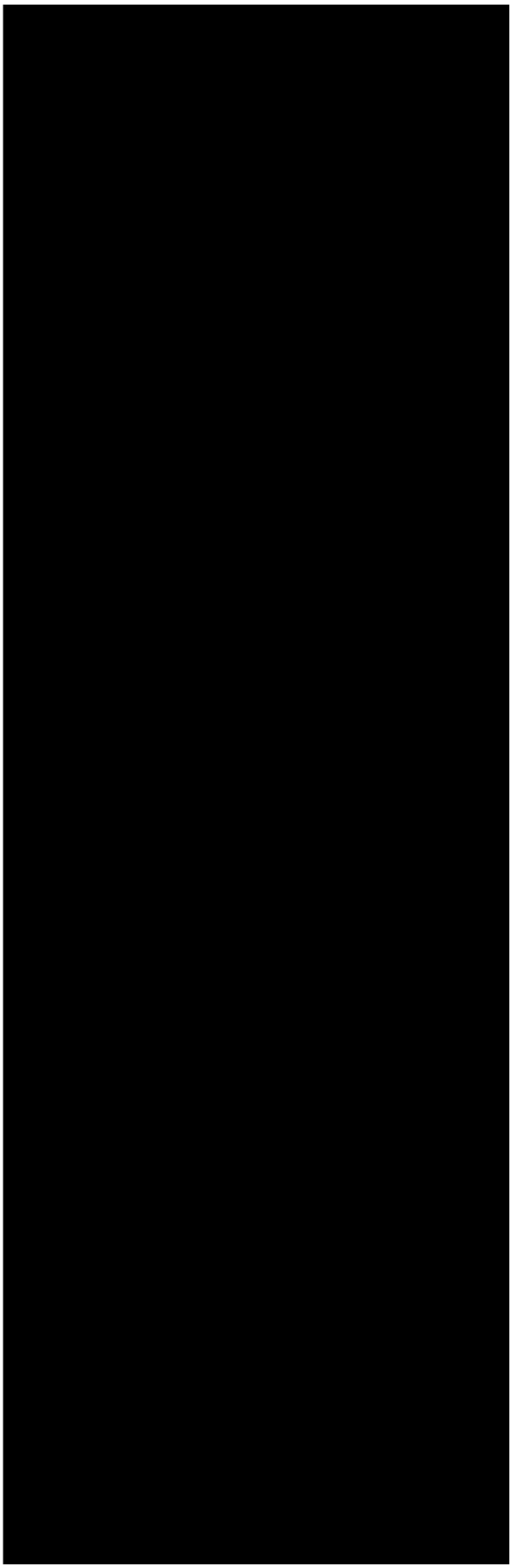
The Cyber-Posture of the National Information Infrastructure



Critical Technologies Institute
RAND

The research described in this report was conducted by RAND's Critical Technologies Institute.

ISBN: 0-8330-2621-6

Published 1998 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1333 H St., N.W., Washington, D.C. 20005-4707
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org

The Cyber-Posture of the National Information Infrastructure

Willis H. Ware

Prepared for the
Office of Science and Technology Policy

Critical Technologies Institute

RAND

PREFACE

The United States increasingly relies on information networks for the conduct of vital business. These networks are potentially subject to major disruptions from a variety of external sources. To date, there has been no clear statement of the magnitude of this threat or the ability of the various networks to withstand or respond to such disruptions. This project examines the national communications and information infrastructure. The research was conducted for the Office of Science and Technology Policy with task funding from the National Science Foundation.

This report discusses the vulnerability of the national information infrastructure to external attacks and other kinds of disruptions. It assesses the extent of the data available for measuring this threat and discusses steps that private industry and the federal government can take to reduce national vulnerability.

The Critical Technologies Institute was created in 1991 by an act of Congress. It is a federally funded research and development center sponsored by the National Science Foundation and managed by RAND, a nonprofit corporation created for the purpose of improving public policy. CTI's mission is to help improve public policy decisions by conducting objective, independent research and analysis on policy issues that involve science and technology in order to

- Support the Office of Science and Technology Policy and other Executive Branch agencies, offices, and councils;

- Help science and technology decisionmakers understand the likely consequences of their decisions and choose among alternative policies; and
- Improve understanding in both the public and private sectors of the ways in which science and technology can better serve national objectives.

CTI research focuses on problems of science and technology policy that involve multiple agencies. In carrying out its mission, CTI consults broadly with representatives from private industry, institutions of higher education, and other nonprofit institutions.

Inquiries regarding CTI or this document may be directed to:

Bruce Don
Director, Critical Technologies Institute
RAND
1333 H St., N.W.
Washington, D.C. 20005
Phone: (202) 296-5000
Web: *http://www.rand.org/centers/cti/*
Email: cti@rand.org

CONTENTS

SUMMARY

BACKGROUND

There is no evidence that the "sky is falling in"; the country is not in imminent danger of massive disruption through infrastructure cyber-attacks. In part, this stems from the natural resilience the country has evolved from having to deal with natural disasters and man-caused events of various kinds and magnitudes; in part, from the natural responses of organizations to protect themselves against anything that causes operational intrusions or upsets.

The country can readily withstand some levels of attack and recover, and can even enhance its ability to do so by strengthening and/or expanding the mechanisms now in place to handle what are commonly called disaster areas or business disruptions. It follows that, for extreme events, the national preparation that has been completed for lesser ones will provide an enhanced basis for response to a "big one." For small attacks especially and for some moderate and/or coordinated attacks, the country can make do without—or with impaired—sectors of the normal infrastructure for limited periods of time; but at the cost of such consequences as reduced efficiency, inconvenience to the citizenry, loss of living affluence, and disruption of services.

If infrastructure attacks and intrusions are extensive enough and/or disrupt or destroy the functioning of very large geographical areas, or (for example) bring down most of a major industry, or if several kinds of attacks occur in a seemingly coordinated pattern, then the country cannot expect to sustain "business as usual." In fact, we may

have to deliberately stand down or limit some aspects of normal life on a regional or national basis.

FINDINGS

Even though the country is not in imminent danger of major cyberspace attacks, we should not be complacent about the possibility that our national judgment is wrong or our intelligence insight incomplete. Intentional infrastructure cyber-attacks are technically feasible; it is the probability of their happening that is uncertain. We must examine the situation and do a substantial amount of preparatory work to develop an accurate portrayal of national status and risk, level of preparedness, and a realistic estimate of threat.

We do not now have a comprehensive survey of the infrastructure vulnerabilities to cyber-attacks or of the resilience of the country to accommodate them. The resilience of the country can surely be enhanced, but a study of the present status is required before actions could be recommended. A status baseline is essential; e.g., preparedness planning, sources of and status of resilience, industry vulnerabilities, present sources of early warning.

We do not know what normalcy in the infrastructure is and how it varies with such things as season, world events, national holidays, etc. We need to establish what the engineering community would call the "noise level" in the infrastructure—namely, the day-to-day abnormal or accidental events that occur as a matter of routine operation.

Physical attack is one of high probability throughout the infrastructure. The United States government and the private sector must give it attention. Intelligence, early warning, and data sharing are collectively an early order of business.

In the infrastructure scheme of things, energy supplies, telecommunications, and computer-based systems share an inescapable position of centrality. Thus, they are collectively of first priority for attention and remedial actions.

- Without an ongoing supply of energy—electrical and/or petroleum based—an infrastructure will wind down to a state of quiescence over a few days or a few weeks.
- The public switched network (i.e., the national telephone system) is a singular point of concern because it provides the bulk of connectivity among computer systems, people, organizations, and functional entities. It is the backbone of interpersonal and organizational behavior.
- The federal information infrastructure is considered to be weakly postured on computer and network security. Agencies must be motivated—or directed—to respond, and their progress monitored.
- There are specific R&D "cyber-issues" relevant to protecting critical infrastructures, particularly with respect to the computer system/telecommunication/information infrastructure. The research community must become aware of them, and be motivated to respond.

ACTIONS

Immediate actions include improving the information security posture not only in government but throughout the private sector. Physical security needs prompt examination and, as required, attention.

Near-term actions include analytic studies to establish such infrastructure features as source of resilience and characterization of normalcy (i.e., establish the noise level), and to specify R&D requirements.

Medium-term actions include establishment of a warning mechanism and a supporting coordination center.

For some of these steps, White House–sponsored conferences might be an appropriate and useful mechanism, but any mechanism available to the country should also be exploited.

ACRONYMS

CERT	CERT Coordination Center—initially sponsored by the Department of Defense, but now moving to commercial sponsorship. It is the oldest and main United States coordination center and is located at the Carnegie-Mellon University *[http://www.cert.org]*. CERT originally meant Computer Emergency Response Team
CIAC	Computer Incident Advisory Center—sponsored by the Department of Energy *[http://ciac.llnl.org]*
CIP	Critical Infrastructure Protection; a convenient term to refer to that part of the infrastructure warranting specific protective measures
DARPA	Defense Advanced Research Projects Agency
FedCert	Federal CERT; a consortium of public and private CERT organizations that supports the federal agencies collectively
FEMA	Federal Emergency Management Administration
FinCen	(Department of Treasury's) Financial Center for monitoring money flows and related events
FIRST	Forum of Incident Response and Security Teams *[http://www.first.org]*
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation

OMB	Office of Management and Budget
PCCIP	President's Commission on Critical Infrastructure Protection *[http://www.pccip.gov]*
PL	Public Law
PSN	Public Switched Network—a collective term for the national telephone utility
PSTN	Public Switched Telephone Network—a synonym for PSN
SCADA	Supervisory Control and Data Acquisition
SSA	Social Security Administration
TCSEC	Trusted Computer System Evaluation Criteria
USAF	United States Air Force
USDA	U.S. Department of Agriculture

Chapter One

INTRODUCTION[1]

CONTEXT

Because of a growing awareness that the country's infrastructure faces physical and cyber-based threats with risks of consequent damage, President Clinton created, by Executive Order 13010 on July 15, 1996, the President's Commission on Critical Infrastructure Protection (PCCIP).[2] According to the terms of the Mission Objectives (drafted by the Commission during its first 30 days), it was to

> . . . examine physical and cyber threats to the critical infrastructures, as well as the effects of natural disasters . . . identify and leverage ongoing initiatives at federal, state and local levels, in industry, and throughout society that address infrastructure vulnerabilities, threats, and related issues . . . [and] then integrate these initiatives and results into the formulation of realistic national assurance strategies.

[1]The final draft of this document was completed on the same day but prior to the announcement that the President's Commission on Critical Information Protection had posted its final report on its web site. Since the Commission report had not then been read or studied, we have not modified our discussion to reflect what it said. On the other hand, we did have knowledge of that report, derived as described below. Any overlap or similarity of position between this document and the Commission report is a result of coincidence of interests and a common understanding of the issues. This discussion intentionally includes supplementary and background discussion to make it complete and readable in itself.

[2]See the Commission web site at *http://www.pccip.gov* for the text of the executive order, the mission objectives, and related documents.

The report of the Commission was released to the White House on October 20, 1997, but a great deal of information about its findings had become available through media releases and presentations by Chairman Robert (Tom) Marsh (General, USAF, retired) to various groups[3]—in particular, his keynote address to the 1997 National Information System Security Conference.[4] We therefore have generally been aware of the thrust and views of the Commission but not its detailed recommendations. Material releasable to the public has been made available through the Commission's web site,[5] including a summary of the Commission's report.[6]

The concept of guarding the national infrastructure—especially its critical components—against attack is also referred to as *cyberwar* and in a broader context, as *strategic information warfare.*[7]

THIS DOCUMENT

This discussion is neither a critique of nor a commentary on the PCCIP report. Rather, it should be considered an adjunct document with an independent viewpoint.[8]

We concentrate on the information and communications sector of the national infrastructure, one of the five discussed in the Com-

---

[3]For example, the Commission meeting with its Advisory Committee (co-chaired by Senator Sam Nunn and Jamie Garelick), September 5, 1997, National Press Club, Washington, D.C.

[4]Opening keynote address, National Information System Security Conference, October 7–10, 1997, Baltimore, Md.

[5]*http://www.pccip.gov.*

[6]This summary is available at *http://www.pccip.gov/summary.html.*

[7]For an analytical treatment of these larger aspects, see R. C. Molander, A. S. Riddile, and P. A. Wilson, *Strategic Information Warfare: A New Face of War,* Santa Monica, Calif.: RAND, MR-661-OSD, 1996, which sets information attacks in the context of game exercises as a tool to help policymakers understand the effects and implications of an infrastructure attack; and J. Arquilla and D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age,* Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997, a collection of essays to set the context of such attacks and innovate measures against them. For a fictionalized treatment, see John Arquilla, "The Great Cyberwar of 2002," *Wired,* February 1998, p. 122ff., a vivid, cautionary short story.

[8]Concurrent with the completion of this document, the full text of the Commission report was made available through its web site. See, however, footnote 1.

mission report. The others admittedly are also of importance and in fact embed both telecommunications and information technology within them. But we are not concerned in this discussion with such events as poisoning of a domestic water supply, explosive destruction of bridges across a major river, the introduction of chemical or biologic agents into the general population, or any threat that is unique or novel to other sectors.

At the same time, we acknowledge that the technology, techniques, and even components (both hardware and/or software) from the telecommunications and computer fields are widely used in other sectors, notably in control systems and control mechanisms; e.g., SCADA[9] in the power industry, computer-based controls in nuclear and other powerplants; computer-based controls in automated factories.

We also note that the national infrastructure, even trimmed by the Commission to five areas for study, is extraordinarily complex; a thorough analysis and understanding of it will take a long time. This document, therefore, can only be a beginning analysis, plus some synthesis, of just one sector. In the same vein, we appreciate that examination of one sector by itself risks the possibility that important cross-sector or multisector vulnerabilities and aspects will be missed. More extensive studies will have to be done, but after individual sectors are well understood.

We specifically address the protection aspects of the information and telecommunications sector (which are implied and contained in every other sector), and we highlight some of the relevant parameters. However, it is not possible to discuss cyber aspects in particular without crossing over, to some extent, into other sectors. Indeed, some of the discussion that follows, and the actions suggested, apply equally well to several sectors. It is particularly convenient to use examples from others to illustrate the concept of resilience and the general aspects of the infrastructure.

To characterize the situation in the information infrastructure, extensive context and collateral exposition has been included to bring this document within reach of a nontechnical reader.

---

[9]For all acronym definitions, refer to p. xi.

A STRUCTURE FOR DISCUSSION

To maintain consistency in the policy discussion and to avoid inadvertent confusion in the dialogue, we will adopt the same division into sectors that the PCCIP has used. Initially these were, as assigned by the implementing Executive Order:

Telecommunications

Electric Power Systems

Transportation

Gas and Oil Transportation

Banking and Finance

Water Supply Systems

Emergency Services

Continuity of Government.

There was seemingly a significant omission in the list, although it is contained by implication in "telecommunications," namely, the totality of computer-based systems connected to and depending on telecommunications not only for outreach of individual systems but also for intersystem connectivity. While not all computer systems embedded in the infrastructure require the national telecommunication structure to exist and function properly, most do and even more will in the future.

As the Commission proceeded, it revised, slightly modified, and aggregated these sectors into five:

Information and Communications

Banking and Finance

Energy, including electrical power, oil, and gas

Physical Distribution

Vital Human Services.

Also for consistency in the national dialogue, we have adopted and will use, as necessary, the same acronyms introduced by the PCCIP. In particular, CIP is shorthand for Critical Infrastructure Protection;

namely, that portion of the national infrastructure which is considered most critical to national interests and, therefore, requires protection against cyber- and other attacks.

As a corollary observation, the PCCIP was not directed to address all possible sectors of the national economy, nor did it introduce sectors different from those stipulated by the implementing executive order. For example, the commission did not address food distribution (in all of its dimensions—physical, crop growth, electronic benefits, financial aspects) as a sector issue.

HISTORICAL PERSPECTIVE

We emphasize that the information and communications sector is central to all other sectors, indeed to essentially every aspect of national functioning. While this particular sector has flourished and expanded remarkably in the last decade or so, there is little national experience with protecting it against intentional destructive or intrusive action. Computer security (as it was initially called) was first definitively characterized in a Defense Science Board report in 1970,[10] but practical and operational experience, in particular incorporation of security safeguards into systems, commenced much later.

The decade of the 1970s was devoted largely to research funded by the Department of Defense, notably the U.S. Air Force and DARPA, but real-world experience did not begin until the publication of a document entitled *Department of Defense Trusted Computer System Evaluation Criteria*—commonly known as The Orange Book or the TCSEC.[11]

---

[10]Willis H. Ware, ed., *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security,* Santa Monica, Calif.: RAND, R-609-1, published by RAND for the Department of Defense in February 1970 as a classified document and republished as an unclassified document in October 1979.

[11]DOD Computer Security Center, *Department of Defense Trusted Computer System Evaluation Criteria,* National Security Agency, CSC-STD-001-83, August 15, 1983. While the document is characterized in its preface as "a uniform set of requirements and basic evaluation classes," the TCSEC really filled the role of a standard and was subsequently adopted as a United States Government Department of Defense standard.

Even then, systems incorporating security safeguards were not installed until the late 1980s. Within government, the major experience had been with classified systems, with at least one example dating from the middle 1960s.[12] On the other hand, in the private sector, the principal experience has been in the financial community. Overall, little progress occurred until the last several years, when various malicious attacks against, and penetrations of, computer-based systems and networks began to grow in number.[13]

In contrast, there is some accumulated experience for telecommunications as a result of exposure of the national telephone system to malicious acts (e.g., the "blue-box phreaks" and other attacks) plus the government-funded cold-war protective actions that were taken in its behalf. Nonetheless, the intensive computerization of the telecommunications industry has introduced entirely different and new vulnerabilities with which there is much less experience.

---

[12]Bernard Peters, "Security Considerations in a Multi-Programmed Computer System," *AFIPS Conference Proceedings*, Vol. 30, 1965, p. 283ff.

[13]See, for example, *Cybernation, The American Infrastructure in the Information Age*, Office of Science and Technology Policy, Executive Office of the President, p. 18. This document has an internal date of April, 1997, but it was embargoed until November 12, 1997. It is subtitled *A Technical Primer on Risks and Reliability*, is tutorial in nature, and presents an overview of the infrastructure issue. It concludes by suggesting areas for public policy attention.

Chapter Two

THE NATURE OF THE PROBLEM

To put damage to the national infrastructure in context, consider first that a major point driving modern automation—in particular, its intense dependence on information technology—is efficient and economical operation not only of the infrastructure itself but also of the national industrial base. A second driver is new functionality—often, more-elegant functionality.

Such advances include the following examples.

- Smart roads that automatically collect tolls without impeding traffic;
- On-line air travel, hotel, and auto reservations that bring such actions into the home for personal convenience and customer attraction;
- On-line banking and other financial transactions, for example, to conduct stock transactions from the home;
- Automated control of the power grid to minimize cost of needless generation of power or to rapidly restore/reconfigure the network during periods of heavy demand or emergency;
- Computer-based switching and routing in the telephone network to quickly adapt system configuration to demand, and to optimize the utilization of the installed plant;
- Efficient delivery of finished goods to minimize on-site storage requirements and to optimize their placement with market demand;

- Support of manufacturing technology to improve uniformity of products, to enable unattended extra shift operations—including use of robots, or even just to be able to manufacture such things as microcircuits;
- Automatically scheduled maintenance actions of many kinds; e.g., oiling schedules for large power generators, route scheduling of aircraft so that each one is near a maintenance facility when a compulsory overhaul becomes due;
- Automatic operation of manufacturing plants for all manner of finished goods; e.g., automobiles, pharmaceuticals, foodstuffs.

While these examples would superficially seem to be stand-alone functional systems, in fact most will have connectivity to other systems—for example, through local-area networks, corporate networks, dial-up connections via the public switched networks, wide-area networks, or satellite links. Such connectivity, for example, could be (a) to other facilities within a corporate structure or to other systems outside the immediate corporate structure (such as inventory control, or vendor systems); (b) for remote electronic maintenance actions (as is common in the telecommunications industry); (c) to accommodate facilities that are geographically widespread (such as the power grid or some water supply systems); or (d) to support multisite, multivendor development of software.

In each such instance of automation, the sources of operational economy include such things as

- Fewer people for both operations and maintenance;
- More efficient use of resources, such as coal or oil;
- Convenience for public users (and thus a competitive advantage);
- New services for the public, such as on-line business licenses and permits;
- Just-in-time manufacturing (minimization of capital tied up in inventory);
- Timeliness of actions;

- Conservation of time and efficient use of time;
- Prompt connectivity among parties needing to interact.

It is to be noted that the very drive for automation diminishes the size of a workforce that knows how and is trained "to do it the old way." Thus, one concludes that the more highly automated an industry or a sector is, the more vulnerable it is to malicious cyber intrusions; and the more difficulty such an industry would have to resurrect or create manual workarounds. This discussion identifies one of many tradeoffs that exist in the infrastructure issue; namely, how much efficiency and/or cost savings should be sacrificed for the sake of retaining people in the system as a hedge against accidental or deliberate failures in an automated system. The same point can be made for safety considerations: How should the retention of people in the system with their experience, training, and responsive problem-solving capabilities be traded off against the advantages of automation, which is likely to be less nimble and accommodating to abnormal situations?

DISRUPTIVE PHENOMENA

Admittedly, events will occur in the infrastructure that cause disruption to smooth system and overall operation, that cause dislocation of delivered services, or that force annoyances on end-users. Even significant disasters, especially regional ones, will occur. Abnormal events in the information structure occur on a daily basis and can arise from such sources as

- Natural phenomena—storms/floods/earthquakes/fires/volcanoes;
- Carelessness—often unintended, sometimes due to system design flaws, to extra-system events such as a backhoe severing a fiber cable, to inattentive people, to people under the influence of alcohol or controlled substances;
- Accidents—failure of system components, unanticipated conditions not included in the initial design but leading to destructive consequences;

- Oversights—actions or inactions of operators, improper interfaces in user/operator interfaces with the system, poorly trained operators.

INFRASTRUCTURE NOISE

It is convenient to borrow the concept of *noise* from the engineering discipline; namely, any spurious activity (in the form of electrical signals, audible signals, or other events) that perturbs, distorts, overrides, obscures, or interferes with the intended valid signal or communication or in general makes it less certain. It is an engineering truism that the intended valid signal can be completely obliterated or made unusable by sufficient noise—the ratio of (desired) signal to noise becomes too small.

Noise should be thought of as the unintended spurious events that occur daily throughout the national infrastructure; in effect, noise characterizes the normal state of affairs, some aspects of which are statistically predictable. Examples include

- Daily road accidents (numbers and locations);
- Daily numbers of banks that have problems with reconciliation of cash balances (numbers, names, locations, possibly also amounts);
- Daily outages throughout the public switched network (locations, nature, time extent, causes, remedial actions);
- Daily outages or interrupted services in urban utilities (locations, nature, time extent, causes, remedial actions);
- Daily interruptions and outages in the power grid (locations, causes, time extent, remedial actions);
- Daily criminal actions reported to national authorities;
- Pipeline outages and incidents;
- Major forest and brush fires.

And, as relevant, international events as well.

In the context of the above discussion, let us examine the relevance of noise.

- We often bring an event onto ourselves; we unintentionally create our own problems as a by-product of simply having and operating some aspect of the infrastructure. Our own day-by-day actions create infrastructure noise.
- Many disturbances to the infrastructure are from things we can do nothing about (natural events); as such, they must be accepted as a part of "doing business"—another contributor to noise.
- Such events must be accepted (so to speak) as a normal aspect of life. Collectively, they establish the normal status and background "noise level" in the infrastructure.

This noise floor, or noise background, is what we expect to happen each day; it equates to normalcy or the usual state of affairs. Since the country must function in spite of abnormal events, it follows that the noise floor collectively includes those events with which the country and its organizations are accustomed to dealing and are organized to handle.

The significance of infrastructure noise to CIP is simply that detection of and reaction to deliberate offensive attacks have to be distinguished from the noise, although they may have been carefully hidden in it. Thus, noise is a nuisance for the defense; an exploitable feature for the offense.

A collateral observation is that offensive acts of the kind typically hidden in infrastructure noise can be deliberately mounted to engage defensive procedures and forces in order to make them unavailable for more subtle and extensive cyber-attacks—i.e., in military parlance, a feint.

MODERATE AND LOW-LEVEL CIP ATTACKS AND INTRUSIONS

Next, consider the scale of events that might be intentionally created within the infrastructure. Start with low-end attacks. Several observations are pertinent.

- To the extent that infrastructure attacks approximate events that already happen as normal perturbations in the infrastructure—that is, approximate the noise background—the measures that the country and its organizations have developed and/or evolved are ready to combat them, to thwart them, to minimize their consequences, and to recover from them. This is the situation today.
- To the extent that infrastructure attacks exceed the consequences of routine events, the response mechanisms that have been developed and have evolved can be stretched and supplemented by ad hoc arrangements and actions. For example, we might
  - — employ large-scale use of military and national guard forces;
  - — use military airlift to move people/equipment/supplies as needed;
  - — use trucks to bring water into deprived areas;
  - — operate aircraft under manual flight procedures;
  - — suspend some services and/or the affluent aspects of normal life;
  - — make emergency money payments that preparedness plans already provide for; e.g., by FEMA or the SSA;
  - — use emergency provision of foodstuffs and shelter by private organizations such as the Red Cross.
- However, in this line of argument there is an inherent assumption that fuel and energy will be generally available to
  - —maintain some level of communications facilities;
  - —physically move goods and personnel from place to place;
  - —provide for the well-being of personnel; and
  - —provide for operations of emergency and recovery mechanisms, equipment, systems.

Moreover, there is a second implicit assumption that most of the country will have largely normal communications and infrastructure status and that affected areas will also have some level of communi-

cations and some level of operational infrastructure. Otherwise the unaffected parts could not come to the aid of the damaged part(s).

Observe that some things are stored as a normal part of infrastructure operations; e.g., gasoline, fuel oil, water, emergency supplies. Others are prepositioned to known places of consumption; for convenience, efficiency, or surge capability (e.g., the vehicles and equipment of the National Guard); or for smoothing delivery from sources (e.g., manufacturing inventory, raw materials). Collectively, these normal business and government activities add to a response mechanism for low-end infrastructure attacks.

EXTREMELY HIGH-LEVEL ATTACKS AND INTRUSIONS

If infrastructure attacks and intrusions are extensive enough to disrupt or destroy the functioning of very large geographical areas or (for example) bring down most of a major industry, or if several kinds of attacks occur in a seemingly coordinated pattern, then the country cannot expect to sustain "business as usual." In some sense, the country will have to be on a national emergency footing.[1]

We can expect that some things might have to be suspended or deferred—e.g., personal air travel, entertainment networks, pleasure driving. We can expect that some things will be minimized; e.g., elective surgery, imported or esoteric foods, low-priority use of water (lawns, car washes). On the contrary, we can expect some things to be escalated or maximized; e.g., preventive medical inoculations, public assistance (clearing debris, patrolling damaged areas), public service announcements (via television, radio, sound trucks).

But the high-end risk reflects an extreme possibility and certainly should not be an unwarranted driver that dominates the immediate response and actions of the country to the CIP issue.

---

[1]Terminology to describe national status following a major attack is of concern. One might be tempted to call it *wartime footing* or possibly *semi-wartime footing* but such phrases can imply that military forces or actions are involved, that Congress has taken some action, or that particular federal agencies have become active. The phrase *national emergency* or perhaps *regional emergency* would seem to be preferable.

It follows that, for extreme events, the national preparation that has been completed for lesser ones will provide an enhanced basis for response to a "big one."

PHYSICAL ATTACKS

Almost certainly, physical attacks against the facilities of the infrastructure will occur and probably will be among the first kind to materialize. Neither the threat nor the consequences will be uniform across all sectors. For example:

- It takes much more explosive to breach a concrete dam than to destroy or damage a building.
- It takes much higher skill levels to electronically disrupt computer-based systems than to blow up some of their facilities or sever their telecommunication cables.
- Bombing a ground terminal is much easier than destroying a communications satellite in orbit.

The common belief is that bombings are a preferred means of expression for terrorist organizations. They are relatively inexpensive, relatively easy to orchestrate and organize, relatively easy to execute, and make a very visible impact that attracts media attention.

For all these reasons, physical vulnerability across the infrastructure is of prime importance and deserves prompt attention.

CROSS-SECTOR ASPECTS

While this document focuses on the telecommunications and computer-system sector, there is interplay between it and all other sectors studied by the PCCIP. There is an emergent new and difficult "supra-issue"—one that transcends the separate protection of telecommunications and individual computer systems, even intensively networked ones. Because of the enormously widespread use of information technology in all manner of applications, new vulnerabilities arise not only from intersector dependencies but also, importantly, from intrasector, but intersystem, relationships.

It would be unwise to study and argue only about individual vertical sectors without regard for lateral interplay. Yet at the present stage of understanding and examination, it is expedient to examine sectors one by one to ascertain their vulnerabilities, identify the threats against each, and ascertain the general state of preparedness and posture of each. Some lateral effects will be self-evident and they can be included in sector studies. There are others that will emerge only as we improve our understanding and insights to individual sectors. Throughout the examination of individual sectors, we will have to be cautious lest we concentrate too intensely on one sector and overlook essential aspects of cross-sector interactions.

One sector can support another in various ways. Among them are

- Services—such as transportation, health care;
- Computing support and computer-based functions;
- Data—such as health care and disease incidence data collected by the Centers for Disease Control from the health-care industry;
- Utilities—such as electrical power, potable water, natural gas.

These examples tend to be self-evident ones, but there might be hidden or subtle ones as well—for example, a cross-sector data flow that is thought to originate in another sector but is found on close examination to arise from yet a third, flowing through the second on its way to the first. Events such as this simple illustration might well be dynamic in nature, especially as information systems become more autonomous and make their own choices about operational parameters and configuration, and their telecommunications arrangements.

Another way to frame this dimension of the problem is in terms of assumptions. When considering the vulnerabilities of the information and telecommunications sector and its ability to respond to a cyber-attack or even to a natural event, what assumptions have been made, either explicitly or implicitly, about support from other sectors?

Chapter Three

SETTING PRIORITIES

Of all the many sectors in the infrastructure—those studied by the Commission plus numerous others—are there some that are more pivotal to national interests than others? This is a question of some importance because availability of funds (in addition to other factors such as state of knowledge, detailed characteristics of a sector) will not permit doing everything concurrently that might possibly be conceived.

CENTRALITY OF ENERGY, COMMUNICATIONS, AND INFORMATION

Consider the following line of argument.

- It is obvious that all sectors of the infrastructure depend on telecommunications for efficient operation—sometimes, even for operation at all.
- It is also obvious that at the present level of dependence on information technology and computer-based systems and for some aspects of the infrastructure, the information base must also function; namely, the computer systems that are attached to the telecommunications structure and depend on it for connectivity among systems and for outreach.
- It is equally obvious that energy, in some form, is absolutely essential to make facilities and equipment function, and to sustain a minimum standard of living.

Consider a biological analogy. Deprive an organism of food and it dies from lack of energy. Deprive an organism of its nervous system and/or its brain and, at best, it will vegetate aimlessly. It will no longer be capable of purposeful behavior. These same observations apply equally well to the information infrastructure.

UNEVEN CONSEQUENCES

Not surprisingly, the consequences of these observations are uneven across the infrastructure.[1] Some examples illustrate the diversity.

- Except for locally stored fuel and electrical sources, a hospital cannot function effectively.
- Without fuel, trucks, trains, and aircraft will not operate and soft goods/food supplies/medical supplies/hard goods/personnel cannot be delivered or moved as needed.
- Without its information base, however, a smart highway can continue to operate, although probably at reduced efficiency and without collection of tolls.
- A bridge, if physically undamaged, can function but possibly without collection of tolls.
- Without its information base, the stock market would not operate.
- Without energy and some minimal information base, production of currency could not function (e.g., a U.S. Mint), nor could financial institutions distribute funds, except possibly gratis on a manual basis but limited to amounts on hand.
- Without energy, most water plants could not supply water. Some might function on a gravity-flow basis.
- Except for emergency battery-operated communications, emergency vehicles could not respond adequately.

---

[1]Formally, from the viewpoint of physics, *energy* and *power* are different concepts. In ordinary usage, they are often used loosely as synonyms; and in some cases energy is thought of as a generalized word for power. In this discussion, it is not necessary to distinguish between the two, and each is used as it commonly would be for the topic under consideration.

- Except for locally stored fuel and electrical sources, the public switched network (PSN) could not function.

CONSEQUENCES OF NO ENERGY

The bottom line is clear: *Without an ongoing supply of energy—electrical and/or petroleum-based—an infrastructure will, over a few days or a few weeks, wind down to a state of quiescence.*

The only exceptions would be those components that are totally physical in nature and are undamaged; e.g., highways, bridges, rails (but not trains), gravity water systems. With energy, but without communications or the necessary information base, some parts of the infrastructure could function at some level, but with seriously impaired efficiency. Other parts, in particular those heavily dependent on information/computer processing/telecommunications, are not likely to function at all.

Some sectors of the infrastructure are durable and with energy, can continue to function, perhaps almost normally. For example:

- With adequate sources of energy, water supplies could continue to function at some level, even without an information base, but possibly under manual, rather than automated, control. Large systems that span many hundreds of miles, such as the California Aqueduct or the California State Water System, would be more vulnerable to loss of the information and communication base than a small municipal system having only a few wells.
- With energy, trucks and trains could operate although at lower efficiency because of manual, rather than automated, control.
- With energy, but without its automated information base, air operations could continue at seriously reduced efficiency.
- With energy, but without its automated control system that depends on telecommunications, oil and gas pipelines could operate at some level of efficiency.

The end conclusion is quite clear: *In the infrastructure scheme of things, energy supplies, telecommunications, and computer-based services and controls share an inescapable position of centrality.*

Of these three, however, energy sources must come first. Without them, nothing much of significance will take place—certainly for an extended period of time—even though every computer system and telecommunications arrangement were functionally complete and, in principle, could be operational. To the extent that widespread storage of fuels and backup electrical power sources exist, energy—as a source of concern—might not at a given moment be of first priority, at least until emergency supplies have been exhausted.

In the case of electrical energy—or electrical power—there are many alternative sources (nuclear plants, coal-burning or gas-fired plants) that can provide robustness, provided that the distribution infrastructure is largely intact. There is great redundancy at the power-grid level but generally not near the end-user. Therefore, the vulnerability of electrical power is highly context dependent and, likely, also user-specific.

CONSEQUENCES OF NO INFORMATION BASE

Of the remaining two, it is a judgment call as to which prevails over the other. Without communications, some computer systems can perform useful work for local usage. In the evolving national and worldwide environment, however, it is most likely that networked systems and computers with electronic outreach will dominate the installed base. On this argument, one concludes that telecommunications ranks above the computer systems to the extent that they compete for allocation of national resources.

In fact, *the public switched network (PSN) is a singular point of national concern because it provides the bulk of connectivity among computer systems, people, organizations, and functional entities. It is the backbone of interpersonal and organizational behavior.*

In the allocation of the government's attention and in the allocation of resources, these three[2] must be of highest priority; but the PSN dominates the demand for attention partly because it is visible and accessible to so many people, partly because it is a softer target than energy sources and supplies, partly because it is so vulnerable to

[2]The three items we have discussed map into two of the sectors identified by the PCCIP.

cyber-based intrusions, and partly because its outside plant[3] is generally easy to physically damage.

RELATIVE PRIORITIES

Among energy, telecommunications, and computer systems, it is not clear, without more detailed examination of threats, industry status, and preparedness, how policy attention and R&D resources should be distributed. Given that anything must physically exist and operate if it is to perform functionally, certainly energy sources would seem to be in first place. Attacks against that sector, however, will most likely be physical ones, at least in the short term.

Since telecommunications has utility even in the absence of computer systems, it would seem to be in second place with computer systems following. On the other hand, both of them have a role in energy systems—so it is not obvious, without deeper insights into the precise nature of cyber- and other attacks, that this apparent ranking should be the dominant one for government and private-sector attention.

Moreover, the R&D needs among the three are, to some extent, different in nature—although telecommunications and computer systems share many. Thus, allocation of resources and setting of research priorities must await a careful and more detailed analysis of the infrastructure as it now exists.[4]

---

[3]Telephone jargon for the cables on pole lines, microwave towers and facilities, satellite ground stations, buried cables—in short, largely everything in a telephone system except for the switching centers and the administrative support facilities.

[4]Such an analysis is explored more fully in "Action 4" in Chapter Four. It is there referred to as "homework" to be done at the national level.

Chapter Four

KEY ELEMENTS OF A SOLUTION APPROACH

RELYING ON WHAT WE ALREADY HAVE

In view of our discussion above of background noise in the infrastructure and the observation that the country regularly accommodates a variety of natural and man-created events, there are clearly responses in place that can equally well address critical infrastructure anomalies. Examples include the following.

Resilience

The country has an inherent resilience against infrastructure disturbances. Many things contribute—among them, the following.

- The very size of the United States provides resilience. Natural disasters cannot—or at least, so far, have not and are not likely to ever—affect the entire country. Hence, the unaffected parts can and do respond with help for the affected part(s).

  Natural disasters (say, an earthquake), or infrastructure events triggered by natural causes (say, high winds blowing a tree across a power line) or civil disturbances are generally regional (e.g., a few counties and many cities in California when an earthquake occurs; hundreds or thousands of acres of brushland or forestland for a forest fire; a geographical segment of the country during a hurricane; one or more major cities and a few hundred thousands or many ten thousands of square miles of service area during a power grid collapse; a major part of a large city when a riot takes place).

On the other hand, natural disasters can be imagined that would be nationwide, but they would be extraordinary circumstances outside the scope of this present discussion. Perhaps the most devastating example would be an earth collision with a large asteroid; another, a major nuclear powerplant event or meltdown, triggered possibly by a major earthquake.

Most individual perturbations, short of extreme natural disasters, simply do not have the wide effect and nationwide consequences that (for example) a cold-war nuclear attack would have had.

- The experience and preparedness of companies in dealing with the normal perturbations in their corporate operations achieves resilience; e.g., telephone companies fly in repair crews to help disaster areas; fire crews deploy by air to combat major forest fires; special disaster relief forces move around the world as required (for example, the fighters of oil well fires in the Mideast); companies establish and use backup copies of their databases; corporations have alternate communication arrangements or provide backup electrical power or have their own fire fighting establishment; various levels of government cooperate with private sector organizations as required (for example, in fighting forest fires or preparing for large floods).
- The leftovers of the cold war, especially all the things that the country did to be ready for nuclear attacks and major conflicts, support resilience; e.g., the Red Cross, stockpiles of materials, civil defense (to the extent that it was implemented).
- Government preparedness, especially military readiness, brings resilience; e.g., FEMA, various emergency preparedness plans at national and state and local levels, planning and arrangements for continuity of government. There can be spillover from government preparedness to support in the private sector.

Enhancement

On an ad hoc basis or even on a programmed basis, storage and/or prepositioning can be expanded to enhance national resilience.

For example:

- Some things are easily expandable; e.g., stocks of gasoline and petroleum products, consumables such as pharmaceuticals and foodstuffs, potable water in reservoirs.
- Other things have fewer options; e.g., electrical power is more difficult to store but can be in the form of water (for hydropower sources) or nuclear power sources.
- Other examples include oil that can be and is stored; natural gas that can be and is stored (in underground caverns, in above-ground tanks in some parts of the country); storage of on-site consumables such as lubricating oils for nuclear powerplants.

Operating with Impaired Infrastructure

Based on the discussion above, it follows that, for limited spans of time, *the country can make do without—or with impaired—sector(s) of the normal infrastructure.*

This position is most likely to be accurate and applicable for small attacks against a single sector; it is less likely for large, complex, multisector attacks.

At the same time, just how long we can make do is unclear but certainly is related to the nature of the attack, the sector and its systems that are involved, and even on the proper functioning of other sectors. For example, the recovery of a damaged telecommunications region might be seriously delayed by a concurrent attack on the transportation sector because the needed materials could not be transported as required.

Moreover, there is a collateral observation of importance for larger, especially multisector, events. Given the high level of automation throughout the national infrastructure and the consequent dependency of all sectors on information technology, the national infrastructure might have to function at some, possibly a major, level of inefficiency. The inefficiency would, in effect, be one aspect of "not being able to sustain business as usual."

Under some attacks, the country could function adequately for some reasonable time—for example, without the National Severe Storm Warning Center or without the Centers for Disease Control, without some airports, or with limited scheduled air service. Other infrastructure losses that could be accommodated for some period include a loss of automated air traffic control, loss of a working stock exchange, even the loss of oil wells or petroleum supplies, the loss of water supplies in some parts of the country, the loss of parts of the telecommunications base.

Infrastructure losses of functionality aside, to offset shortages and/or to facilitate recovery and/or to minimize consequences of the attack, some things might have to stand down, be minimized, or be deferred—for example, financial transactions (international fund transfers), domestic and international stock transactions, possibly severe storm/tornado warnings, minimal air service, extensive but scheduled power brownouts.

Surely, there will be dislocations, interruptions, possibly fiscal losses, personal anguish and anxiety; the country—or at least regions of it—will not function with normal efficiency and with a normal complement of goods, services, and functions. While there will be both personal, corporate, and local-government annoyances and inconveniences, the country will not find itself in a major catastrophic position for low—even moderate—levels of infrastructure attacks. It will not collapse; it will eventually recover and survive.

Immediacy of the Need for Greater Action

There is an important "but" in this line of argument. In spite of observations that tend to be reassuring or even to suggest that government intervention might not be needed, the country must not be indifferent to the possibility of even low-level threats and events. Any one of them might be a harbinger of larger things or the precursor of a large multisector event. One cannot rule out the possibility that we could be under attack but fail to realize it, even with a functioning national warning center in place.

Since any event beyond those of normal day-by-day occurrences affects the country's status and well-being, at minimum we need to be

as knowledgeable as possible about cyber- and other attack possibilities, about threats, about preparedness, about counteractions and protective mechanisms. We must get protective measures in place, especially those that will serve other purposes and are well within the state of the art. Although there is no evidence that orchestrated intentional cyber-based attacks by sovereign powers or organized groups are occurring, the country should not dawdle in understanding them and instituting reasonable precautions.

The prior discussion notwithstanding, the very pervasiveness of the CIP issue throughout all aspects of the national structure—especially the pervasiveness of the telecommunications and computer system sector—makes government attention and leadership imperative.

RESEARCH AND DEVELOPMENT

Concentrating only on the telecommunications and computer-system sector, consider now the history of information-oriented research and the present R&D thrust of the information sector. Since the telecommunications sector is heavily computerized, achievements in the information sector will also benefit it. While there are specialized telecommunications R&D needs (e.g., the vulnerability of the electronic components of the system to high electromagnetic-energy radiation weapons), they are not treated here.

As with many of the country's national efforts (e.g., defense), the effectiveness of the money spent operationally is determined by know-how and the state of knowledge. The same relationship is also true for the protection of the critical infrastructure. There are problems for which we do not now have adequate answers; for some things, we have no answer. Thus, the nature of the investment in R&D will importantly determine how effective the country will be at using its available resources for the CIP mission.

Historical Setting of Computer Security R&D

The impetus for the security of computer systems and later data networks arose in the defense and intelligence communities during the late 1960s. Hence, the threat against the systems and the goals in providing security safeguards automatically mirrored defense con-

cerns. Moreover, all of the R&D at the time was funded by the United States government, especially the Department of Defense and the military services.

At the time (1970s–1980s), the focus of concern was the military/defense/intelligence threat—namely, a major foreign opponent that could mount a major military offensive and would conduct large-scale intelligence operations. The perceived threat against computer systems and networks, their operating environments, and their general embedding in an administrative setting all reflected the defense/intelligence mindset and concerns.[1]

The nondefense part of the federal government, and notably the private sector, was uninterested in computer security and contributed little to it beyond the work done on behalf of defense considerations. Thus, the R&D projects, particularly in academia, also reflected federal government defense interests and generally addressed problems whose solution would improve the security strength of the defense/intelligence computer-system base. To the extent that such solutions had importance to nondefense systems, they were adopted on a small scale. For example, a vendor that had invested the resources to produce a security product or system and had it evaluated by the government would substitute it for his normal commercial product and thus move the technology into the marketplace.[2]

---

[1]Willis H. Ware, *A Retrospective on the Criteria Movement*, Santa Monica, Calif.: RAND, P-7949, 1995; *New Vistas on Info-System Security*, Santa Monica, Calif.: RAND, P-7996, May 1997.

[2]Under the regime established by the TCSEC (Orange Book), vendors can submit products incorporating security safeguards to the National Computer Security Center (formerly the Department of Defense Computer Security Center) for "evaluation." This process is in addition to testing and product examination done by the vendor and includes extensive testing; examination of the engineering development process, especially for software; and review of the design process and its documentation. It is both expensive and time-consuming—typically, two years at minimum. Hence, an evaluated product, because of such a thorough post-vendor analysis, would generally be much improved relative to its preceding commercial version and could bring a market premium.

Contemporary Environment

From 1970 to the present, the nature of computer and communication technology has changed dramatically. Not only have the hardware and software technical and architectural aspects changed significantly, but so also has the nature of the services offered by computer-system networks to the public and among federal agencies.

Consider these contemporary computer-based services.

- The USDA now administers the food stamp and other welfare programs electronically.
- The SSA delivers some of its products to the public electronically.
- Federal agencies electronically interconnect their computer systems.
- Federal agencies are increasingly putting their database and information sources in an electronically accessible environment.
- The payments mechanism for medical insurance is now largely computer based but involves linking of government and private-sector systems and databases.
- Electronic-based fund transfers and payments are of growing importance.
- Commercial organizations (e.g., airlines, hotels, entertainment) provide public access to their databases for reservations and bookings.
- The financial industry, notably the bank-card segment, is largely automated and interfaces with the general public in many ways.
- Corresponding government services are provided electronically at state level.
- Extensive networking of computer systems has taken place. This includes not only outreach from a particular system but also interaction among systems, often on a wholly automated basis. Certainly the Internet and the World Wide Web that it supports are the prime example of this direction of progress.

- Many companies market, bill, and receive payments completely electronically.
- Internationally, electronic communications and financial transactions are extensive. So also are news/television/media broadcasts and exchanges.
- Companies whose workforce functions partly or largely in the home depend heavily on electronic communications and computer systems.

What we are seeing will become even more commonplace and add to the complexity of the information-telecommunications infrastructure. Computer systems, both inside and outside of the United States government, are increasingly opening their databases and systems to general public access for enhanced services, and consequently will be exposed to a broader threat spectrum of malicious individuals and organizations that, for various purposes, might attack/manipulate/penetrate/subvert/deny a system.

Contemporary R&D Needs

The point of this discussion is to stress that contemporary R&D has yet to adequately address the threats that much of the contemporary information infrastructure faces; rather, the R&D community tends to still address security considerations that originated with the earliest defense and intelligence interests. This is not to say that such R&D is irrelevant to the current threats and concerns; rather, that the present R&D menu is incomplete so far as infrastructure protection is concerned.[3]

The conclusion is that *the nationally funded R&D efforts should be reoriented to align with CIP requirements.*

Attention should be focused on them until the level of progress becomes equal to that in traditional defense-oriented research efforts. Here are a few examples, expressed in very general terms, of R&D

---

[3]R. H. Anderson and A. C. Hearn, *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After ... in Cyberspace II,"* Santa Monica, Calif.: RAND, MR-797-DARPA, 1996.

that is implied by an information-sector future that we can already see.[4]

- The so-called insider threat (dissident employee, in-place activist, former employee with continued access, the subverted employee, the angry or financially stressed system operator) is now of paramount importance everywhere. What technical and/or procedural and/or management safeguards and/or personnel safeguards can be conceived to help thwart this dimension of threat or to identify its presence?
- In the traditional computer security approach, application software (account posting, database updating, benefit determinations and calculations, check issuance) depends on security safeguards elsewhere in the system (notably, in the operating system software). With today's systems that "push" the databases and the systems outward to public exposure, there is an emerging awareness that "applications will have to take care of themselves."[5]

  The implication is that security safeguards, tailored to the details of the processes embedded in the application, will be required to recognize and counter emerging threats and should be included within the applications. Research on application-centric safeguards has had little attention.

  Similarly, there are specialized threats against the telecommunication systems—which are largely computer based and controlled—and corresponding specialized safeguards are implied.

  What R&D efforts should be in place to support these emerging aspects of the computer/network system security threats and risks?
- As computer-based systems more and more interconnect automatically on an ad hoc demand basis, there arises the issue of mutual recognition and authentication among systems, among users, among processes, among databases, and among combina-

---

[4]For fuller discussion of some of these items, see Ware (1997).

[5]From a private conversation with Mr. Colin Crook, retired Chief Technology Officer of Citibank, New York City.

tions of them. Eventually, there will probably have to be mutual recognition and authentication procedures at such interfaces as

— user-to-system

— user-to-process

— user-to-data

— system-to-system

— system-to-process

— process-to-process

— process-to-data.

What are the appropriate security safeguards and mechanisms for such a complex environment? Modern cryptography is one possibility, but not the only one.

- There is an extension of the prior point; namely, as two systems interconnect on an ad hoc demand basis, how does each know what data may be exchanged or accessed, what processes may be used by what users on which systems against what data, and even what processes may be automatically called (without user intervention) by one system for execution on another? Pre-arrangements are obviously one answer, but automated arrangements will be required.

  New protocols are probably implied; certainly, new safeguards and parameter/data exchanges are indicated.

- Establishing personnel trustedness, especially in the private sector and in some parts of the civil government, is an issue of concern and related to the insider-threat problem. Technical and/or procedural safeguards must be developed to offset such risks; e.g., two-person control such as that used in the military forces for sensitive assignments (particularly as developed for nuclear-weapon command and control and nuclear-weapon storage bunker access).

  What R&D, especially that oriented toward technical safeguards, should be undertaken?

UNITED STATES GOVERNMENT RESPONSES

The PCCIP has urged that the United States government must show—and lead by example—that the infrastructure protection issue needs attention and action. Nowhere is this more important than getting the government's house in order with respect to computer-system and network security and safety. The government has been flirting with such an effort for about two decades, and various policy documents have been put in place (e.g., OMB Circular A-130 and its Appendix III[6]) and documents written (e.g., the NIST computer security handbook[7]). The Computer Security Act of 1987 (PL 100-235) was intended to strengthen system security, but it has not had enough impact.[8]

Various study groups, interagency task forces, advisory boards, etc., have addressed the issue and flagged its importance to the government,[9] but the prevailing opinion continues to be that *federal computer-system and network security is not in an adequately strong posture.*

In the end, good security in the computer system and network portion of the CIP will be a first line of defense not only within the government but also throughout the infrastructure.

---

[6]Office of Management and Budget, *Management of Federal Information Resources, Appendix III—Security of Federal Information,* Circular A-130, February 1996.

[7]*An Introduction to Computer Security: The NIST Handbook,* Special Publication 800-12, Gaithersburg, Md.: National Institute of Standards and Technology, February 1996, *http://csrc.nist.gov/nistpubs/800-12.*

[8] HR 1309, introduced by Congresswoman Morella and others, will act to improve the original Act; but it is not yet clear whether it will be enough to bring the agencies into action.

[9]For example, the Defense Science Board examined information warfare in the context of the Department of Defense (*Information Warfare Defense, Report of the Defense Science Board Task Force,* Office of the Undersecretary for Acquisition & Technology, Department of Defense, Washington, D.C., November 1997). It cautioned that the security status of military systems was not adequate. Also, the Computer System Security and Privacy Board (a statutory group under the Computer Security Act of 1987) has noted on several occasions that the security of federal information systems needed attention, and made various suggestions and recommendations *(http://csrc.nist.gov/csspab/).* Even the government has addressed this issue itself; the interagency Information Infrastructure Task Force identified security as needing attention.

SPECIFIC NATIONAL ACTIONS

The following suggestions are in the nature of "getting started" and "understanding the scene." By no means are they intended to define a total starter set, but they are fundamental to instituting an initial effort that can help create a foundation for more extensive and subsequent considerations. Some of these are of necessity government initiatives; others, government and/or private-sector ones.

The sequence reflects an intuitive ordering based on several factors: existing interest or activity already under way in the government; near-term versus longer-term importance and payoff, difficulty, and duration of the task; contribution to an improved national infrastructure posture; the calendar period over which the severity and probability of a major attack are likely to increase. Clearly, some of the actions could be undertaken concurrently.

Action 1: The United States government should organize to improve its information security posture expeditiously. It should direct the agencies to bring the security status of their information systems up to the best current practice; agency response and progress should be monitored.

In addition to the inherent importance of this action, it would also exhibit government leadership and concern about the vulnerabilities. Moreover, it is an action that the government can take without considerations of a public-private partnership.

Action 2: The government should highlight the information security issue vigorously throughout the private sector and take such steps as can be conceived to urge and motivate the private sector to rapidly improve its computer/network security posture.

Action 3: Assess the physical vulnerability of the infrastructure, especially the telecommunications and computer system dimensions. The situation might prove to be in relatively good condition because corporations and businesses are alert to such threats and take precautions as a normal aspect of business conduct. Moreover, for telecommunications, redundancy (e.g., alternate cable routings) tends to mitigate, but not eliminate, physical weaknesses.

Action 4: Sponsor national conferences, by sector initially but cross-sector eventually, to

- Identify the attributes of the country, its structure, its institutions and organizations that inherently contribute to resilience, and derive an estimate of the present level of resilience. This may be a difficult task—at minimum, it needs concerted attention to illuminate how parts of the country mutually support and buffer one another against risks and emergency events. Such an examination would be especially important in the telecommunications sector. Case studies (e.g., ice storms, hurricanes, forest fires, collapses of the power grid) could be useful in this process.
- Assess the present level of readiness to handle emergency situations throughout the infrastructure. This is an issue of special importance in the information and telecommunications area. Again, case studies could be useful.
- Assess the present level of computer/network security throughout the private sector (in part to supplement and support Action 2 above).
- Identify near-term actions that could be promptly taken to improve readiness or resilience, especially in the telecommunications and information sector.
- Solicit and identify ideas for urging an adequate private sector response to self-improvement of information security.
- Identify special CIP R&D requirements and needs, particularly in any sector that is heavily computer-based.
- Assemble a roster of currently existing "early warning mechanisms" that could contribute to a national alerting and monitoring center; e.g., the Centers for Disease Control, the various existing incident centers for computer/network security (CERT, CIAC, FedCert, FIRST), the Department of Treasury FinCen.

This group of actions is in the nature of "homework" that needs to be done before the country can make wise resource investments in CIP and establish appropriate guidance and policy. The intent is to

establish a current baseline and posture of the infrastructure. Without knowing how well the country is currently postured to withstand infrastructure attacks, resource allocation will not be optimal, may miss important targets of opportunity, and may be excessively costly.

We must also know how capable the country already is to respond to such infrastructure threats with in-place capabilities. The goal would be to assemble the best overall picture of the country's resilience—what the exposures to attack are and what mechanisms might be in place to counter them, the vulnerability status of various industries—and then at least to commence preparation of an overall national preparedness plan. In this regard, the PCCIP has done sector studies that can contribute insights.

Action 5: Realign the R&D programs funded by NSA, NIST, NSF, and DARPA to include new directions of information and security research as indicated by CIP requirements.

Action 6: As the PCCIP has indicated, put warning mechanisms in place together with a coordinating center to provide a dynamic overview of unusual or abnormal activity in the infrastructure, and do so with special emphasis on cyber concerns. Such functions must be alert to seemingly natural events that occur in the infrastructure on a daily basis that could be rehearsals for a larger cyber-attack, experiments in progress to probe the infrastructure, or trials of cyber-attack techniques. In this connection, the defense and intelligence establishments have long experience in operating such assessment centers; their wisdom and experience should be utilized.

Action 7: Construct national databases, by sector and using such historical data as may be available, to characterize normality (i.e., the noise level) in the national infrastructure; portray its dependence on other influences and forces in the country and world.

As discussed previously, there will always be some level of abnormal/unexpected/unscheduled/accidental events throughout the infrastructure. If unusual events occur or if attacks commence, it will be correspondingly harder to recognize them if we do not know (a) the normal status of the national infrastructure, (b) the noise inherent in it, (c) its seasonal or annual variation of status, (d) the influence of world events on it, (e) the influence of planned actions by the government for (say) military action. Without such insights, any warn-

ing mechanism will have a more difficult task of identifying attacks, especially ones that are penetration experiments, probes, or practice. Indeed, clever attacks might be intentionally disguised as normally occurring events.

ISBN 0-8330-2621-6

MR-976-OSTP