integration
UT	Universal Time
UTC	Coordinated Universal Time (Universal Time, Coordinated)
VAN	value-added network
VLSI	very large scale integration
VSAT	very small aperture terminal
WAN	wide area network



National Academy Press

The National Academy Press was created by the National Academy of Sciences to publish the reports issued by the Academy and by the National Academy of Engineering, the Institute of Medicine, and the National Research Council, all operating under the charter granted to the National Academy of Sciences by the Congress of the United States.