To reform political campaigns, Congress could consider the following options:

- extend public funding, such as that provided to presidential candidates, to congressional candidates, State or local candidates, and nonprofit groups; 152
- reconsider and extend the limits on individual campaign contributions; [153]
- decrease the amounts that PACs can contribute to a candidate or establish an overall limit on the PAC contributions that Federal candidates can accept; [154]
- restrict the length of the campaign season; 155
- clarify what is meant by "lowest unit rate" that can be charged for political broadcasting; [156]
- provide free media time to candidates for Federal offices; 157
- initiate legislation placing limits on the amount of money that can be spent on political advertisements; [158]
- impose standards on the form of political advertisements, thereby making them more uniform, cheaper, and less subject to price differences; [159]
- hold hearings to assess the impact of negative advertising on recent Federal elections and consider ways to regulate negative advertising;
- investigate the impact of media practices, such as news-program coverage of political candidates [160] and polling; [161] and
- investigate the influence of political consultants and the impact of technology-supported campaign practices.

---

[152] In the 100th Congress, the focal point of such efforts was the Senatorial Election Campaign Act of 1987 (S.2), introduced by Senators Boren and Byrd, which provided public financing and spending limits in Senate elections. Republicans opposed to spending limits and public funding were able to filibuster the bill. For a review of campaign financing reform, see Joseph E. Cantor and Thomas M. Durbin, "Campaign Financing," Library of Congress, Congressional Research Service, CRS Issue Brief, May 12, 1988,

[153] One loophole that Congress created in 1979 is that national parties can solicit unlimited contributions from corporations, labor unions, and individuals for State and local parties, routine expenses, and party-building activities. See Charles R. Babcock, "$100 Million in Campaign Donations Belie Notion of Federal Limits," *The Washington Post, Nov. 8, 1988,* p. A12, and Carol Matlack, "Backdoor *Spending,' 'National Journal,* Oct. 8,1988, pp. 2516-2519.

[154] A number of such bills have been proposed, including the Campaign Reform Act of 1987 (H.R. 166), the Comprehensive Campaign Finance Reform Act of 1987 (H.R. 573), the Senate Campaign Cost Limitation and Public Financing Act (S.645, S.725), and the Bipartisan Commission and Congressional Campaign Financing Act (S.1672). See Cantor and Durbin, op. cit., footnote 151, p. 6. Such changes, however, could be sidestepped by PACs increasing their independent expenditures, which under *Buckley* cannot be limited.

[155] A restricted Campaign season could be a requirement for receiving public funding, as is presently the case. Affecting the length of campaigns might also be accomplished by reforming the nominating process. Either a national primary or a regionat primary might restrict the length of pre-convention campaigning. Kevin J. Coleman, "The Presidential Nominating Process: The Regional Primary Movement and Proposed Reforms," Library of Congress, Congressional Research Service, CRS Issue Brief IB861 17, Mar. 7, 1988.

[156] The Campaign Cost Reduction Act (S. 2627) would establish that a station's charge for preemptible political time would have to equal its lowest preemptible rate for that spot, and that a fixed spot rate could be no more than one-half again the preemptible rate. "Congress Looks for Better Deals on Campaigns," *Television/Radio Age,* Oct. 3, 1988, p. 17.

[157] For example, in the 100th Congress, Representative Stratton introduced the Free Political Broadcasting Act of 1987 (H.R. 521) to provide free radio and TV time to Federal candidates. He also co-sponsored, with Senator Pen, the Informed Electorate Act of 1987 to require TV stations to provide free time to political parties for communications by House and Senate candidates.

[158] The 1971 Federal Election Campaign Act imposed spending limits on media advertising by Federal candidates, but these were repealed in 1974. To be consistent with *Buckley,* limits on advertisements would have to be part of a public funding scheme.

[159] In the 98th Congress, Senators Rudman and Inouye, adopting this approach, introduced the Fairness in Political Advertising Act. Among other things, this act would require that the purchaser of the ad or a designee: 1) speak to the camera for the duration of the ad; 2) permit some variation in backgrounds, provided they are taken with the same lens as the speaker; and 3) mandate written material identifying the speaker and purchaser of the ad. Curds B. Gans, testimony before the Senate Committee on Commerce, Science, and Transportation, Sept. 10, 1985, pp. 12-13.

[160] The FCC has exempted broadcasters from the equal time requirements when candidates appear on a bona fide news interview or documentary program, which includes television shows such as "Donahue" and "Entertainment Tonight." Some candidates supply tapes to broadcast stations, raising another question about the definition of a bona fide news program. Jack Loftus, "FCC Goes Easy on Political TV," *Television/Radio Age,* Apr. 4, 1988, pp. 43, 132.

[161] A number of bills have been introduced to either restrict the use of or lessen the impact of exit polls. One proposal that has been supported by the media is to adopt a uniform poll-closing time; the networks have given their verbal commitment that, if such a law were enacted, they would not announce exit-poll results until the polls closed. Statements of representatives from ABC, CBS, and NBC on S. 182 before the Senate Committee on Rules, May 12.1988.

Chapter 10

Security and Survivability of the Communication Infrastructure

CONTENTS

Figures

Chapter 10
Security and Survivability of the Communication Infrastructure

INTRODUCTION

Security and survivability are essential characteristics of the communication infrastructure.[1] However, establishing a secure and survivable infrastructure requires tradeoffs between security and survivability on the one hand, and access, cost, and ease of use on the other.[2] Experts estimate, for example, that security features constitute approximately 10 to 20 percent of a network's overhead costs. Moreover, adding features to provide additional security not only increases network traffic; it also slows down the speed of transmission. Thus, although most people would probably support the general goals of security and survivability, they might disagree significantly on the levels of security and survivability required, and the extent to which other communication goals should be sacrificed in order to achieve them.

THE PROBLEM

In the past, the security and survivability problems of the communication infrastructure were not particularly germane to most members of the American public. Where such issues did arise, they were generally resolved outside the public policy arena, either in the private sector or behind the scenes in government. In the future, these issues will become less containable. OTA found that security and survivability are becoming more important and more visible as communication policy goals; in addition, it is becoming more difficult to make the tradeoffs required to achieve them. Equally important, OTA found that the views of stakeholders may diverge to a greater extent over how these tradeoffs should be made. Moreover, the institutional mechanisms by which security and survivability issues are to be resolved and security goals achieved are not optimally designed. OTA identified a number of factors that might contribute to security and survivability problems in the communication infrastructure. They include:

1. the increased reliance of business and government on communication and information-based systems, and hence a greater vulnerability to their failure;
2. an increase in the number and variety of problems that may threaten the security or reliability of communication systems;
3. an increase in the complexity, decentralization, and interdependence of communication systems and, hence, in the difficulty of coordinating them to achieve security and survivability goals;
4. a growing divergence in stakeholder needs for security and reliability; and
5. an increase in the number of people who have access to communication systems and who are knowledgeable about their use, occurring at a time when there is no consensus about the legitimate use of the technology.

These factors are discussed below.

Factor 1: The increased reliance of business and government on communication and information-based systems, and hence a greater vulnerability to their failure.

Chapters 5 and 6 depict the growth and dependence of business and government on communication and information-based systems. More and more, in all business activities, companies are employing their communication systems and the information stored in them to achieve a competitive advantage. In addition to using these systems to extend their markets, many businesses are using them to actually

[1]The word "survivability" is used here to denote reliability, recoverability, contingency planning, and/or Operating under extreme conditions.

[2]One instance where this tradeoff is evident is the UNIX operating system. UNIX's open structure made it highly popular among academics and researchers, who spent years enhancing its flexibility. But, by virtue of its openness and its capacity for networking, UNIX has suffered from being inherently more vulnerable and insecure. For a discussion, see Sanford Sherizen and Fred Engle, "Striving for UNIX Security," *Computerworld*, Mar. 20,1989, pp. 85-93. For a discussion of the tradeoff between security and access, and the special problems that this tradeoff presents to the research community, see Kelly Jackson, "Virus Alters Networking," *CommunicationsWeek*, Nov. 14, 1988, pp. 1, 75.

restructure their organizations on a regional or global basis. Thus, the failure of a communication system can lead not only to market losses, but also to the failure of the business itself. For an indication of industry vulnerability to computer outages, see figure 10-1.

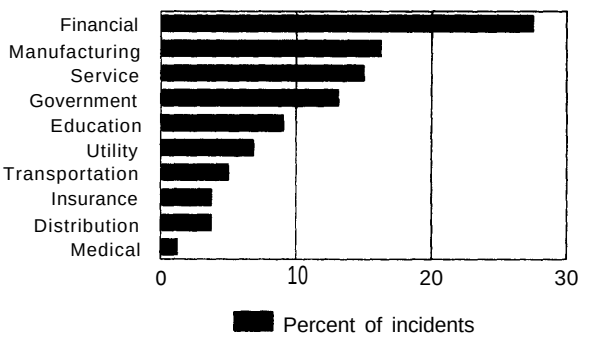
In a recent survey conducted by the Center for Research on Information Systems, University of Texas at Arlington, researchers identified four major consequences for businesses when information/communication systems fail:[3]

1. the reduction in, or perhaps complete termination of, the business function;
2. a loss in revenues;
3. increased costs of doing business; and
4. intangible costs entailed in the loss of image and customers, or legal or regulatory violations.

As depicted in figure 10-2, the damage to business increases with the time it takes to achieve recovery.

Government, too, is becoming more dependent on communication and information systems, and hence more vulnerable to their failure.[4] Faced with increased costs and budgetary constraints, many government agencies are looking to communication systems as a way of improving the efficiency and effectiveness of their operations. For example, online telecommunication systems are now being used for the delivery of Medicare and food stamp benefits, as well as for processing Federal income tax forms.[5] Failures in these systems will not only create administrative havoc and serious problems for the individuals involved, but they may also serve to undermine the support for, and legitimacy of, government operations themselves.

Figure 10-1-Vulnerability of Industries to Computer Outages



'Based on 1,000 disasters tracked over a 2-year period

SOURCE: Copyright 1989 by CW Publishing Inc., Framingham, MA 01701. Reprinted with permission from *Computerworld*, *VOI* 23, No. 16, Apr. 17, 1989, p. 21.

The need for a secure and survivable communication infrastructure has become especially acute in the realm of national security and emergency preparedness. It has long been a matter of national policy that telecommunication services required by the Federal Government, including for defense purposes, should be procured from the commercial sector, unless special circumstances dictate otherwise.[6] However, the operational requirements to meet the government's security and defense needs are becoming greater and greater all the time. For example, in October 1981, President Reagan announced a strategic modernization plan that was designed to prevent the realization of strategic

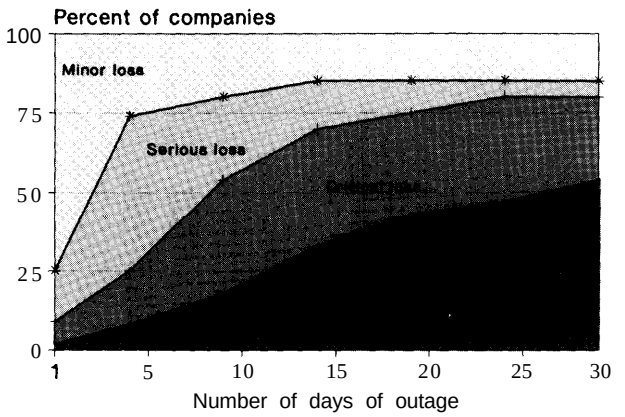
[3]Steven R. Christensen and Lawrence L. Schkade, "Financial and Functional Impacts of Computer Outages on Businesses," CRIS-87-01, Center for Research on Information Systems, College of Business Administration, The University of Texas at Arlington, TX, January 1987.

[4]See U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, *OTA-C1T-31O* (Washington, DC: U.S. Government Printing Office, October 1987); and U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security, and Congressional Oversight*, OTA-CIT-297 (Springfield, VA: National Technical Information Service, February 1986).

[5]See Katherine McGrail, "The Government's Expenditures on Data Will Soon Equal Money Spent *on Voice*," *Government Networking*, Sept. 21, 1987, pp. 7-14.

[6]Such a policy, however, has not been without its opponents. The "Continuing Resolution for Appropriations for Fiscal Year 1988" requires all government agencies to be connected to the Federal Telecommunications System 2000 (FTS 2000), although some exemptions will be made on the basis of existing systems and special needs. The Defense Nuclear Agency and the U.S. Army, Navy, and Air Force, among others, have generally resisted transferring their services to FTS 2000 for both logistical and security reasons. In December 1988, contracts (estimated to be worth $3 billion to $15 billion, depending on the number of Federal agencies included) were awarded to American Telephone & Telegraph Co. (AT&T) and U.S. Sprint Communications Co. to build the all-digital private network for the government. In accordance with the contract, AT&T will be responsible for developing a network for agencies representing 60 percent of all traffic, while U.S. Sprint will handle the rest. See Mitch Betts, "Feds Sign FTS 2000 Net Pact," *Computerworld*, *Dec.* 12, 1988, pp. 1, 4. See also Kelly Jackson, "Gov't May Be Forced To Deal Only With FTS-2000 Winner," CommunicationsWeek, Aug. 1, 1988, p. 16.

Figure 10-2--Severity of Loss Due to Computer Outages



SOURCE: Center for Research on Information Systems, The University of Texas at Arlington. Reprinted with permission from *Computerworld, vol. 23, No.11*, Mar. 13, 1989, p. 1. Copyright 1989 by CW Publishing Inc., Framingham,MA01701.

dominance by the Soviet Union. In essence, U.S. deterrence strategy, encapsulated in National Security Decision Directive-13 (NSDD-13), was moved one stage further from one based on mutual assured destruction, or even flexible response and counterforce nuclear targeting, to one of flexible response in which the United States would be equipped, and demonstrably able, to prevail in any conflict from low-intensity operations to prolonged strategic nuclear war. For the policy to succeed, and to be credible, U.S. military Command, Control and Communications and Intelligence (C^3I) systems had to be "fool-proof."[7]

Extensive reliance on technology may also make it more difficult for organizations to recover from system failures.[8] When technical problems occur, the people trained to operate systems manually may no longer be available. The Department of the Navy was confronted with such a situation, for example, in the late 1970s. When faced with a computer outage in their computer-based Combat Information Centers, the Navy's radar operators found it very difficult to effectively perform their task of target-tracking because many of their basic skills had become rusty.[9]

Factor 2: An increase in the number and variety of problems that may threaten the security or reliability of communication systems.

With the advance of information and communication technologies, communication systems are becoming vulnerable to a much wider range of possible disasters-from earthquakes, fires, and floods, to power outages, disk crashes, and intruding hackers.[10] Two major incidents occurred in 1988 that illustrate the variety of system security/reliability problems that can occur, as well as the extent of the damage that can result. These events were a fire at Illinois Bell Telephone Co. 's Hinsdale central office; and the most serious case of computer hacking to date, involving the implanting of a computer virus into the Internet, a major packet-switching network that connects research and government computers.

The Hinsdale fire occurred on May 8, 1988, at a major transmission hub that links local telephone switching centers with one another and with long-distance networks. The center provides voice and data communication services to several communities, as well as to a number of corporate data networks operated by companies such as United Air Lines, Montgomery Ward & Co., American Express Co., and Sears. Approximately 42,000 local lines and 118,000 trunks for local and long-distance call-routing are connected to the Hinsdale central office. In the wake of the fire, services were suspended for 7 days. An investigation found that, similar to many such incidents, the disaster resulted from both human error and mechanical failure—in this case, faulty wiring. Many who were affected by the outage sought unspecified damages for their losses. However, the court ruled to dismiss their class-action suit, on the grounds that an existing Illinois tariff limits telephone company liability in the event of a service outage to a 200-percent credit, which in this case amounted to approximately $3.5 million. However, to reassure its customers about

[7]Martin Edmonds, "Defense Interests and United States Policy fOr Telecommunications," OTA contractor report, June 1988, p. 30.

[8]Steven R. Christensen and Lawrence L. Schkade, "Surveying the Aftermath," *Computerworld*, Mar. *13*, 1989, p. 82.

[9]Ibid.

[10]Peter Scisco, "No Such Thing as a Small Disaster," *Computerworld*, July 11, 1988, pp. S I-S11.

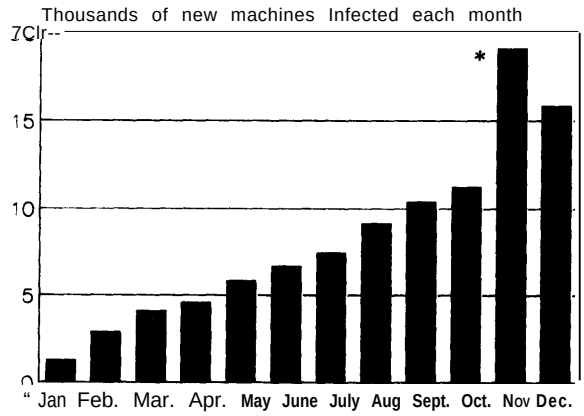
the integrity of the network, Ameritech announced that it will invest $80 million during the next 5 years to preclude a similar mishap in the future.[11]

The impact of the fire in Hinsdale was not only felt by those in the immediate vicinity. Throughout the country, many users began to examine and investigate the security and reliability of their communication networks. For example, a number of large users and user organizations in New York began to press the public telephone company to develop an emergency backup system that would allow them to connect their businesses to two central offices instead of one. *2 The fire not only heightened users' awareness of their growing vulnerability; it also raised some fundamental questions about liability in the event of major system failures.[13]

Reinforcing and underscoring this growing concern about system vulnerability has been the significant growth in the phenomenon of computer viruses.[14] As can be seen in figure 10-3, while only 3,000 machines were damaged by viruses in the first 2 months of 1988, over 30,000 systems were affected in the last 2 months of the same year.[15] Moreover, because viruses occur surreptitiously and act subtly to cause all sorts of damage, they serve to epitomize and symbolize the unpredictability of communication system failure, and the problems of anticipating and preparing for it. In fact, as depicted in figure 10-4, the damage resulting from computer viruses occurs in a series of four stages, becoming increasingly more severe the longer the virus remains unobserved.

One of the most publicized and disruptive computer-virus incidents to date occurred in November 1988, when it was reported that a 23-year-old, first-year computer science graduate student at Cornell University had tapped into the Internet

Figure 10-3--1988 Increase in Computer Devices Infected by Viruses "



"Includes the Internet infection

SOURCE Copyright 1989 byCW Publishing Inc., Framingham, MAo1701. Reprinted with permission from *Computerworld*, vol. 23, No. 6, Feb. 13, 1989, p. 90.

network. By taking advantage of a well-known weakness in the UNIX operating system and its accompanying electronic mail application, Sendmail, a virus was implanted that, within a few hours, infected more than 6,200 computers. Among the networks affected were those belonging to a number of government laboratories, including the Lawrence Livermore National Laboratory in California where research is conducted on nuclear weapons and civilian energy.[16]

Given the growing number of ways in which communication systems are becoming vulnerable, users now have to adopt multiple approaches to provide for secure and survivable networks. This requirement complicates the processes entailed in protecting communication networks, and can greatly add to the, expense of providing that protection.

[11]Steven Titch, "Illinois Delays Fire Report," *CommunicationsWeek*, No v. 14, 1988, p. 12; and Beth Schultz, "Ill. Bell Crafts Disaster Plan," *CommunicationsWeek*, Mar. 20, 1989,

[12]John Foley, "Telco Switch Vulnerability Worries Financial Users," *CommunicationsWeek*, June 27, 1988, PP. 1, 17.

[13]Ibid. As Foley notes, although most users already have their own contingency plans—including those that use fiber optics, microwave, or s systems-to bypass the local loop, most of their plans to restore their private networks in the event of disaster require a healthy public network.

[14]A virus is a computer program that is surreptitiously passed on to other computers online or through the exchange Of memory disks. Introc by piggybacking onto legitimate programs or messages, they are generally intended to cause damage by destroying data or overloading computer sys They can be designed to act immediately, or set to operate at a given time.

[15]See John D. McAfee, "Managing the Virus Threat," *Computerworld*, Feb. 13, 1988, p. 89.

[16]For accounts of this incident, see Tony Fainberg, "The Night the Network Failed, ''New *Scientist*, vol.121, No. 1654. Mar. 4, 1989, pp. 48-42; Philip J. Hilts, 'Virus' Hits Vast Computer Network," *The Washington Post, Nov. 4, 1988*, pp. A-1, A-4. For a discussion of the impact on netwo see Jackson, op. cit., footnote 2, pp. 1, 74-75.

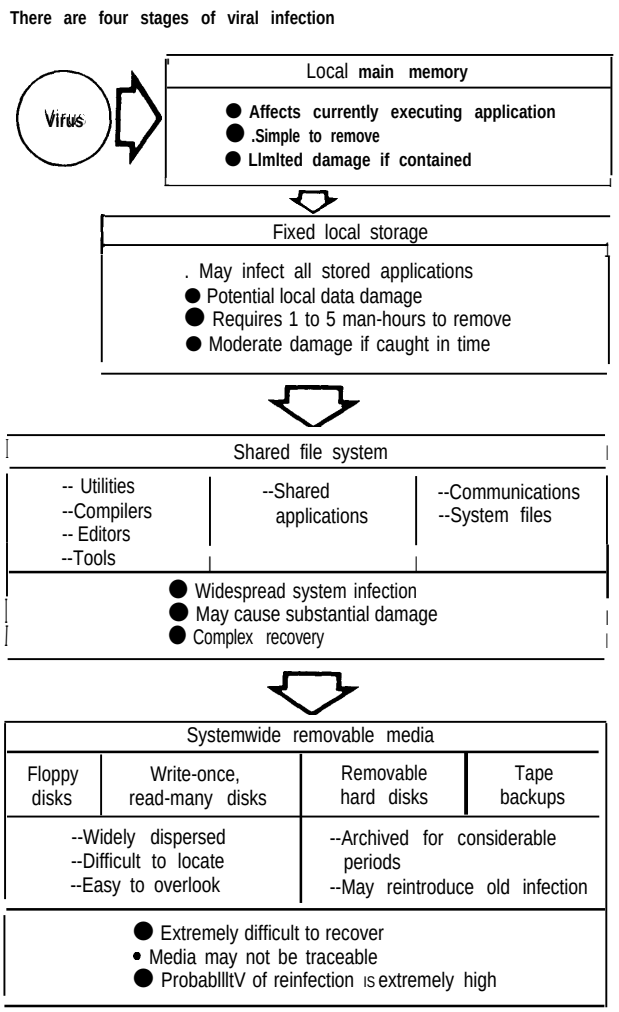
Addressing security problems is also complicated by rapidly changing technologies. New technologies bring with them novel, and often unforeseen, security problems. For example, when voice mail began to be widely deployed, hackers quickly discovered ways of using this technology to tap long-distance telephone lines.[17] Questions are now being raised about how the introduction of integrated services digital networks (ISDN) will affect the security requirements of present and future networks.[18] In addition, with the increased use of cellular radio for data transmission and facsimile calls, there is increasing concern about the security risks entailed in the use of these technologies.[19]

The convergence of computer and telecommunication technologies also gives rise to problems of contingency planning because the requirements for the two systems are quite different. Moreover, security personnel for computers and telecommunication differ greatly on what they see as the major security problems and safeguards. Because there is no consensus in government or in the private sector as to whether computer managers or network managers should be responsible for information security, effective security arrangements are often hindered by political turf battles, uncoordinated activity, and lapses in security coverage.[20]

Factor 3: An increase in the complexity, decentralization, and interdependence of communication systems and, hence, in the difficulty of coordinating them to achieve security or survivability goals.

Increases in computing power and decentralization of computing functions have increased the vulnerability of computer and communication systems to unauthorized use. Early systems were designed to be used by trained operators in reasonably controlled work environments; therefore, only local access to systems was of concern. Today's

Figure 10-4-Four Stages of Viral Infection of Computer Systems



SOURCE: Copyright 1989 by CW Publishing inc.,Frammgham,MA01701. Reprinted with permission from *Computerworld*, vol. 23, No. 6, Feb. 13, 1989, p. 91.

[17] See, for a discussion, John Burgess, "Hackers Find New Way To Tap Long Distance Lines," *The Washington Post*, Oct. 6, 1988, p. F-1.

[18] A recent report by Coopers & Lybrand, "The Security of Network Systems," concludes, for example, that: "in view of the changing environment and the importance of network system security, increased emphasis should be given to security within ISDN." As cited in Clare Lees, "Security: A Management Issue," *Telecommunications*, February 1989, p. 37. On the other hand, it has been suggested that the out-of-band signaling on the D charnel is a major security feature of ISDN, making it easier to audit and authenticate user identification through the network. See, for a discussion, James Sherman and William Demlow, "ISDN: A Telecom Security Blanket," *Telephony*, Mar. 6, 1989, pp. 33, 35.

[19] See Nick Vafiadis, "Cellular Radio: Vulnerable to Attack," *Telecommunications*, February 1989, PP. 55-56.

[20] Sanford Sherizen, "Federal Computers and Telecommunications: Security and Reliability Considerations and Computer Crime Legislative Options," OTA contractor report, February 1985.

systems, on the other hand, are designed for maximum use—that is, to be used by anyone, anywhere.[21] One measure of this kind of security problem, for example, is the rapid proliferation of local area networks (LANs), whose market was estimated to grow from $2.6 billion in 1987 to $4.2 billion in 1988.[22] Moreover, according to one market research company, by 1992, 35 percent of all personal computers (PCs) sold will be networked, and 50 to 60 percent of all new PCs acquired by Fortune 1000 companies will be connected to LANs.[23] Characterizing the problems of control that this spread of LANs is likely to generate, one observer has said:

> Once stand-alone personal computer users are given access to a local-area network, controlling them is like trying to corral fish within a public fence.[24]

The increased concentration of data in fewer and fewer facilities also makes communication systems more vulnerable to breaches in security. When operating a T3 network (circuits that operate at 44.736 megabits per second). network recovery is critical. The T3 signal is capable of transporting a total of 672 voice channels at 64 kilobits per second each; few networks could handle a simultaneous loss of 672 circuits. And high-capacity digital switches can connect and process more than a million calls in a single hour. As the executive vice-president of Contel has described it: "The network is getting thinner and thinner, and switches are getting bigger and bigger."[25] Given this ability of optical fibers and electronic switches to handle vast quantities of data through fewer and fewer facilities, the number of people affected by a system failure will be much greater than ever before.[26]

These technological complexities are compounded by organizational ones. Organizations frequently fail to make the important decision of who will control information, and where within the organizational structure the responsibility for such control will reside. These organizational problems are likely to increase, moreover, to the extent that businesses employ new communication technologies to expand the scope of their operations. More often than not, technologies are deployed without consideration of their security implications.[27]

Factor 4: A growing divergence in stakeholder needs for security and reliability.

Although virtually all users are concerned about some combination of confidentiality, integrity, and continuity of service, government agencies and the business community often have very different outlooks and needs when it comes to safeguarding information in computer and communication systems. Business-users have tended to consolidate their requirements for common information safeguards through voluntary participation in the activities of U.S. and international organizations that develop open public standards.[28] In contrast, the National Security Agency (NSA) sets its own standards in a process that is sometimes open to the public (e.g., computer security) and sometimes not (e.g., communication security).

These and other differences raise the question of whether information safeguards designed by and for the defense and intelligence agencies are well suited

[21] Based on the growth of networking, the market research company, Frost & Sullivan, has estimated that the overall market for computer security would jump from $588 million in 1988 to $1 billion by 1993. See Kelly Jackson, "Virus Fosters Growth in Sales of Security Products," *CommunicationsWeek*, Nov. 21, 1988, p. 16.

[22] See, for one discussion, Michael I. Sobol, "Securit, Concerns in a Local Area Network Environment," *Telecommunications*, March 1988, pp. 96, *98-99.*

[23] This estimate was made by Forrester Research, Inc., and reported in Marc Cecere, "Backdoor Lans: How to Manage Unsanctioned Networks," *Computerworld*, *Nov.* 2, 1988, p. 31.

[24] Ibid.

[25] As quoted in ibid., p. 9.

[26] Ellen Block and Henry D. Levine, "Protecting the Last Mile: The Quest for a Robust Local Exchange Network," *Telematics*, vol. 5, No. 10, October 1988, p. 9.

[27] See Lees, op. cit., footnote 18, pp. 37, 38, 40.42.

[28] Recently, for example, the Corporation for Open Systems (COS) has been giving thought to the idea of establishing a special task force to develop network security standards. The task force would review current and future security efforts and make recommendations to the American National Standards Institute. In addition, it would seek to encourage vendors to provide products meeting these standards. See Kelly Jackson, "COS Is Getting Serious About Network Security," *CommunicationsWeek,* Feb. 6, 1989, pp. 34-35.

to the needs of commercial and other users. As noted by Albert Belisle, the banking community, for one, is becoming increasingly concerned about:

> . . . the move to protect all sensitive information in the same manner-business information, information of importance to the national interest, and classified defense information. Within both the public and private sectors, there is a need for a broad spectrum of information systems security standards, techniques, and tools. There must be a range of security "solutions" that can be matched to the value of the information being protected, and the nature of the threats. Outside of the classified and national security arenas, both the private and public sectors must select cost-effective security measures.[29]

Some citizens' groups have also questioned the level of security required by government for some types of information and communication activities. Responding to the President's National Security Decision Directive 145,[30] in September 1984, the American Civil Liberties Union expressed the fear that such measures went too far, and could be used to deprive individuals of access to the information they need to perform effectively as citizens.[31]

Given these divergent security needs, questions arise with respect to how much security should be provided in the public network, how its costs should be determined, and how it should be paid for. In the past, these costs were generally included in the regulated common carrier's rate base. In is not clear, however, how they will be allocated in the future. Some have suggested, for example, that the Department of Defense (DoD) might provide direct funding for system upgrades.[32] In the State of New York, large users have been negotiating with NYNEX to provide greater redundancy in the public network. Elsewhere, other businesses have been informed by telephone company managers that, although technically feasible, the cost of such security measures would be too high. As one telephone company manager characterized it: "There is nothing we can't do; there are only things that you can't afford."[33] Competitors of local exchange carriers argue, moreover, that the best way to provide for a reliable, secure communication infrastructure is to promote competition at the local level.[34]

Factor 5: An increase in the number of people who have access to communication systems and who are knowledgeable about their use, occurring at a time when there is no consensus about the legitimate use of the technology.

As more and more people have gained access to communication and information-based systems, the problems of piracy and unauthorized use have mounted alarmingly .35 These occurrences range from those that might be characterized as "benign mischief' to those that clearly constitute serious

[29]Albert R. Belisle, Vice Chairman of the American Bankers Association's Information Systems Security Management Committee, testimony at hearings on military and civilian control of computer security issues, before the House Committee on Government Operations, Subcommittee on Legislation and National Security, May 4, 1989. For a perspective that posits a more complementary relationship between business and defense needs, see Ashton B. Carter, "Telecommunications Policy and U.S. National Security," in Robert W. Crandall and Kenneth Flamm (eds.), *Changing the Rules Technological Change, international Competition, and Regulation in Communications* (Washington, DC: The Brookings Institution, 1989).

[30]This directive provided NSA with responsibility to secure, "by such means as are necessary," all government, military, and civilian computer and telephone systems that handle classified information, as well as "other sensitive" information, the loss of which "could adversely affect nationat security interests."

[31]Nathan Weber, "Telecommunications Crime,''&ro~~the Board, vol. XXIII, No. 2, February 1986, p. 21. See also Steven L. Katz, "National Security Controls, Information, and Communications in the United States," *Government Information Quarterly*, vol. *4, No. 63, 1987;* John Shattuck and Muriel Morisey Spence, "The Dangers of Information Control," *Technology Review, vol. 91, No. 3,* April 1988, pp. 62-73.

[32]Carter, op. cit., footnote 29, p. 224. As Caner notes: "A precedent exists in the Civil Reserve Air Fleet program, where the department pays commercial airlines to modify the floors and doors of large aircraft so they can supplement military airlift in wartime. "

[33]Block and Levine, op. cit., footnote 26, p. 10.

[34]For example, as Robert Atkinson, Vice president of regulatory and external affairs for Teleport Communications, New York, has noted: "The lesson of Hinsdale is that instead of paying lip service to competition, regulators and legislators must start developing affirmative policies to encourage local competition. The issue is not how the Bell system companies can be unleashed, but instead how their bottleneck over the local communications network can be loosened enough so that a Hinsdale catastrophe will not happen again. Both the public sector and private sector have a role to play in insuring the basic integrity of the nation's telecommunication network." Robert Atkinson, "Where m the Blazes is Security?" *CommunicationsWeek,* Aug. 8, 1988, p. 8.

[35]For some recent cases, see John Burgess, "Hackers Find New Way To Tap Long-Distance Phone Lines," *The Washington Post,* Oct. 6, 1988, p. F-1; Christine Winter, "Legislators Alerted to Computer Virus Danger," *The Washington Post,* Oct. 14, 1988, p. F-1; and Lisa Stein, "The Intrigue and Art of Hobbling the Hackers," *Cablevision,* Sept. 12, 1988, p. 34.

computer crimes. Moreover, these activities appear to feed on themselves; what begins as a prank by one person is later refined into a more destructive or criminal form by another. As communication systems become more user-friendly and more interoperable, these problems are likely to multiply.

One factor underlying the growth of computer "hacking" is the lack of an agreed-upon ethic about the use of new technologies.[36] In fact, many of those using new technologies today share the view that some "computer crimes," such as unauthorized entry to a private computer system or the use of illegal decoders, are less than serious.

STRATEGIES AND OPTIONS

To address these problems, Congress can pursue six basic strategies. It can:

1. undertake further study and analysis of the changing security and survivability needs of the communication infrastructure;
2. facilitate the transfer of information about security and survivability, garnered in public agencies, to the private sector;
3. establish security and survivability standards for key industrial sectors;
4. provide special emergency facilities for private sector use;
5. improve coordination of survivability planning; and
6. increase activity geared to preventing security breaches.

These strategies, and the potential options that Congress might adopt to carry them out, are discussed below and summarized in figure 10-5.

Strategy 1: Undertake further study and analysis of the changing security and survivability needs of the communication infrastructure.

Option A: Continue funding and support for the National Research Council (NRC) to evaluate the state of reliability of the U.S. communication infrastructure for purposes of national security and emergency preparedness.

In 1983, the Defense Communications Agency (DCA), acting on behalf of the National Communications System (NCS), commissioned NRC to address the main problems then confronting National Security/Emergency Preparedness (NS/EP) telecommunication provision, and make recommendations. In the next 4 years, four reports were issued that collectively focused on the paramount need for telecommunication survivability. Acknowledging the fluidity of the telecommunication market—within which the motivating forces had become the emerging technologies, open competitive opportunities, and new commercial studies—the NRC reports clearly recommended that NCS and DCA should take stronger initiatives to influence both the market and new technologies that were in the interests of national security and emergency preparedness. For example, suggestions were made that electromagnetic pulse-resistant and radiation-hardened designs should be encouraged in NS/EP-dependent facilities. or even made mandatory; fiber optic cables should be specified wherever possible; fault-tolerant systems should be employed; and software for use in switching should be expanded to meet NS/EP priority capabilities. Emphasis was also placed on standardization and the need for common practices to assist and enhance network-to-network interface interoperability and common channel interoffice signaling.[37]

A fifth report, issued in May 1989, examines how society's greater reliance on information increases the vulnerability of the Nation's communication infrastructure. It concludes:

> Already there are disturbing signs of increased vulnerability of the public networks to disruptions . . . The social and economic consequences of serious outages can only increase in a society which becomes daily more reliant upon information transfer services for smooth functioning.[38]

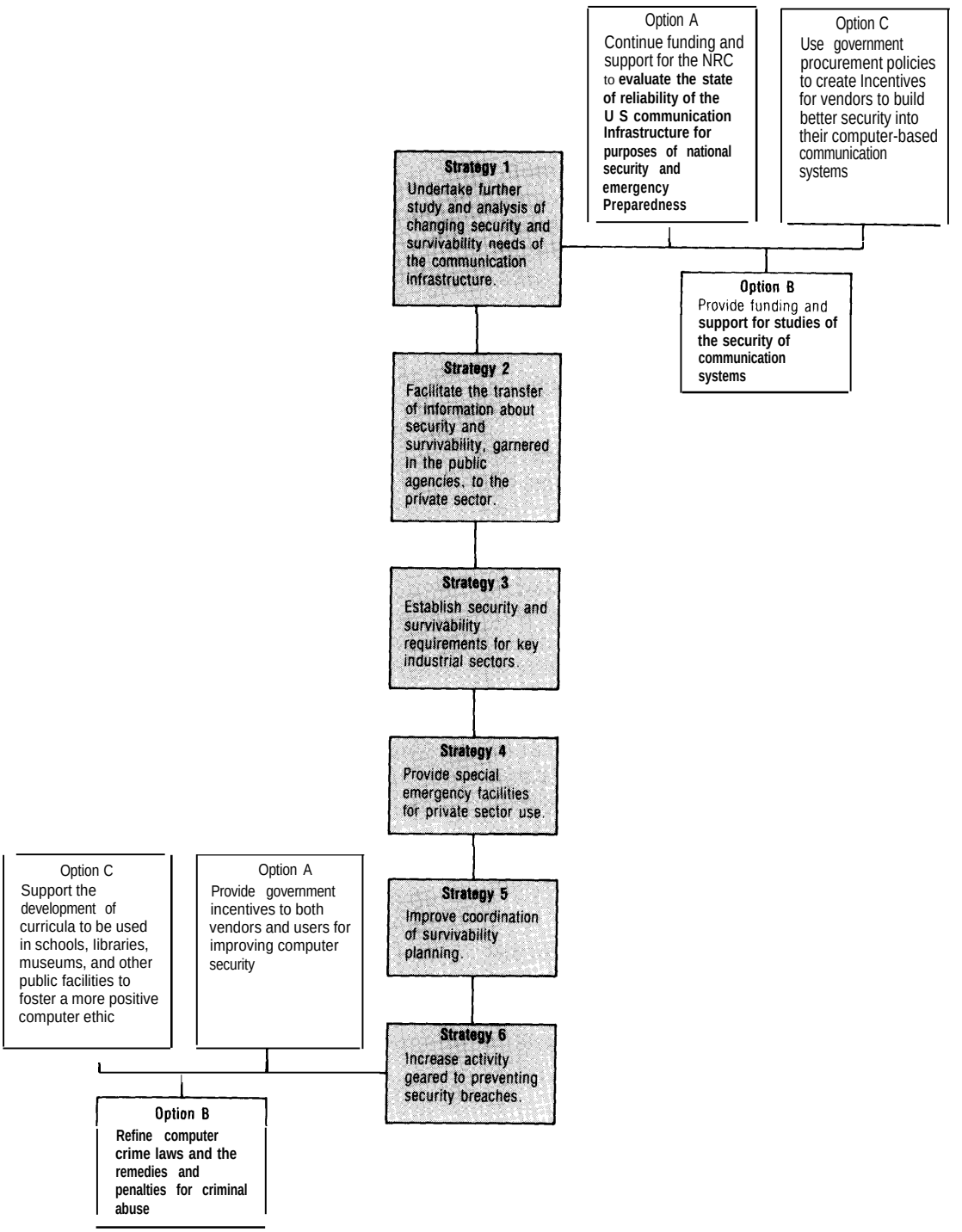
External evaluations of this kind are critical because,

[36]Steven Levy, *Hackers: Heroes of the Computer Revolution* (Garden City, NY: Anchor Press/ Doubleday, 1984). As the author points out, hacking originally occurred among computer science buffs, and it was a practice that actually gave rise to a number of technological advancements in the field. This original role has given a somewhat ambiguous meaning to the term "hacker." and even to the whole concept of "hacking."

[37]Edmonds, op. cit., footnote 7, p. 43.

[38]National Research Council, Growing *Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness* (Washington, DC: National Academy Press, 1989).

Figure 10-5--Congressional Strategies and Options To Address Security/Survivability of the Communication infrastructure



SOURCE: Office of Technology Assessment, 1990.

short of an emergency, there is no secure way to test the system's reliability.

Option B: Provide funding and support for studies of the security of communication systems.

Although events such as the fire in Hinsdale, Illinois, and the paralysis created among thousands of computer systems due to the spread of a powerful computer virus have recently highlighted the problems of security and survivability, very little hard data exist on the extent to which the private sector has experienced these problems. This lack of data is due in part to the business community's reluctance to make this kind of information public. Many business leaders fear that doing so would not only increase the problem by challenging others to engage in similar activities, but would also undermine their credibility with their customers.[39]

Although the private sector is not inclined to undertake a broad investigation of the scope of security and survivability problems, it may be in the government's interest to do so. As discussed in chapter 5, the economy is becoming increasingly dependent on information-based industries whose continued operation is dependent on the security and survivability of their computer-based communication systems. For example, in November 1985, a computer problem in the offices of the Bank of New York prevented it from completing an exchange of government securities. This fault in the system not only cost the bank $1.5 million after taxes, but it also forced it to borrow $24 billion from the Federal Reserve System.[40] A major fault in a telephone company computer system would be even more problematic; it might affect many more businesses and last for days, not hours.

Without better information about the extent of the security/survivability problem in the private sector, the government will not have an adequate basis for choosing appropriate courses of action. Hence, this option would be a prerequisite for the more proactive options discussed below.

Option C: Use government procurement policies to create incentives for vendors to build better security into their computer-based communication systems.

The Federal Government is the largest buyer o computers and computer equipment in the United States. The FTS 2000 contract alone, for example, i valued at between $3 billion and $15 billion. Moreover, government's purchase of the UNIX operating system (with two-thirds of it going to defense) amounted to $1.93 billion in 1988,[41] This kind of market leverage provides a way for the government to foster secure communication system: by structuring government procurement policies in ways that will induce vendors to enhance the security of their products.[42] Recently, for example, DoD issued Directive 5200.28, which requires that, by 1992, all multicomputer systems meet a minimum of C-level security standards. The C-level standard calls for need-to-know protection, audit compatibility, and user accountability.[43] Moreover, NSA's Secure Data Network Systems Project (SDNS) has been working for over 2 years to develop open systems interconnection (OSI)-based security standards. In addition, government regulations sometimes require firms with Federal contracts to have contingency plans for reliable communication services.[44]

Vendors are likely to be responsive to such incentives. To participate in SDNS, for example, vendors must agree to produce products based on protocols developed through the program.[45] Moreover, as products become more standardized, vendors have been trying to differentiate their wares,

[39]For one discussion, see John Foley and Jennifer Samuel, "Users Ponder Net security," *CommunicationsWeek, Nov. 14, 1988,* pp. 1, 74-75. According to Foley and Samuel, users refuse to discuss the security of their communication systems, fearing that public knowledge of their systems could leave them open to intrusion.

[40]Block and Levine, op. cit., footnote 26, pp. 9-12.

[41]Sherizen and Engle, op. cit., footnote 2, p. 92.

[42]For a discussion, see George Jelen, *Information Security: An Elusive Goal* (Cambridge, MA: Harvard University, Program on Information Resources Policy, Center for Information Policy Research, 1985), especially ch. 10.

[43]Mitch Betts, "Secure UNIX Aimed at Fed Deals," *Computerworld*, Nov. 7, 1988, pp. 23,25.

[44]James Daley, "Disaster Recovery To Hit Big Time, Study Says," *Computerworld*, Apr. 17, 1989, p. 21.

[45]A number of major vendors are participating, including AT&T, BBN Communications, Digital Equipment Corp., GTE Corp., Honeywell Inc., IBM, Motorola Corp., Unisys Corp., Wang Laboratories, Inc., and Xerox Corp. See Jackson, op. cit., footnote 28, p. 35,

and security features represent one way of doing this.[46] However, one limitation to this option is the lack of well-developed procurement standards within government agencies.

Strategy 2: **Facilitate the transfer of information about security and survivability, garnered in public agencies, to the private sector.**

The Computer Security Act of 1987 assigns to the National Institute of Standards and Technology (NIST) the responsibility for developing technical, management, physical, and administrative standards and guidelines for security of sensitive information in Federal computer systems. The act requires, moreover, that each Federal agency provide mandatory periodic computer security training for employees involved in the management, use, or operation of Federal computer systems within, or under the supervision of, that agency.

Given the wisdom and experience gained by establishing security standards and secure information practices in the public sector, the Federal Government might want to develop more systematic ways of sharing this knowledge with the private sector. For example, NIST might enhance its programs to certify vendors, transfer technology, standardize designs, procure devices, and encourage the development and use of improved safeguards.[47] Closer cooperation between NIST and the private sector in security-related matters would also allow the government to benefit from innovations and new technologies developed in the private sector. One step that NIST has already taken in this regard is to set up a program for bringing together government organizations and private contractors interested in interoperability and security in the OSI computer network architecture and the ISDN computer architecture. The fundamental objectives of this program are to:

- develop demonstration prototypes of applications and equipment, including hardware and software, that provide one or more levels of security in an OSI and/or ISDN environment;
- develop data formats, protocols, interfaces, and support systems for security in an OSI/ISDN environment that can be used as a basis for Federal information-processing standards. Such standards may then be used as bases for Federal procurement of services and systems in the future; and
- provide a laboratory in which users, developers, and vendors can jointly define, develop, and test systems that will provide a range of telecommunication, network management, and security services in a distributed information-processing environment.

In addition, DoD's Advanced Research Project has recently created the Computer Emergency Response Team (CERT), which is designed to act as a central clearinghouse for information concerning the detection of viruses. It will also distribute solutions, as they become available, to those who have been affected. Its members include staff from the Federal Bureau of Investigation, as well as other technical and management experts. CERT is located in the Software Engineering Institute, Carnegie-Mellon University.[48]

The major problem involved in the sharing of security information between government and the private sector stems from the role that security plays in intelligence and defense. Whereas businesses are accustomed to working out criteria and standards in open processes, the defense community is typically more secretive. Moreover, as the OTA assessment, *Defending Secrets, Sharing Data,*[49] points out, this conflict of interest is exacerbated by the fact that the law fails to clearly delineate between the responsi-

---

[46] Betts, op, cit., footnote 43.

47 Since the early 1970s, NIST has conducted a laboratory-based computer security program to develop cost-effective solutions for protecting reclassified information, These solutions are made available to Federal and private organizations through the development and publication of' standards, guidelines, and other technical documents; sponsorship of conferences and workships; and other technology-transfer activities. The fiscal 'ear 1990 budget submission to Congress proposes a NIST research program that provides for activities such as laboratory-based research, the levelopment of cost-effective management and technical security methods and solutions, leadership m developing national and international information ecurity standards, encouragement and facilitation of technology transfer, and development of materials to support security awareness and training.

[48] Chris Roeckl, "User Organizations Offer 'Virus' prescription," *CommunicationsWeek*, Jan. 16, 1989. p 24.

@Office of Technology Assessment, *Defending Secrets, Sharing Data,* Op. cit., footnote 4.

bilities of NIST and NSA in this area.[50] One way of encouraging private-public cooperation on security issues, therefore, would be for Congress to clearly separate the responsibilities between NIST and NSA, based on defense considerations.[51]

An additional constraint on the development of this option might be the limited budget and lack of personnel that are available to NIST to handle this task. The Reagan Administration budget, which the Bush Administration adopted with only minor exceptions, proposed a reduction in NIST's budget from $158 million in 1989 to $153 million in 1990.[52] This reduction was budgeted, moreover, even though in the past NIST has had to contract out to NSA much of its broad research on security standards.[53] Moreover, a recent study by the General Accounting Office found that NIST has been slow to implement the Computer Security Act, insofar as 21 agencies reported that, as yet, they did not have security training programs in place .54 Given this lack of progress in developing technical standards and common procedures, many are concerned that the limited funds available to NIST might prevent it from carrying out its responsibility in this area. Testifying recently at *Hearings on Military and Civilian Control of Computer Security Issues,* before the House Committee on Government Operations, a spokesperson for the Information Industry Association, noted, for example:

> We believe that NIST is underfunded. It has insufficient resources to expeditiously carry out its mission under [the Computer Security Act of 1987]. This resulted, for example, in NIST falling behind its own schedule for completion of reviews of agency security plans, even though the agency has the assistance of NSA in this task.[55]

Strategy 3: Establish security and survivability, requirements for key industrial sectors.

Given the increased dependence of many corporations on communication and information-basef systems, Congress could identify businesses whose continued functioning is critical to society, and establish guidelines or requirements for making their communication facilities secure. As a result o the destruction caused by a telecommunication cable fire in Tokyo, for example, the Japanese Government considered ways of establishing safety and reliability standards, as well as the means 01 implementing them. They mandated technical improvements, including increased redundancy of critical circuits and better fire-prevention designs; designated some users whose service should be restored on a priority basis in case of disruption; and instigated studies of the need for improved damage compensation and insurance schemes for communication-related accidents.[56]

There is a U.S. precedent for such an approach. Since 1983, for example, the Office of the Comptroller of the Currency has mandated that all national banks undertake contingency planning for key operational areas, which now include microcomputers.[57] In accordance with these rules, the bank's management will be held accountable for the failure to develop a sound plan.

In general, businesses have been slow to adopt security measures or to prepare for emergencies,

[50] Notwithstanding the provisions of the Computer Security Act, NSDD-145 has assigned similar responsibilities to NSA, which is charged with reviewing and approving all standards, techniques, systems, and equipment for telecommunication and automated information systems security. The relationship between NIST and NSA was the subject of oversight hearings before the House Committee on Government Operations, Hearings on Military and Civilian Control of Computer Security Issues, May 4, 1989,

[51] Options for reorganizing the responsibilities of NIST and NSA in this area are analyzed in Office of Technology Assessment, *Defending Secrets, Sharing Data,* op. cit., footnote 4.

[52] Daniel S. Greenberg, *Engineering Times,* April1989, P. 3.

[53] For a discussion, see statement of Lance J. Hoffman, Professor of Engineering and Applied Science, Department of Electrical Engineering and Computer Science, The George Washington University, hearings, op. cit., footnote 29.

[54] U.S. Congress, General Accounting Office, Computer *Security: Compliance With Training Requirements of the Computer Security Act of 1987* (Washington, DC: U.S. Generat Accounting Office, February 1989), p. 17.

[55] Kenneth B. Allen, Senior Vice President, Government Relations, Information Industry Association, hearings, op. cit., footnote 29. See also statement of Miriam A. Drake, Dean and Director of Libraries, The Georgia Institute of Technology, on behalf of the American Library Association and the Association of Research Libraries, ibid.

[56] Naruko Takanashi et al., "The Achilles' Heel of the Information Society: Socioeconomic Impacts of the Telecommunication Cable Fire in the Setagaya Telephone Office, Tokyo," *Technological Forecasting and Social Change,* vol. 34, No. 1, August 1988, pp. 27-52.

[57] Sanford Sherizen and Albert Belisle, "Begin Contingency Planning Or You Might Become an Outlaw," *Computerworld,* July11, 1988, p. S-10.

often postponing action until after a problem has occurred. For example, in a recent survey of users, it was found that only 17 percent of Fortune 1000 sites were protected by encryption or call-back.[58] One major reason cited for the failure to use such systems is cost.[59] Thus, many businessmen are likely to be opposed to the government setting security/survivability standards or preparedness requirements on the grounds that such action would constitute undue interference in the affairs of the private sector.[60] And many would be concerned that, with standardized security practices, they themselves might be held liable if something were to go wrong. This is not an idle concern. As Sherizen and Belisle have pointed out:

> There are already an increasing number of laws defining acceptable business practices. Legal attention will soon be paid for failure to survive a major business interruption, which will be considered a malfeasance of duty.[61]

Others might contend that the market will take care of the problem. In this view, the decision to protect against risks is a matter of business strategy; when businesses experience the increased costs entailed in communication failures, they will proceed quickly to resolve their own security problems. Already there is evidence of a growing market for security products. A recent survey conducted by Frost and Sullivan Inc., for example, predicts that the market for computer security will be $1 billion by 1993.62

On the other hand, as noted above, businesses have generally been slow to respond to security threats. And they may be particularly reluctant to invest in communication security because its value has to be traded off not only against cost, but also against system access and interoperability.

Strategy 4: Provide special emergency facilities for private-sector use.

If the two New York Telephone switching centers were to fail, among those affected would be many of the world's largest financial institutions, including the Federal Reserve Bank, domestic and international banks, investment banking firms, stock exchanges, and large corporations.[63] Given their increased dependence on computer-based communication, many such companies are investing heavily to protect against natural or manmade failures in their networks. Some have called for redundant central offices, for which they would be willing to pay a considerable fee. Others are taking out special insurance policies and contacting for redundant processing capacity, known as "hot spots," to be used on an emergency basis. At a cost of approximately $50,000 per month, this option is clearly not available to all businesses.[64]

To the extent that the ability to pay for such protection is not correlated with a company's strategic value to the government or to the economy, the government may want to make special provisions to assist in some emergencies. One way would be to allow some private companies to make temporary use of the Nationwide Emergency Telecommunications Service (NETS).[65] At present, this service is available only for 20,000 authorized Federal Government users.

Members of the defense community would likely be opposed to such an option, given the need to keep the system secure and available for defense-related emergencies. Moreover, setting rules and proce-

58 Survey conducted for *CommunicationsWeek* by Computer Intelligence Corp., as cited in Foley and Samuel, op. cit., footnote 39, p. 75.

59 Ibid. Experts estimate that security measures make up about 10 to 20 percent of the overhead costs Of networks.

60 This was, in fact, a point emphasized by the American Petroleum Institute in its review of the OTA draft, as well as a point stressed by Albert R. Belisle in his testimony on behalf of the American Bankers Association, *Hearings*, op. cit., footnote 29, May 4, 1989.

61 Sherizen and Belisle, op. cit., footnote 57.

62 Jackson, op. cit., footnote 21; see also Clinton Wilder, "Cashing In On Virus Anxieties," *Computerworld*, *Nov. 21, 1988*, pp. 1, 6.

63 Foley, op. cit., footnote 12. See also U.S. Congress, Office Of Technology Assessment> "Information Technology and Securities Markets," in progress.

@For a discussion, see James Daly, "Electronic Vaulting Catches On," *Computerworld*, *Dec* 19, 1988, pp. 21, 26; and James Daly, "Comdisco furnishes Disaster Recovery Hot Site To Go," *Computerworld*, *Nov*. 28, 1988, p. 18.

65 As described by the National Research Council, NETS is". . . one of three programs that will provide telecommunications capabilities as required by Presidential Order in National Security Decision Directive (NSDD) 97. . . . These programs are designed to meet current and future requirements of the federal government for national security and emergency preparedness telecommunications. NETS is the largest of the three programs and is intended to provide survivable, switched, voice, and data service."

dures for access might be very difficult. However, using the service for business-related emergencies might have some positive defense benefits; it would provide greater information about how well the system works in an actual emergency. The arrangement for use by businesses might be worked out and authorized through the Federal Emergency Management Agency.

Strategy 5: Improve coordination of survivability planning.

In evaluating the policy planning environment of national security telecommunication, NRC, in its 1986 report to DCA, called for a "bottom up" response to emergency situations, and stressed the need for improved coordination with, and assistance from, State and local governments. NRC also called for better coordination among providers of communication services.[66]

The delayed response to the Hinsdale fire suggests that additional improvements can be made in the planning and coordination of emergency response measures. Reportedly, the response time after the switch failed was 10 hours, the delay being due, in part, to the need for verifying the request for assistance.[67] Moreover, as described in chapter 13, State approaches to telecommunication policy are, in fact, becoming less uniform, making coordination with them more difficult. Some States, for example, having greater concentrations of businesses, may have more incentive for promoting the reliability of communication systems than do other States. Also compounding the coordination problem is the failure of telecommunication vendors to agree on common standards, as well as the continued migration of many businesses from the public switched network to their own private networks. In addition, the impact of the open network architecture process and the move towards an intelligent network with common channel signaling will need to be assessed in terms of security criteria.[68]

Strategy 6: Increase activity geared to preventing security breaches.

Option A: Provide government incentives to both vendors and users for improving computer security.

As Robert Morris, chief scientist at NSA, has noted: "To a good approximation, every computer in the world is connected to every other computer."[69] In this sense, a network's security is no greater than its weakest link. For example, over a period of 5 years, a person in London was able to employ a computer network to break into more than 200 military, corporate, and university computer systems in Europe and the United States.[70] And a network can serve as a "conduit for infection," proliferating computer viruses.[71]

As already noted, despite these interdependencies and the greater risks that they entail, many users continue to ignore security issues. Under these circumstances, where the negligence of some may have a considerable negative impact on others, Congress might want to provide incentives to induce both vendors and users alike to adopt greater security measures. As in the case of energy efficiency, such incentives might take the form of tax credits. Developing the appropriate incentives, however, will require a greater understanding than we now have about the incentives that lead corporate management to adopt security measures.[72] It may be necessary, moreover, for government to help de-

66"Policy Planning Environment for National Security Telecommunications," final report to the National Communication System, Nationat Research Council, Washington, DC, July 1986.

67Personal communication with Martin Edmonds, OTA contractor, Nov. 8, 1988.

68In one recent report, NRC points out ho, common channel signaling, which is a characteristic of the intelligent network, will make nationwide emergency telecommunication service more vulnerable. "Interim Report to the National Communication System," August 1988.

69"The Complexity of Computer Security," *Science News*, vol. *134, No. 13,* Sept. 24, 1988, p. 199.

70John Markoff, "Briton Said To Penetrate U.S. Computers," *The New York Times,* Oct. *24, 1988,* p. D-1.

71 Boyce Rensberger, "Networks Are Conduits for the Infection," *The Washington Post, Nov. 4, 1988,* p. A-41.

72Senior management tends not t. understand information security, since it seldom receives an evacuation in senior management terms. Consider, fOr example, the lack of incentives involved with the direct costs associated with improving information security, These costs include negative impact on organizationat productivity, possible system degradation, unhappy and inconvenienced users, as well as the cost of the security product or device. Sanford Sherizen, personat communication, Mar. 27, 1989.