Stanford University

CISAC

Center for International Security and Arms Control

The Center for International Security and Arms Control, part of Stanford University's Institute for International Studies, is a multidisciplinary community dedicated to research and training in the field of international security. The Center brings together scholars, policymakers, scientists, area specialists, members of the business community, and other experts to examine a wide range of international security issues. CISAC publishes its own series of working papers and reports on its work and also sponsors a series, *Studies in International Security and Arms Control*, through Stanford University Press.

Center for International Security and Arms Control
Stanford University
320 Galvez Street
Stanford, California 94305-6165

(415) 723-9625

http://www-leland.stanford.edu/group/CISAC/

CISAC Working Paper

Review and Analysis of the Report of the President's Commission on Critical Infrastructure Protection

Stephen J. Lukasik

Center for International Security and Arms Control, Stanford University
Center for Global Security Research, Lawrence Livermore National Laboratories

January 1998

The views expressed in this report are those of a small team assembled to consider the "what next" issues following the publication of the Report of the President's Commission on Critical Infrastructure Protection. In order to give this response a single voice and style, one of the members of this group, Stephen J. Lukasik, took primary responsibility for drafting the manuscript. The ideas are shared ones that grew out of a close collaboration with the other team members: David D. Elliott, Seymour E. Goodman, and Stanley Trost.

ISBN 0-935371-49-4

Author

Stephen J. Lukasik is a former director of ARPA, a former chief scientist of the FCC, and has served in various capacities as vice presidents of TRW, Inc., the Xerox Corp., and the Northrop Corp. He is now "retired."He received his Ph.D. from the Massachusetts Institute of Technology.

Acknowledgments

Several people were helpful in the preparation and review of this report. In particular, Edward Feigenbaum and Paul Edwards provided thoughtful and constructive comments on the penultimate draft, and we would like to thank Diane Goodman for her help in editing and preparing the manuscript for production.

The Center is grateful to the Presidential Commission on Critical Infrastructure Protection and Lawrence Livermore National Laboratories for supporting this project. The opinions expressed here are those of the authors and do not represent positions of the Center, its supporters, or Stanford University.

Contents

Preface

In July 1996, President Clinton established the Commission on Critical Infrastructure Protection (PCCIP), with a charter to designate critical infrastructures, to assess their vulnerabilities, to recommend a comprehensive national policy and implementation strategy for protecting those infrastructures from physical and cyber threats, and to propose statutory or regulatory actions to effect the recommended remedies. The charter gave examples of critical infrastructures (most notably telecommunications, electrical power, banking and finance, and transportation systems), and the types of cyber threats of concern (electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures).

Some of the infrastructures are owned or controlled by the government, and hence the government can harden and restructure these systems and control access to achieve a greater degree of robustness. However, the President's Executive Order recognized that many of the critical infrastructures are developed, owned, operated, or used by the private sector and that government and private sector cooperation will be required to define acceptable measures for the protection and assurance of continued operation of these infrastructures.

The Stanford Center for International Security and Arms Control (CISAC), as part of its ongoing Program on Information Technology and International Security, and the Center for Global Security Research (CGSR) of the Lawrence Livermore National Laboratory (LLNL) have been conducting workshops to examine many of the issues related to the work of the Commission. In addition to the questions of vulnerabilities, threats, and possible remedies, we consider the impact on the marketplace of possible protective actions, costs in terms of capital and functionality, legal constraints, organizational responsibilities, and the probable need for international cooperation.

The first of these jointly sponsored workshops was held March 10-11, 1997, and included participation by members and staff of the Presidential Commission, the Stanford community, the information technology industry, and security specialists at infrastructure organizations, research companies, and the national laboratories. The results were published in two CISAC reports: *Workshop on Protecting and Assuring Critical National Infrastructure*, Stanford Center for International Security and Arms Control, July 1997, and Stephen Lukasik's *Public and Private Roles in the Protection of Information-Dependent Infrastructure*, Stanford Center for International Security and Arms Control, May 1997.

The second of these jointly sponsored workshops was held July 21-22, 1997. Participation again included members and staff of the PCCIP, and experts from the academic, government, national laboratory, and industrial communities. The results of the second workshop were published in *Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda*, Stanford Center for International Security and Arms Control, October 1997.

The PCCIP published its report, *Critical Foundations: Protecting America's Infrastructures*, in late October 1997. It offers 72 recommendations to improve the protection of the nation's critical infrastructures.

The following report, put together by a group of the organizers of the two CISAC-CGSR workshops, draws on the analyses and discussions of these earlier efforts, particularly on the Commission's Report, to assist in planning for the implementation of the Commission's recommendations. It starts by revisiting some of the Commission's central premises, and suggests that while there is reason to believe that the Commission's concerns over the long term are valid, more work is needed on these issues to fully support the PCCIP recommendations.

Next, the Commission's recommendations are examined from the standpoint of priority, in order try to provide a clear focus for early implementation efforts. Of the 72 recommendations, ten are identified as important first steps.

Due to the private ownership of most infrastructure systems, the Commission proposes new partnership relationships between the public and private sectors to accomplish the goal of protection. This paper questions and extends the Commission's thinking regarding the implementation of such arrangements. It concludes that the sharing of information between the public and the private sector will have to be carefully designed to protect the interests of all the parties involved. It also notes that while the nature of infrastructure systems makes them global in their operation, the Commission's Report treats the problem almost exclusively from a domestic viewpoint. This will work against organizing the international partners who will, of necessity, be an important part of the solution.

This paper is intended to be a constructive response to the Commission's Report. In terms of implementation, the paper suggests a number of organizational, management, and cost-sharing principles to guide the next steps. It presents a specific "strawman" program for discussions on "what to do next" with regard to the important and complex problems connected with the assurance and protection of critical infrastructures. In particular, it is intended as an input to help direct and focus further consideration of these problems at a third joint CISAC-CGSR workshop to be held February 26-27, 1998.

Michael M. May, Co-Director
Center for International Security and Arms Control

Seymour E. Goodman, Director
Program on Information Technology and National Security
Center for International Security and Arms Control

Ronald F. Lehman II, Director
Center for Global Security Research
Lawrence Livermore National Laboratories

Executive Summary

The Commission's Report speaks to a wide range of physical and cyber attacks on the nation's critical infrastructure systems. It reaches six major conclusions:

- That while the potential for interference with critical infrastructure from cyber threats is growing, both by the proliferation of tools that attackers might employ and by the increasing electronic connectivity of infrastructure control systems, there is little immediate threat of severe national-level attack. There is, however, reason to believe that the threat in the longer term is significant.

- In view of the substantial private ownership of infrastructure systems, effective action to counter what is believed to be a growing threat requires a partnership between the public and private sectors.

- The basis for a public-private partnership is the sharing of information related to current infrastructure operations, threats, vulnerabilities of hardware, software, and communications, and risk management methodologies.

- The threat to infrastructure systems is exacerbated by the tendency for failures in one part of an infrastructure system to spread, thus impacting a greater part of the system than that initially attacked.

- The Report outlines in general terms the need for certain organizational actions by the federal government for all of the infrastructures to which its attention was directed in its implementing directive. These include:

  A coordinating office within the National Security Council structure
  A support office in the Department of Commerce
  A Presidentially-appointed National Infrastructure Assurance Council
  Seven lead agencies to structure public-private information sharing
  Sector coordinators for each of the identified infrastructures

An Analysis Center to receive and analyze attack information
A national attack warning capability
Enhanced federal R&D expenditures in infrastructure assurance

- The Report calls for other long range programs to increase national awareness of the problem, to lead by example by improving the security of infrastructure systems under its direct control, and to review current legislation to determine where it is inadequate to deal with infrastructure threats from a law enforcement standpoint.

In the analysis presented here, there are nine areas identified where consideration of the Commission's findings can be usefully augmented. These include:

- A discussion of the time scale available for coordinating public and private initiatives, in view of the lack of immediate threat.

- The need for priorities, in view of the very large number of recommendations made by the Commission.

- An expanded discussion of the nature of the proposed public-private partnership, taking greater account of the incentives driving the suggested private sector participants.

- Broadening the scope of the public sector partners beyond that of executive branch organizations to include state and local regulators, international organizations, and other sovereign nations.

- The degree to which infrastructure systems are robust and the degree to which they are susceptible to cascading and catastrophic failure.

- The working of the market in providing enhanced security through the private investments of infrastructure operators, product vendors, and system integrators.

- The relationship between public and private R&D investments.

- The relationship between infrastructure assurance and the administration's controversial encryption policy.

- What costs will be incurred in protecting the nation's infrastructure and who should pay them.

This paper suggests eight areas where the Commission's proposals should be modified:

- That further action be confined to the telecommunications and the electric power infrastructures until more definite assessments of vulnerabilities and threats can be validated.

- For the same reason, the creation of new organizations be limited to the minimum necessary and that existing organizations be used, augmenting them as needed to handle new responsibilities. What is proposed here is:

  Proceed with the creation of a coordinating office in the NSC
  Expand the NSTAC to include the electric power industry representatives
  Use the FCC NRIC as the telecommunications sector coordinator
  Use the industry-supported NERC as the electric power sector coordinator
  Include the FCC as a telecommunications industry lead agency
  Include the FERC as an electric power lead agency
  Defer the establishment of the Analysis Center until the information flows are agreed upon

- Rely on the private investments of infrastructure operators, product vendors, and system integrators to improve the security of the nation's critical infrastructures.

- Limit federally-supported R&D to those areas of market failure, areas where investments are necessary but where private industry will not invest. This will require strong private industry participation in the formulation of a federal R&D program.

- Examine, as part of this R&D program, the failure modes of complex systems and the degree to which they are or are not susceptible to catastrophic failure.

- Provide such exemptions from the current encryption policy as may be required to protect the telecommunications and the electric power infrastructure operations, as has been done for the banking and finance industries.

- Focus early attention in the implementation of the Commission's recommendations to a short list of high priority actions. Prioritizing principles are proposed here and ten high priority actions are identified.

- In view of the complex issues surrounding information sharing, it is suggested that this not be the centerpiece of follow-on actions. Instead, it is proposed that federal actions be focused on those that require a minimum of joint public-private action.

Beyond simply providing enhanced security from a new "threat," it is suggested that implementing an infrastructure assurance program provides an important opportunity for the United States to exercise global leadership in understanding and controlling the adverse consequences of the technologies on which we all increasingly rely.

Introduction

Two previous CISAC–CGSR workshops have addressed policy and research issues related to infrastructure protection and were intended to assist the Commission in its difficult task. This paper is for use by attendees, including the Commission Transition Team, at the final workshop of that series. Its purpose is to raise issues for discussion to assist in the assessment and implementation of the Commission's important and far-reaching recommendations.[1] We identify and explore four issues central to the implementation of the Commission's recommendations:

- The nature and timing of possible cyber attacks on infrastructure systems
- Priorities for immediate actions
- The framework within which public and private entities interact
- How the costs of enhanced infrastructure protection might be allocated among the many organizations and funding sources potentially involved.

This paper presents notional ideas to stimulate further discussion, addressing the issues in sufficient detail to suggest some of their dimensions and possible solutions. It is organized into five major sections:

- An examination of some *premises* underlying the Report's findings and recommendations
- The identification of two issues, the *international* side of the problem and federal government *encryption* policy, which require further discussion
- A selection from the large number of recommendations in the Report that would appear to be of highest *priority*
- An exploration of the proposed public-private *partnerships*, taking, in contrast to the heavily federal government perspective of the Report, greater account of the objectives of the private sector organizations which may participate in the anticipated actions

[1] *Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection, Oct. 1997. Hereafter this will be referred to as the Report.

- Proposals for transforming the Commission’s Report into a plan of *implementation*. Besides adding detail, this section provides an alternative framework for proceeding that is less dependent on the partnership concept proposed by the Commission.

Premises Revisited

The Nature of Information Attacks and the Need for Action

The idea that highly automated and interconnected infrastructure systems might be successfully attacked through the adversarial employment of information technology is not a subject high on the public's agenda, nor even one that is easily appreciated. That computers can be unpredictable and that infrastructure systems fail on occasion are matters of common experience. The Commission's task was to link them into a credible threat of national importance now or in the future, and thus to justify changes in infrastructure management and regulation and the expenditure of resources to mitigate possible damage.

The Commission's argument is that while complex information-based systems contain within them the seeds of their destruction, the dimensions of these vulnerabilities are inadequately mapped. The Report provides two examples of information attacks on civilian infrastructure. One is that of a large scale attack on infrastructure widely distributed in space and concentrated in time:

> "… cyber attacks could be combined with physical attacks, against facilities or against human targets, in an effort to paralyze or panic large segments of society, damage our ability to respond to incidents …, hamper our ability to deploy conventional military forces, and otherwise limit the freedom of action of our national leadership."

The Report also presents a second example, what some members of the Commission have referred to as "death by a thousand cuts":

> "Many facilities whose physical damage or destruction would have a disruptive effect on infrastructure are purposely located in sparsely populated or even unpopulated areas. If they are physically attacked it may take some time before the attacks are reported. Even when they are reported, each incident is at first a local event, and if several such events occur over a period of weeks or months it may take

> considerable time before they are recognized as part of a pattern. Recognition that an attack is in progress could be delayed even if physical attacks were to occur simultaneously, if the targets were spread across several jurisdictions and no mass casualties were produced to generate 'breaking news' at the national level."

These illustrate the point made by the Commission that in addressing information attacks, there is a wide spectrum of possible attackers ranging from recreational hackers, criminals, and terrorists, to state-supported "information warriors."[2]

What is not made clear in the Report is that technical and management defenses against the various threats in the spectrum differ, as well as the responsibility for addressing them and the allocation of costs incurred. There is a "one size fits all" sense to the Commission's recommendations.

This lack of clarity in the threat to be countered can impede the implementation of the Commission's recommendations. Public bodies must adopt laws, support regulations, and appropriate funds. Government agencies and departments must implement programs. Private entities' operations, and balance sheets, will be impacted. The international community must respond in some way. All must share a reasonably common view of the situation to which they are reacting.

What is proposed later, presuming broad public support for the aggressive program that the Commission proposes does not materialize, is a modest and pragmatic subset of the Commission's recommendations. The objective is to suggest the most sensible and inexpensive measures available at this point in our understanding of the threats and of our vulnerability to those threats. In this way, it is hoped that some degree of public buy-in to the Commission's central thesis can be obtained, but at a price that is affordable in view of other national needs.

The Robustness of Infrastructure Systems

While infrastructure systems provide service over large geographical areas, their vulnerable points consist of identifiable nodes and links. The impact of physical attacks on a node or link will be limited to the area served by that part of the system. In the design of infrastructure, several obvious precautions are taken to limit the impact of the failure of individual nodes and links: redundancy, flexible interconnection of its parts to allow for reconfiguration, failure monitoring subsystems connected to system control facilities, avoidance of architectures that would be susceptible to cascading failures, etc. Such measures are taken to cope with a wide range of "expected" accidents: natural events, component failures, human error, and the like. Thus, to cause widespread infrastructure failure that would have national consequences, coordinated physical attacks would have to be directed against a number of nodes or links and would have to occur in a period short compared to the time to repair or reconfigure the system. While some number of coordinated physical attacks are feasible, the larger the number of such attacks the greater the chance that they will be detected and thwarted.

Cyber modes of attack can amplify the effectiveness of infrastructure attacks. Malicious code inserted into communication switches and the corruption of Internet addresses suggest that cyber attacks can cause widespread disruption of service. The demonstrated ability of outsiders to penetrate computer systems, as well as the damage potential of disgruntled or dishonest insiders support these concerns.

[2] The Report, pg. 20.

The presumed efficacy of cyber attacks is enhanced by the view that its effects will cascade through the system like falling dominos, each node failure serving to bring down connected nodes. There are some examples of such behavior—the storm over the Rockies that disrupts air travel through much of the United States; electric transmission lines dropping out as power drawn from surrounding regions to compensate for a plant or line outage causes overloading; and computerized trading that feeds orders into the market so phased in time as to amplify price movements:

> "More than any other country, we rely on a set of increasingly accessible and technologically reliable infrastructures, which have a growing collective dependence on domestic and global networks. This provides great opportunity, but it also presents new vulnerabilities that can be exploited. It heightens risk of cascading technological failure, and therefore of cascading disruption in the flow of essential goods and services. Computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways we cannot yet conceive."[3]

The robustness of infrastructure systems and the degree to which designed-in capacity is or is not adequate to handle abnormalities resulting from malicious attack is central to the Commission's argument. There is, however, no evidence to date of national paralysis from cascading system failures initiated, for example, by natural disasters or accidents. Such failures as do occur reach natural limits, either when designed-in protection mechanisms operate or when inherent system stability asserts itself.

On the other hand, the Commission notes that it "*may* [emphasis added] be possible" to be harmed "in ways we cannot yet conceive." This is the crux of the Commission's argument, and it receives support from the "normal accident" school of system reliability.[4] Since there is no easy way of assessing the "strength" of a cyber attack or the degree to which it could be successful, it is difficult to estimate the cost of mounting cyber attacks and the cost of defeating them. This is not to say that such matters need remain a mystery. Some of the R&D that the Commission proposes should be spent on infrastructure system simulation facilities, to shed light on these questions. Analyses of infrastructure system failures over the years; the way regulators and system operators have responded to revealed weaknesses; and an assessment of how new technical and management approaches to system design and operation have increased or reduced system robustness would also be informative.

In contrast to the "normal accident" view that system failure is unavoidable is the position that any required degree of reliability can be designed into a system.[5] It is also the case that studying system failure is a part of engineering design.[6] Since cyber attacks are unlikely to be a "bolt out of the blue, we can expect to learn the art and science of cyber defense from analyses of system penetrations and the design of countermeasures, from attacker probes, and from system vulnerability studies, both theoretical and experimental.

The point is that improved protection of infrastructure systems will come from an increasingly rich and deep understanding of the fundamental nature of complex systems. The Commission having begun the process of highlighting the issue, it is reasonable to expect

[3] The Report, pp. 4–5.

[4] Charles Perrow, *Normal Accidents: Living With High-Risk Technologies*, Basic Books, 1984.

[5] Scott D. Sagan, *The Limits of Safety*, Princeton University Press, Princeton, New Jersey, 1993, Chap. 1.

[6] Henry Petroski, *To Engineer is Human: The Role of Failure in Successful Design*, Random House, New York, 1982.

that through R&D investments of the type outlined in their Report, as well as through continuing engineering practice, there will be an evolving understanding of infrastructure vulnerabilities and an increasing level of intrinsic protection. This notwithstanding, the issue requiring illumination is whether the threat from state-supported attackers will increase more rapidly than will the normal growth in system robustness.

In brief, cascading system failures having serious consequences at the national level is a matter still open to study and analysis.

Federal Support of R&D

The Commission Report notes that the current level of federal R&D investment in information assurance is about $250M/year and it proposes that this be increased to a level of $1B/year over the next six years.[7]

There are three issues to be addressed before establishing a program of federal R&D for private infrastructure system protection. The first is to determine the degree to which infrastructure protection is a management problem, for which process "fixes" are appropriate, and to what extent it is a technical problem requiring R&D for its solution. The Commission recognizes this where, for example, it addresses the "insider" problem, and suggests ways in which the employer-employee relationship might be modified.[8] Related management issues are the control of the distribution of information, access to sensitive information, audit controls, and the like.

The second issue is to establish the R&D needed to enhance the protection of classified government infrastructure systems such as those related to national security, recognizing that these expenditures are less likely to yield results of utility for the protection of private sector systems. Clearly such systems have unique requirements by virtue of their critical national importance and their attractiveness as the targets of state-supported cyber attacks.

The third issue is to identify areas of market failure, where the R&D that should be undertaken is unlikely to be funded by information system product vendors. While the Report itself provides few details, the Commission reviewed current R&D on information assurance in some detail. An internal paper provides the basis for the following.[9] The level of private sector expenditures on information security R&D, estimated in an Institute for Defense Analyses study of 21 computer and telecommunication technology companies, is between $120M and $350M/year.[10] An internal PCCIP study of the R&D budgets of thirteen major companies suggested private information security R&D of $1B to $1.5B/year, a level of investment that is likely to increase over the next several years.[11]

Nevertheless, despite these levels of private investment, there are certain to be critical areas that are under-funded despite market pressure for the protection of proprietary information and for secure electronic commerce. The Report identifies several such areas: tools for the real-time detection, identification, and tracking of intruders across widely distributed networks; sensor technologies for monitoring network status; modeling and

[7] The Report, pg. 89.

[8] The Report, pp. 87-88.

[9] John C. Davis, *Research and Development Recommendations for Protecting and Assuring Critical National Infrastructures*, PCCIP, September 24, 1997.

[10] W. Mayfield and R. Ross, *Evolving a National Information Assurance Research Agendas: Issues and Opinions from Commercial Information Technology Providers*, Institute for Defense Analyses, Alexandria, Va., July 1997.

[11] M. Adams, private communication, September 1997.

simulation facilities and tools for system-level studies; proof-of-principle demonstrations of new technology; and prototype analysis/warning centers. A particularly important area is that of basic research in complex systems, in their nature and their failure modes, and ways of reducing unanticipated behaviors.

Until the needs for information assurance R&D are understood in these terms, it is difficult to see how realistic R&D funding levels can be established. The level and focus of public funding for R&D should be carefully integrated with private investment to assure the most effective combination. The Report recommends that the National Research Council, working with federal departments and agencies already engaged in relevant R&D, define an appropriate program.[12] This is an important task to be undertaken as a first order of business.

[12] The Report, pg. 90.

Anomalies

The International Dimension of Infrastructure Protection

In the opening chapters of the Commission's Report, the fundamental international character of the infrastructure protection problem is clearly established:

> "We must learn to negotiate a new geography, where borders are irrelevant and distances meaningless, where an enemy may be able to harm the vital systems we depend on without confronting our military power."[13]

Later, in discussing federal responsibilities, the Commission offers a more detailed description of the international dimension of the problem:

> "In the new geography, protecting our infrastructures at home is not enough. Many aspects of infrastructure operations extend beyond our national borders, and even beyond the control of their owners and operators. The very nature of the cyber dimension renders national borders almost obsolete, and national laws and policies based on those borders of less and less consequence. Initiatives to construct partnerships between and among sectors and infrastructures must of necessity take into account the international character of business. The overall success of our own infrastructure assurance efforts will therefore require substantial international collaboration. The federal government should continue efforts to work with appropriate international bodies to address infrastructure protection concerns and raise the level of international cooperation and coordination on computer intrusion matters. An effective international regime to deter cyber crimes and cyber attacks will be more effective than purely national sanctions. Clarification of the dynamics surrounding a "cyber attack" under international law would also contribute to deterrence. Other

[13] The Report, Executive Summary pg. ix.

> issues worthy of international dialog include the handling of cyber crimes that transcend borders, and legal responsibilities in multinational infrastructures. Diplomatic efforts can also contribute to the success of our national encryption policy and the development of internationally accepted standards for computer security and information technology."[14]

At earlier meetings at CISAC, it was noted that attackers are likely to launch their attack from outside the United States or, even if they are located within the United States, are likely to route their attack through non-U.S. locations to impede defenders from establishing the attacker's identity and to introduce jurisdictional complication into the pursuit:[15]

> "It sometimes takes months, even years, to determine the significance of individual computer attacks. In a highly publicized 1994 Rome Labs case, the main intruder—a London teenager—was caught in the act; but his accomplice and mentor—who turned out to be a Welsh computer specialist only a couple of years older—was not identified and arrested until more than two years later."

Other arguments reinforce the need for an international perspective on infrastructure protection. Some infrastructures are international in extent, and corporate ownership is becoming increasingly international. These large organizations can themselves be targeted, and their responsibilities will extend over several legal jurisdictions.

Despite this ample evidence that the Commission fully appreciates the international aspects of the problem, including the need to focus the intelligence community on information threats (ref. 27), the Report is largely silent when it comes to making recommendations for action. There is only one among the 72 recommendations that recognizes the need to address international cooperation:

> "We recommend the Administration lead efforts to clarify and improve current procedures for investigating computer crime; work to create a network of international law enforcement agencies and telecommunications carriers to facilitate international investigations of computer crimes; and continue efforts to enhance international cooperation in computer crime investigations."[16]

Shaping the international environment for cooperation in controlling information attacks will be a lengthy process and, like R&D, the sooner one starts the sooner something is likely to happen. Two CISAC reports structure the issue of international cooperation and provide a number of starting points.[17,18]

[14] The Report, pp. 63-64.

[15] The Report, pg. 18-19.

[16] The Report, pg. 85.

[17] Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, *Old Law for a New World? The Applicability of International Law to Information Warfare,* Stanford University Center for International Security and Arms Control, February 1997.

[18] Kevin J. Soo Hoo, Kenneth B. Malpass, Kevin Harrington, David D. Elliott, and Seymour E. Goodman, *Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda,* Stanford University Center for International Security and Arms Control, October 1997.

The paradigm for much of the thinking about response to information attacks is detect-locate-identify-punish, which, if punishment is sufficiently certain, can add deterrence as a preventative technique. But if efforts to reach out to attackers, in effect the traditional forward defense strategy of the United States, are not undertaken, then we are reduced to leaving the initiative with the attacker and being forced to rely on terminal defense. In the near term, this may be our only option, but there is no reason why, for lack of attempting to generate international response options, we should forgo more pro-active defense concepts. In this sense the Report leaves part of the solution space unexplored.

There are several actions that might be undertaken to stimulate international interest in the problem. The first step must be to gain international partners who are likely to recognize their potential vulnerabilities to information attack. Concern over the possibility of attacks on highly automated infrastructure systems will be limited to technologically developed countries. This argues for raising the issue with single countries and small international organizations rather than with large organizations, most of whose members will be less developed and will tend to be indifferent to the issue.

One obvious such partner is Canada, which shares the management of the North American power grid. Another is Japan, which has established an activity like the PCCIP's sponsored by the Ministry of International Trade and Industry (MITI).[19] The G-7 Group is also an obvious place to begin a discussion of our concerns.

Another step that might be taken to begin to build a coalition is to schedule occasional sessions of the NRIC and NERC devoted to international issues and to invite foreign observers. NATO technical meetings on electronic and information warfare can also be used for the same purpose.

International consultative mechanisms organized to combat terrorism can provide fora for discussion of infrastructure protection. Protection of international air travel can provide an important precedent. While only advanced countries will identify with information attacks on sophisticated infrastructure systems, a larger set of countries can relate to the same situation when it is presented in terms of international state-supported terrorism.

We anticipate that bilateral and especially extensive multilateral international efforts to address these issues will take a long time to come to fruition. A common process for negotiating important and sensitive international agreements begins with exploratory conferences, leading to a framework convention that is essentially a commitment to participate in developing specific agreements, finally followed by treaties with real content. This often takes at least ten years. A decade from now, global integration of information and communications and other extensive infrastructure systems will be much further along among both advanced and less developed countries. Given this very long lead time, at least some serious consciousness raising efforts should start soon, and the United States is in the best position to take the lead.

Encryption Policy

The Commission Report recommends:

> "Expediting the several government pilot projects underway or recently announced as a means of testing the technical and policy concepts involved and building public confidence and trust with the KMI (Key Management Infrastructure) key recovery

[19] Press release, Tokyo, Japan, Kyodo report by Ministry of International Trade and Industry, Sep. 1, 1997.

> approach. Further, the Administration should promote efforts to plan for the implementation of a KMI that supports lawful key recovery on an international basis. Finally, the federal government should encourage efforts by commercial vendors to develop key recovery concepts and techniques." [20]

The Report notes that:

> "Key recovery is needed to provide business access to data when encryption keys are lost or maliciously misplaced, and court-authorized law enforcement access to the plain text of criminal-related communications and data lawfully seized."

This would appear to be related more to adding support to the Administration's encryption policy than to meeting a necessary requirement for infrastructure protection. The infrastructure in probably greatest need of encryption to safeguard its effective operation is that of banking and finance, and it has, through an exemption from the U.S. policy, the right to export strong encryption technology for the specific and limited purpose of conducting its global operations.

To the extent that other infrastructures similarly require the export of strong encryption for international operations, it would seem far simpler to grant further limited exemptions from the current policy than it is to embroil them in the broader policy debate. Infrastructure system operators constitute a quite specific set of users, subject to substantial regulation and oversight. It would seem that their use of strong encryption for infrastructure protection could be kept separate from uses that are the concerns of the law enforcement community. Licensing and auditing infrastructure operators for their specific needs would seem to be preferable to tying them to a key recovery scheme that is unlikely to achieve international acceptance.

Recommending tying infrastructure operator's use of strong encryption to key recovery runs counter to what the Commission was chartered to do and, if maintained, will limit the technical options available to infrastructure operators. Less, not more, infrastructure security will result.

Another consequence of linking the important task of infrastructure protection to key recovery schemes is that it raises objections to the Report quite unnecessarily. To the degree that the Report is a bridge to potential industry partners, there is no point in weakening it through its unnecessary association with a controversial policy.

[20] The Report, pp. 75.

Setting Priorities

Establishing Infrastructure System Priorities

The Commission was chartered to look into the protection of critical infrastructures, those being defined for it as eight, or nine if one treats information and its underlying communication infrastructure as separate: transportation, oil and gas production and storage, water supply, emergency services, government services, banking and finance, electrical power, and information and communication.

There is no question that these infrastructures are critical to the nation's well-being. But this does not mean that they are equally attractive or vulnerable targets. Some, for example, are more highly protected than others while others do not make extensive use of automated, and possibly vulnerable, national control facilities. Furthermore, the Report notes repeatedly that it is in the area of system *interdependencies* where attention is most needed.[21]

Finally, in the 5 September 1997 meeting of the Commission's Advisory Committee, the Commission was asked for priorities. It was noted that there are a large number of recommendations and that it is important to avoid overwhelming the public with proposals of varying degrees of importance. The Commission was also asked for near-term (1–2 year) goals and mid-term (3–6 year) goals. While the Commission responded in part to the latter request, with anticipated three-year outcomes, the Report does not offer guidance on the former.

Starting with the interdependency criterion, there are two infrastructures in a class by themselves in terms of the degree to which they underlie all other infrastructures: communication and electric power (note that the identification is the communication infrastructure only, not the information infrastructure that rides on it.) So in the following discussion, whenever organizational structures and tasks are indicated, they refer only to these two infrastructures, not to all the systems called out in the Commission's charter.

There are several other reasons for this choice. Both infrastructure systems are quite complex, highly automated, and dependent on interconnected control facilities, the communication system more so than electric power at this point but it too is moving toward more

[21] The Report, Executive Summary pg. ix.

centralized control even as it deregulates in a market sense. Both have relatively effective regulatory structures at the federal and state level. And both already have organized structures that could serve as a location for the Commission's proposed sector coordination function. In the case of the communication infrastructure these are the Network Reliability and Interoperability Council (NRIC) of the Federal Communications Commission, and the Joint Board that provides an interface between the federal government and state public utility commissions. The electric power industry has the North American Electric Reliability Council (NERC) to serve as the location of an infrastructure security coordinating group. Communications also has the National Security Telecommunications Advisory Committee (NSTAC), which could serve as the beginning of the Commission's proposed National Infrastructure Assurance Council.

To summarize, the selection criterion is interdependency, but the trend to central control that makes them targets, the existence of effective regulatory structures, and existing industry coordinating organizations that makes them easy starting points are also factors in their selection. The Report also identifies the NRIC as an organization to be tasked to address the collection and dissemination of infrastructure reliability data.[22]

When drawing a line through a list, it is often useful to ask what is the first item below the line. Using the above criteria, the banking and finance infrastructure would be next in terms of interdependency, central control structures, and effective regulatory organizations. There are several reasons why it probably does not need additional attention from the federal government at this time. It is on the firing line every day to prevent fraud and thus has practical experience in system protection. Risk management is deeply ingrained in the thought processes of its operators. It has won an exception to the rule barring the export of strong encryption. And enough money flows through the system that it should be able to finance its own needs for enhanced security. It has been burned in the past and it appreciates the difference between the individual criminal and organized crime, so the extrapolation to organized state-supported attack should not be difficult for it. As the Report notes in Appendix A:

> "Our principal finding is that, due to its carefully structured mixture of public oversight and private initiative, the U.S. financial system is among the world's finest. The modern U.S. financial system has never suffered a debilitating catastrophe, and for that reason among others carries an extraordinarily high level of global confidence."
>
> "The institutions comprising the financial services industry are further ahead than most in employing sophisticated and, in some cases, unique defenses against loss of assets and corruption of core data systems. Consequently, the U.S. financial system is unusually well protected at the national level and is well prepared to confront a broad range of threats to its operations and integrity."[23]

Whether or not this confidence in the robustness of the banking and finance infrastructure is fully justified, it does suggest that the industry is less likely to play a major partnership role of the type visualized by the Commission. However, since banking and finance systems are oriented more to the prevention of theft than to disruption, there may still be some need for

[22] The Report, pg. 41.

[23] The Report, pg. A-37.

their managers to avail themselves of the proffered public-private partnership. They may also have something to offer to other infrastructure operators in the matter of security lessons learned.

For the present, all other infrastructure systems can be left to their own devices pending a review in a few years of how well a focused federal infrastructure assurance program is working, getting a better understanding of information warfare threats, and recognizing that progress in other infrastructure areas can, if needed, be faster because of the organizational, legal, and technological developments achieved as a result of working with the communications and electric power industries.

A Short List of High Priority Recommendations

The Commission has made, in Chapters 5–11, a total of 72 recommendations. In addition, in Tables 3–7 in Chapter 7 it identifies 43 specific national functions required for infrastructure assurance. What criteria can one use to sort through this plethora of ideas to extract starting points and early targets? There are three. One selection criterion would be to invest resources in areas where larger resources can be leveraged, thereby achieving some early results for minimal outlay. A second is to do long term things first because they will take the most time to come to fruition. And a third is to "pick low-hanging fruit."

Applying these criteria to the recommendations in the Report suggests the following starting points. In offering this list, a near term period covering the first 12–18 months of an implementation program is intended. Thus, the suggestions below are only places to start, and are not intended to suggest that the other Commission recommendations are unimportant. If staff and resources are limited, it is suggested that these merit first action:

1. *Establish the Office of National Infrastructure Assurance (ONIA).* The task of this office will be to organize a coherent national program. With respect to funding, the ONIA can operate in two ways. It can coordinate infrastructure-related programs that are funded directly through agency budgets throughout the government. In this role its concern would be policy, strategy, program oversight, and formulation of legislative and regulatory proposals. A second mode of operation would be for ONIA to be directly responsible for program funds, managing them as the Defense Advanced Research Projects Agency (DARPA) does by transferring funds with program guidance to other organizations in government for implementation. The receiving organizations either undertake the work in-house, or they contract for all or part of the work to be performed externally. In the latter case they would provide the necessary procurement and contract management services. In either case it would be wise to start small and increase the ONIA staff as needed. Initially it could operate with a small number of positions, with individuals having experience in communications/computer engineering, regulatory law, foreign relations, and program planning. The NSC, in which it would be embedded, would provide the necessary support functions. The first mode of operation would fit more naturally into the NSC structure. Since there are existing programs and responsibilities in the various federal departments and agencies that could be applied to the task of infrastructure assurance, new funding could be minimized. Nevertheless, giving the ONIA at least some funds to use in direct support of its mission will aid its responsiveness. In particular, the ONIA should control the allocation of funds for new R&D.

2. *A first task for the ONIA should be to begin to leverage the enormous potential of market forces to achieve the purposes of infrastructure assurance.* The premise is that infrastructure assurance is highly desirable to system owners and operators because it translates to quality of service, customer satisfaction, competitive advantage, decreased regulatory interference, lower cost, and higher returns. It may be that there are currently laws and regulations on the books that are impeding the normal operation of market forces to achieve the levels of system protection the Commission seeks. Task the ONIA to confer with infrastructure operators and to come back in, say, four months with a specific list of action items to reduce current impediments to infrastructure assurance, either through executive order, through the regulatory process, or through legislation. In this way, it can demonstrate to the private sector that it is listening to them and that it is attempting to improve the climate to achieve enhanced system protection.

3. *Get the National Research Council started, per the Commission's Report on formulating the long term R&D program.*[24] Normally it requires some time to negotiate a task with the NRC and for the NRC to assemble the required committee. In this case there is an ongoing activity directed to infrastructure protection under the aegis of the Computer Science and Telecommunications Board that can at least serve as the nucleus of the desired group. Ask for an interim report in six months, to provide the ONIA a companion piece to its own regulatory review. The normal NRC process of soliciting outside views can also be used to start implementing the recommendation for the National Academy of Engineering to establish a strategy and awareness Round Table.[25] If the ONIA is established promptly and this and the previous suggestion are accomplished in the times indicated, there will be a good basis for the Office to begin its work early in FY 99.

4. *Upon receipt of some early input from the NRC, work with OSTP, DoD, DoE, DoC, and other government science and technology agencies to begin to work new R&D ideas into ongoing or new programs and contracts.* Expect to do some institution building in this area using current Federally Funded Research and Development Centers, university research centers, government laboratories, national laboratories, and industry-supported organizations. Leverage ONIA funding through joint programs and cost-sharing. While it will take 6–12 months to move money into the right places and to the right people, it will provide useful modes of ONIA outreach through the proposal solicitation and contract negotiation process.

5. *The recommendation calling for NSA, DoD, and DoE to provide assistance with vulnerability assessments is an example of how the federal government can bring a valuable asset to the partnership at small cost to itself but having a high value to private sector partners.*[26]

6. *The recommendation to elevate and formalize information threats as a foreign intelligence priority should also be implemented promptly.*[27] There is more to this initiative than simply generating information for limited distribution within the federal govern-

[24] The Report, pg. 90.

[25] The Report, pg. 68.

[26] The Report, pg. 39.

[27] The Report, pg. 75.

ment. Using such interface mechanisms as the NSTAC, NRIC, NERC, the NRC Round Table, and such other federal government-industry interfaces as may be utilized, a solution to the problem of communicating sensitive information to non-government infrastructure operators must be found. The simple way, of course, is to grant government security clearances to selected managers of infrastructure operations. But this extension of the security envelop to top management will achieve little if the recipient of the classified information can not use it in dealing with company employees and vendors. Nor, in fact, will industry people at the right places in their organization necessarily be clearable. It may, for example, be possible to use personal networks of trusted people to create a type of "system security certification."

7. *The implementation of a channel for the transfer from the federal government to the private sector of lessons learned in system protection is needed.* Like the transfer of threat information, sensitive information should be made available to an adequate number of private sector personnel that it can be effectively utilized by them. Such information would consist of data and procedures related to system flaws, personnel security, key management systems, multilevel security, connectivity architectures, etc. Useful interactions between the operators of secure federal systems and commercial system security providers should be encouraged through workshops, standards groups, and professional and industry programs.

8. *Implementation of the recommendation to encourage infrastructure operators to develop and adopt security-related standards can grow out of the consultation that the ONIA staff undertake as part of their regulatory review*.[28] This will be a lengthy process, and like R&D, the sooner it starts the sooner it can yield useful results. Its best chance of success is to establish clearly in private infrastructure operators' minds that standards for system security are voluntary "best practices" rather than mandatory regulations.

9. A*s will be discussed later in connection with the partnership concept, it is important that the federal government bring something to the table.* The GPS recommendation is an example of a way the federal government can make a contribution to the proposed partnership.[29] GPS is a government system and the DoD has world-class capability in electronic warfare and electronic countermeasures. The ONIA should broker a joint program between DoD and DOT to provide domestic protection for GPS on behalf of private sector infrastructure operators who will increasingly rely on it.

10. *The recommendation dealing with the National Airspace System is another case in point.*[30] The federal government can undertake initiatives within its jurisdiction to provide an important enhancement to an infrastructure that presents an attractive target for catastrophic disaster. Like the previous suggestion, this is another example of "low hanging fruit" where important benefits to the national infrastructure can be secured relatively easily.

[28] The Report, pg. 42.

[29] The Report, pg. 77.

[30] The Report, pg. 77.

The Concept of Partnership

The case for partnership in the protection of critical infrastructure is most directly put in the cover letter conveying the Commission's Report to the President:

> "Because the infrastructures are mainly privately owned and operated, we concluded that critical infrastructure assurance is a shared responsibility of the public and private sectors. The only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government … you will find some recommendations for collaborative public and private organizational arrangements that challenge our conventional way of thinking about government and private sector interaction."

Thus, the concept of partnership lies at the core of the Commission's proposals regarding infrastructure protection. Three chapters of its Report, entitled "Establishing the Partnership," "Building the Partnership," and "Structuring the Partnership" attempt to convey the Commission's concept. But despite this extensive discussion, the Report does not bring the matter into focus. For example, in one passage three different relationships are suggested:[31]

> "…to forge a partnership between all players—to achieve joint, integrated, and complementary action…"
>
> "The federal government should structure itself for its own mission of infrastructure assurance…"
>
> "…facilitating and supporting the efforts of critical infrastructure owners and operators."

So what is it? Joint and integrated action? Working separately but side by side for a common goal? Or helper on call? Part of the problem is also that the Report delicately avoids the central issue for everyone involved, "Who pays?"

[31] The Report, pg. 45.

When words fail to convey a meaning, it is often useful to return to the beginning. The dictionary definition of "partnership" that most closely matches what the Commission is talking about is:

> "a relationship resembling a legal partnership and usually involving close cooperation between parties *having specified and joint rights and responsibilities* [emphasis added]"

This perhaps points to a way to clarify the partnership concept: specify the rights and responsibilities of each party in the partnership. In principle, then, each party can calculate the costs incurred by it and the benefits flowing to it from these rights and responsibilities and decide whether it is in its interest to join the partnership. Determining who pays for what should also become clearer. From this perspective, the Commission's Report is more than a deliverable to the President. It also must be a proposal to a set of potential partners for a joint enterprise directed to the defense of their organizations, or the organizations they oversee, against physical and cyber attack.

Drafting what amounts to a partnership agreement without benefit of legal counsel is a perilous undertaking. But a starting point is a description of who the partners-to-be are, what they intend to accomplish, what each will contribute to the joint enterprise, and how they will share costs and derived benefits.

Who Are the Partners?

First, there is the federal government. But this is not specific enough. The federal government partners (plural) will include the national security agencies (DoD, intelligence community, NSC, DoS, and FBI for a start), the infrastructure industry's federal regulators, and depending on what money flows where and what anti-trust relief is required, could include Treasury, Justice and the IRS. The Congress will have obvious concerns and responsibilities, including those of the committees dealing with national security, appropriations, and regulatory oversight, and recognizing that new or restructured laws may eventually be required.

Second, since the infrastructure companies operate in various states, the state regulatory agencies will have a direct interest, especially in matters relating to costs, rates, and quality of service. Understanding both statutory and case law relating to the separation of rights and responsibilities between the states and the federal government in the matter of protection is a separate and complex subject.

Third, there are the infrastructure operators, who are by no means a homogeneous group. What most characterizes them is not their shared concern over national security but rather a deeply competitive relationship for market position, one that grows more intense as deregulation occurs. The infrastructure operators typically view their federal and state regulators in an adversarial way, while they are likely to see national security agencies as customers and the law enforcement agencies as both protectors and adversaries depending on whether any public agency is accusing them of alleged transgressions.

The Report notes that the suppliers of security and information technology and services must be involved.[32] Since they are also in competition with one another for infrastructure operator business, the extent of their willingness to participate in the proposed partnership is

[32] The Report, pg. 38.

difficult to judge, although on some subjects such as open standards they can find common cause. It may also be the case that at the outset the presence of suppliers may not be necessary.

Thus the public-private partnership that the Commission proposes would involve some unlikely associates. Participants in a partnership are supposed to start out with a measure of trust and respect, supported by a carefully drawn agreement. But with the infrastructure partners identified, it is hard to decide who distrusts whom the most.

Critical to the success of the public-private partnership envisaged by the Commission will be to make the agreements quite specific. Infrastructure operators will be alert to increased regulation and costly new reporting requirements, and to assuming national security burdens they think should be paid from the federal government's budget.

What are the Goals of Each Partner and How Can They be Accommodated?

The Commission's model of the private partners is that they will recognize the seriousness of the threat of state-supported cyber and physical attack and, spurred by patriotism and recognizing their "front line" position in such attacks, will make appropriate modification in facilities and in their ways of conducting business to prevent or limit the damage from such attacks. This is at odds with the policies of other parts of the federal and state governments that set each infrastructure owner apart from others and force the maximum degree of competition. Shareholder pressure for corporate performance and competitive and regulatory pressures for lowest possible rates suggests that the ability of owners to respond to a call for greater system assurance justified solely on basis of national security will be limited.

The conflict between national security and business performance is mediated by the time scale for action. Were the situation one of preparing for imminent war, crash programs to protect the nation's infrastructure would be initiated, all federally funded, and the infrastructure industries would respond to the clear and present danger. The historical analogy is the nation's pre-World War II mobilization. But the Commission, correctly, rejects this approach on the grounds that the threat is not immediate.

Consider the opposite extreme, where we believe we have considerable time to respond to the threat. Security R&D is undertaken and various technological fixes to infrastructure vulnerability are available. Communication network security improves due to market demands for electronic commerce. Personnel practices are modified in ways that enable private organizations to better protect themselves from dishonest employees. Infrastructure systems adapt to both new security technology and new security processes over several cycles of plant modernization. A culture of electronic security prevails in the United States and the developed world. How long might this take? A decade? A generation? Do we have the time to let society's natural defense mechanisms operate? Or will adversary information warriors strike before this can happen? The Commission recommendation to address this question is to increase the priority for information warfare threats in the intelligence community. This is clearly a step in the right direction and is one of the immediate actions suggested earlier.

Unfortunately, this sense of time is absent from the Commission's Report. A key issue is not only *what* should be done, but *when* it should be done. Will the information attack problem eventually go away, as happened in the Cold War? Will we have to come recover from an electronic Pearl Harbor, as in World War II? Should we start to strengthen the dikes immediately? The Commission's Report should, at the very least, serve to initiate this debate over the seriousness of the threat and the time available to respond.

Information Sharing Among Partners

Information sharing is identified by the Commission as a way to start the implementation of a public-private partnership for critical infrastructure protection. The partnership, under this concept, is thus defined, at least to first order, by the parties who have information they are willing to share. From the national security establishment will come risk assessment methodologies, and assistance to infrastructure operators in determining their vulnerabilities and a clearer picture of the threat evolution.[33,34] The Commission suggests infrastructure operators "establish a relationship with intelligence and law enforcement to assure that information about warnings and threats is communicated in a timely way."[35] How this critical step is to be accomplished is left unspecified. Nor does the proposal apparently recognize the difficulties many companies might have with a relationship with the intelligence community.

The Commission further calls upon infrastructure operators to exchange best practices for improving service reliability and security with their competitors, and to report *possible* [emphasis added] criminal activities to law enforcement agencies and to cooperate with investigations. This last is to be contrasted with the Commission's observation that only 17% of attacks experienced were reported to law enforcement agencies, suggesting significant reluctance to involve law enforcement officers with their operations.[36] The Commission also calls on the NRIC to study the feasibility of collecting and publishing comparative telecommunications infrastructure assurance-related data, and encourages the same be done for other infrastructures.[37] In the case of the electric power industry the NERC could be an agent for accomplishing this.

Having made information sharing a cornerstone for the establishment of this public-private collaboration, the Commission addresses the downsides and recommends steps to address them:

- that private information provided to the federal government is vulnerable to disclosure to competitors through the Freedom of Information Act
- that ways must be found to protect trade secrets and proprietary information from disclosure to competitors
- that exchange of information with competitors can possibly subject them to prosecution under anti-trust statutes
- that failure to share or act on warning information could generate liability exposure to all participants; and
- that information could flow to foreign corporations in contravention of export controls.[38]

The Commission further notes that all of these issues have separate interpretations in each of the fifty states and that this requires further analysis.

[33] The Report, pg. 76.
[34] The Report, pg. 39.
[35] The Report, pg. 37.
[36] The Report, pg. 28.
[37] The Report, pg. 41.
[38] The Report, pp. 31-33.

Finally, there are two information sharing issues relating to security classification. The first is that threat warnings will be classified, or will depend on classified information. Classifying information to be used by private operators poses a number of problems and tradeoffs. Either the information can be known to a few cleared people, which limits its utility for use in generating responses while still imposing costs on the private entities to establish and maintain approved facilities for the storage and use of such material. Or the classified material is more generally distributed within the private organization, thereby increasing its utility, but at a larger cost for the greater number of people to be cleared and the necessity of operating a part of the business on a classified basis.

A second type of classification problem is raised over the matter of system vulnerability. The Commission recommends:

> "The U.S. Security Policy Board be tasked to provide a recommendation to the President on criteria for and means of protecting *otherwise unclassified private sector information* [emphasis added] on threats and vulnerabilities to critical infrastructures."

What this appears to say is that private partners could find some of their own information classified and subject to government control. There are ways of dealing, at least in part, with this concern. Classification of information meets two needs, preventing wide distribution of potentially damaging information, and protecting the interests of the source of the information. One can assure the source of information that it can treat its information however it wants, but that the information is being classified to prevent its wide distribution by other recipients. When the concern of the source is competitors who could have access to classified information, much of the proprietary protection vanishes. Further compartmentation of classified information could address this problem, but at an increasingly complex information handling structure. The point here is not that these approaches are undesirable, but rather to flag the issues as part of what might otherwise appear as a simple notion of pooling proprietary and sensitive system information.

So how will all this sound to a potential private partner? There would appear to be very large negative impacts of joining with the federal government in the proffered information sharing partnership in terms of costs to collect information, the potential for having private information disclosed to competitors, and liabilities for various kinds of civil and criminal missteps. What the federal government offers to provide in return is modest, some of which will already be in the public domain. The exchange seems quite asymmetric and unlikely to attract many takers.

These potential difficulties surrounding information sharing could be minimized were we able to define what amount and kind of information would be required to make what improvement in infrastructure security. For example, would all that is required is to report on computer break-ins and the software penetration path, when known? Or must details of service failures be required, from which competitors could infer proprietary business information? These are the issues to be addressed in the planning of the proposed analysis center, which as suggested in the previous section on priorities, is probably not the first thing to be done anyway. Thus, a more effective way to begin implementation of the Commission's recommendations is to steer away from the information-sharing paradigm until some progress has been made in other areas and the minimal information needs are better defined.

Rights and Responsibilities for Investments in Security

The private infrastructure owner is likely to recognize that it is the corporation's responsibility to respond to hacker and criminal attacks. This means that security investments will be made in terms of their cost and benefit, and in the light of other investment requirements. It is becoming increasingly common to find organizations having a Chief Information Officer as a senior manager, especially where extensive use is made of information technology in the conduct of business. Tracking threats, losses, and available security technology is one of the responsibilities of the job, as is the planning for responses to disasters and other crises. Thus corporations are likely to have internal structures to assist in protecting the organization against such threats. In addition, internal audit organizations provide protection against fraud and theft.

Prior to the Commission's work, this was probably the extent of the corporation's threat horizon. As a result of the public discussion engendered by the Commission's Report, it is likely that many corporations have already expanded their thinking about the possible impact of information attacks and of the extent to which sovereign states rather than single individuals could be responsible for such attacks. To this extent, the Commission has initiated a process to achieve its purpose even if there should be no further organizational or program development. An ONIA, as well as other parts of the national security establishment, can continue to explore and explain the potential for such attacks. And the kinds of modeling and simulation capabilities the Commission proposes in its R&D program will also shed light on the magnitude and nature of potential threats.

In the normal course of market growth, information technology development, and capital investments by technology-intensive corporations, one can expect increasingly powerful security technology to be deployed, either in response to actual losses due to hackers and criminals, or simply because it becomes generally recognized as good business practice. Furthermore, the growth of electronic commerce will require improvements in the security of some infrastructure systems.

All this notwithstanding, will the resulting enhanced level of infrastructure protection be adequate to defend against future high-grade attacks? While it could, we need to consider the case where such an enhanced level of protection falls short and the nation's infrastructures become increasingly vulnerable to the threat of cyber attack. It will be the responsibility of the national security establishment to validate this state of affairs through the kinds of information sharing it proposes (although ONIA could usefully revisit some of the information-sharing issues identified previously).

The question then is how to handle the costs of adding infrastructure protection to private sector systems that are over and above those that can be justified in terms of the threats shown at the lower intensity end of the threat spectrum. A review of previous federal government efforts to shape civil actions for national security purposes noted, as one of its conclusions, that the government should be prepared to pay for some, if not most, of the costs.[39] A first step might be for system operators to prepare security plans and to submit them to the federal government for consideration. Funding could than be provided directly, through regulatory procedures, by means of tax incentives, or such other means as may be developed.

[39] Kenneth B. Malpass et al, *Workshop on Protecting and Assuring Critical National Infrastructure,* March 10-11, 1997, Stanford Center for International Security and Arms Control, presentation by David D. Elliott, pp. 17-21.

There are several advantages to this division of investment responsibility: no security funding is required until a high-level threat is validated by the federal government; the cost of the required protection of the public safety is spread broadly over society; and the details of security implementations are left in the hands of the private owners, subject only to review and approval by the federal government who is paying the bill. The administration of the security upgrade program can be put in the hands of the federal and/or state industry regulators. The federal government can call for any level of defense it deems prudent, but since it sees the cost of that defense and provides the funds, there are natural checks and balances operating. Involvement of state and federal regulators will assure that cost and quality of service issues are adequately addressed.

How Much New Organization Will be Required?

The intent of the above division of responsibilities is that organizations responsible for national-level infrastructure protection remain small until there is a validated threat, and that existing organizations handle the administration of the programs, augmented at the margin where necessary. The only completely new organization required at this time is the small NSC-based ONIA.

To the extent that information sharing can be effected, information from infrastructure systems will be available for use in one or more infrastructure analysis centers. Funding and staffing of such a center should be the sole responsibility of the federal government. The organizations responsible for dealing with private system operators in the matter of specifying information to be provided, its format, timeliness, and the like would be the sector coordinators, proposed here to be the NRIC and the NERC. The government staffs of the analysis center would undertake the primary collation and analysis function but data contributors would have access to their own data as well as to industry-average statistics.

There are several reasons for taking this minimal approach. The nation will want to feel its way until the magnitude of the international threat becomes clearer, while at the same time putting in place all the long-lead items such as an infrastructure protection policy and coordination office and necessary R&D. Beyond that, existing organizations are used rather than creating new organizations so that unnecessary overhead is avoided.

The sparse organizational structure will help it earn the respect of the industrial partners who are themselves under great pressure to reduce overhead and increase productivity and who will be turned-off by excessively large government bureaucracies. And, on the government’s side, it too must show that it is aware of the need to improve organizational productivity and efficiency.

The immediate tasks for the ONIA have been noted in the earlier discussion of priorities.

Implementation

Foundations and Management Principles

The preceding discussion has established some foundations on which to construct an implementation plan. The starting point is to have established *priorities*. From the earlier discussion on priorities, there are two infrastructures, those for communication and electric power, in a class by themselves in terms of the degree to which all other infrastructures are dependent upon them. It was noted that all the other infrastructure systems can be left to their own devices for the present. In the previous discussion ten tasks were listed in priority order. These priorities are used as a basis for the exemplar program below.

In addition, we must have some sense of how quickly we need to act, implying a model for threat intensity as a function of *time*. In the following, the Commission's conclusion that there is no imminence of a state-supported attack on the nation's infrastructure, has been adopted. This is not to diminish the Commission's broader assessment of the longer term risks to the nation's infrastructure, however.

Further, we need *organizational principles* to guide the construction of a plan. These are based on the earlier position that the nation will want to feel its way in these matters until the magnitude of the threat becomes clearer, while at the same time putting in place such long-lead items as an infrastructure protection policy and coordination office and necessary R&D. Beyond that, existing organizations are used rather than creating new organizations so that additional overhead is avoided.

There are four *management principles* that can provide guidance for planning the implementation of an infrastructure assurance program along the lines proposed by the Commission:

1. Implement a pay-as-you-go program rather than a front-loaded one. Spend some money and get something in return. Then spend some more and get more return. Stop increasing the program when you have achieved adequate return or you are no longer receiving value commensurate with what you are putting into it.

2. Consider ramp-up time when starting a new program. It is often the case that in the beginning there are fewer ideas worth funding, though the number of meritorious ideas increase as people have more time to consider the problem. Not only can excessive funding early on result in inefficient spending, but it can create a "lock-in" situation, where early funding commitments preclude supporting later and better ideas. In times of imminent national crisis, you tolerate such inefficiency, but when you have time it is worth using it to advantage.

3. Use leverage. This works several ways. In the case of existing government-funded programs, add money on a task basis to programs that are close to your interest and have a good track record. Usually program managers are interested in increasing the funding for "their" program and, in return, will help manage "your" program. Leveraging privately-funded programs can work through requiring matching funds. Finally, one can lay out a "plan" for what one needs from the private sector absent government funding and track progress, being prepared to consider the addition of government funding should progress be less rapid. Examples of this are to be found in "technology roadmaps" frequently created under the auspices of industry associations.

4. Assess the state of fundamental knowledge about the subject at hand before trying to buy specific results. In the present case, infrastructure systems are of a class referred to as "systems of systems." While we use the term a great deal, there is a dearth of fundamental understanding of systems of systems. The position is taken here that basic engineering concepts need to be developed if we are to understand the nonlinearities, chaotic behavior, and the possibility of cascading failures in systems of systems. Much of our present understanding of these issues is empirical and fragmented.

Proposed Implementation Plan

The following components of an implementation of the Commission's recommendations are outlined to suggest how an infrastructure protection program might evolve.

The time period addressed is 5–7 years, during which time the program is intended to achieve an asymptotic level. During that period it is expected that the information warfare threat will have become better understood on the basis of intelligence community threat assessments, industry vulnerability assessments, and empirical data on system reliability and trends, especially with respect to cyber attacks. At a decision point in year 3, the extension of the infrastructure protection program beyond the communication and electric power industries should be considered. The ONIA could be established for a finite period, at the end of which the administration would have the opportunity to decide the future of the program.

The organizational elements proposed by the Commission cover major functional areas of importance. Figure 1 shows the organizational relationships and how they might evolve over time.

1. ONIA

   The earlier discussion suggested a relatively small group. Locating it in a larger organization such as the NSC assumes that the host will provide the necessary support services. Keeping ONIA small will improve internal communication and will force it to establish priorities.

One should plan on increasing its staff in small increments the first several years to enable it to respond to increasing workload and responsibilities. The concept of operation of the ONIA has been addressed earlier in the section on recommended priority actions.

2. National Infrastructure Assurance Council

The NSTAC is, in effect, an industry advisory council for communications, although it may have to be rechartered or reorganized if it is to assume all of the infrastructure assurance functions recommended. If the electric power industry does not have a comparable organization that can be "borrowed" or merged, the NSTAC should be enlarged by adding electric power industry representatives (and, presumably, changing its name and charter.) Should the two industries find little in common to discuss, which one would hope would not be the case, the parent body could be divided into two industry subgroups. The NSTAC staff might have to be increased to accommodate its increased scope and responsibilities. This could be a good time to review the NSTAC performance to see if there are other changes that would improve its effectiveness. One might expect that it could have its tasking expanded and, at the same time, have its operation made more effective.

3. Sector Coordinators

For communications, this can be the FCC NRIC. Again, its operations should be reviewed to see how it might be improved and how, if necessary, it might be expanded to handle its increased responsibilities. Initially, any increase in staff to handle the infrastructure assurance task should be minimal, with later increases possible if warranted.

For electric power, the NERC can play this role. Since this is an industry organization, its staff size is not for the government to decide, but contracts for required support services could be entered into either with the NERC or with technical support organizations in the private sector.

4. Lead Agencies

The Commission Report identifies the Department of Defense and the Department of Commerce to be lead agencies for communications infrastructure assurance. DoD already has the National Communication System staff doing some of what is discussed here, albeit in a classified environment. It, or some other part of the extensive DoD C^3 structure should be able to take on the tasks required within existing staff. Add two more to the DoC office, presumably NTIA, delegated to handle that Department's part of the responsibility. While not identified by the Commission, the FCC also has an important role to play in the regulation of common carriers.

The Department of Energy is identified as the lead agency for the electric power industry. Plan on providing two staff positions for the new functions.

5. Support Office

In the program structure suggested here, there is no need to establish such a group. The ONIA will work through the lead agencies, the sector coordinator agencies, the agencies over which it has R&D funding oversight, and other existing government activities.

6. Analysis Center

Planning for this should take place in years 1–2 as the other organizational activities begin to function. The goal should be to have useful data flowing into an Analysis Center starting in year 3. For operating efficiency and to exploit technical and management commonalities, both communication and electric power infrastructure data should be accommodated in the same Center. Between the combined facilities of the Departments of Defense, Commerce, and Energy there should be organizations that could serve as a nucleus for a prototype Analysis Center. It would be most efficient to append the Analysis Center to an existing organization that can provide technical support. Its own information security requirements suggest that the Center be isolated from that of the host organization. As in all the other organizational steps, it is important that staff dedicated to the Analysis Center be small in size, at least in its first years.

Referring to Figure 1, an important activity of the ONIA will be to deal with the operators of the two infrastructures indicated, working through the sector coordinators and through the lead agencies and regulators shown as well. During the first two years, it should establish information reporting standards in anticipation of implementing an Analysis Center in year 3. Sometime after year 5, assuming that R&D on real-time network analysis tools has been successful, the Analysis Center would have its function enlarged by the implementation of an attack warning and attack assessment responsibility.

Two advisory functions are shown, one for R&D that can be centered in the NRC, and one for high-level policy advice from industry, what the Commission refers to as the National Infrastructure Assurance Council. The ONIA will work with the intelligence community to assure relevant information regarding threats, both to inform infrastructure operators as well as to modulate the pace of the national program as the community assessments develop.

The ONIA will interact with other government departments and agencies as required. This is represented in the figure by NIST and NSF, but the ONIA is likely to be in contact with a wide variety of government agencies in the discharge of its responsibilities.

Also shown in Figure 1 are three types of R&D organizations. As the Commission indicates, information security vendors will undertake market-driven product development on their own. Research organization, such as universities, national laboratories, and not-for-profits will undertake longer term research and analyses. Most important is the role of the system integrators. These are the commercial organizations that system operators rely on to adapt available security products and expertise to the analysis of their requirements and the incorporation of research results and vendor products into their systems.

Shown at the top of Figure 1 is the interface between public sector organizations and those in the private sector. The placement of R&D organizations is intended to suggest that vendors and system integrators are likely to work directly with system operators, as they do today, while the long term research organizations are more likely to find their funding in the public sector.

R&D Program and Related Issued

It will be important to establish a balanced R&D program, with funding provided for basic research in universities and not-for-profit organizations, as well as for pre-competitive technology development in vendor organizations providing software and security products and services. Federal laboratories will, of course, service the needs of government owned and operated infrastructure systems, but one can expect them to provide results of direct use to the private sector also.

Aside from the research results they will produce, funding universities is important because of the people they will train who are knowledgeable in cyber security and in complex systems, and in the general level of awareness in security they will engender in future generations of information scientists and system engineers. Hence at least a rough scoping of the issues must be a early deliverable of the recommended NRC activity if the FY 99 budget is to reflect the Commission's conclusions and recommendations. The extensive review of the literature undertaken by the Commission should help making a first cut at the various types of R&D required.

There are two ways to establish a level of R&D funding—top down and bottom up. The Commission has done top down planning and suggests that incremental money over the current $250M annual level in FY 98 be provided, starting in FY 99 and over the six year period FY 99–04, amounting to $250M, $350M, $450M, $550M. $650M, and $750M. For the reasons discussed earlier, this "jump-start" approach to R&D management is likely to be inefficient.

Apart from R&D funding, an important role of the federal government is to provide a market for security products developed by the private sector, much as it did for the development of jet engines, high performance computing, and computational fluid dynamics. In view of the size of the federal market and its awareness of the need for security, it can have an important influence on technology through emphasizing security in large system procurements.[40] The Commission calls for the identification of upcoming large federal procurements where system security requirements can be used to further the state of the art.

Another important role for the federal government is notably absent from the Commission's proposals, both in the R&D chapter[41] as well as in the chapter titled "Leading by Example."[42] This is to transfer to the private sector of its own extensive experience in information system protection. Despite imaginative motion pictures such as *War Games* and the like, government computers dedicated to war planning, intelligence, and nuclear weapon design have not, to our knowledge, been penetrated. It would appear reasonable that the techniques and lessons for protecting these systems be made available to private infrastructure system operators. Multilevel security, for example, has been extensively implemented in classified and compartmented federal systems. On the other hand, the security of federal government systems depends heavily on their isolation from public networks, on stringent personnel processes, including security clearances and background investigations, and often on the production and test of software in secure environments. Thus, while the case can be made that there are no "silver bullets" to transfer, use of this possible opportunity to enhance private system security should not be ignored.

To enhance the transfer of the results of this research to the private sector, and to get the greatest bang-for-the-buck, the following management guidelines are suggested:

- No more than 50% of the above incremental funding be spent in-house
- The R&D performed with this money be unclassified and in the public domain
- External R&D contracts with product vendors be cost-shared.

[40] The Report, pg. 75.

[41] The Report, pp. 89-91.

[42] The Report, pp. 73-77.

The research areas suggested by the Commission staff in its R&D (Ref.9) paper are reasonable as general guidance. However, in addition, there is some bottom-up R&D planning that should be undertaken. The following three suggestions are illustrative of the type of long term activity needed:

- Create 2–3 System Security Institutes to do basic research in systems and systems of systems. Fund them at a level of $1M, $2M, and $3M over the first three years. Keep the funding level constant but expect them to attract private sector support, with the intent of terminating public funding after six years. The Software Engineering Institute at Carnegie-Mellon University is a possible organizational model.

- Fund, through NSF, university programs in system science. Plan for something of the order of ten such programs each funded at a level of about $1M/year, with the assumption that matching funds from non-federal sources will be available.

- Fund a series of simulations, of both real systems and prototypes, to provide an experimental basis for investigating system robustness and security. Such funding should include support for system simulation facilities.

Funds for these last suggestions are included in the levels suggested above.

What Costs are Incurred and Who Pays Them?

In addition to showing organizational relationships, Figure 1 also identifies some of the cost elements involved.

There are three major cost areas of relevance to private sector participants. First, there is the cost of long term R&D. As the Commission suggests, the planning and monitoring of this can be done by the ONIA and the lead agencies, and can receive valuable input from academic and industrial organizations working through the NRC, which will require relatively modest amounts of public funding. The funding of the R&D itself will come from the lead agencies and, as appropriate, from other federal organizations.

Second, much of the funding for infrastructure system protection will involve private sector organizations, such as for product development by vendors, by investments of infrastructure system operators in their systems, and through the services they procure from system integrators. All this funding will be market-driven and will have little federal involvement, though it is expected that the results of publicly funded long term research will be transferred to the private sector through a variety of mechanisms. These include open publication of research results; movement of people between research, vendor, and integrator organizations; testbeds, proof-of-principle prototypes, system simulation activities; and the like. As noted earlier, the amount of investment that private system operators will undertake in defending their systems against attack is likely to stop short of what would be required to cope with high-grade attacks. In this case, the federal government will have to decide the degree to which it wants infrastructure protected at public expense and the degree of risk it is willing to assume.

The third major cost results from the new function identified by the Commission required to protect infrastructure against state-supported attack, the Analysis Center. It will involve a new kind of interaction between the public and private sectors, and is indicated at the top of Figure 1 as a “Joint Venture.” Its purpose is to receive information from infrastructure systems relevant to detecting and evaluating possible attacks. From the standpoint of the private system operators, the cost of providing such information is non-trivial. Establishing data formats, threshold criteria, timeliness requirements, common definitions, quality assurance, protection of proprietary interests, and other functions will result in costs to the system operators. In the case of the electric power infrastructure, additional costs for an increase in staffing will be incurred by the industry-supported NERC.

Assuming that the government will not want to mandate the imposition of these costs on competitive corporations, the question becomes why will a private operator participate? It is here that the "joint venture" label is most appropriate. The Analysis Center will have to operate as a business, delivering value to its "owners" commensurate with its costs. Thus, its operating costs will have to be minimized and its "products" will have to provide added value deriving from the pooling of industry information. In effect, the owners of the Analysis Center are also its customers, a situation experienced by industrial consortia generally. Thus, while in the earlier organizational discussion the explicit costs of the Analysis Center were assigned to the public sector, by far the larger costs are those in the private sector.

The above cost allocations and other divisions of responsibilities between the public and private sectors suggested throughout this paper can be summarized as follows:

Infrastructure operators pays costs related to:

- Protection against low grade attacks (of malicious insiders, outsiders, and criminals)
- Integrity of their own data
- Redundancy, backups, and other reconstitution measures
- Personnel screening and management
- Plans and implementation of defense against high-grade attacks jointly with the public sector

Vendors pay the cost of security product development.

Federal government pays the cost of:

- Prosecution of criminal acts
- Support of research in system security and associated infrastructure
- Protection against high-level threats
- International initiatives
- Support of educational initiatives
- Support for the development of risk assessment methodologies
- Assistance in vulnerability assessments, and vulnerability assessment training
- Providing the benefit of lessons learned from its own infrastructure protection[43]
- Assists in reconstitution after attack

Infrastructure operators and the federal government jointly:

- Support the analysis center
- Provide attack warning and attack assessment should network surveillance be feasible

[43] This is not actually proposed in the Report but it seems like the obvious thing to do. See also the previous discussion on pp. 9 and 23.

Leaving a Trail

Viewed as an intellectual concept, infrastructure is the system architect's nightmare come true. No one is "in charge." There are many people who can claim to "own" specific physical parts of a national infrastructure system. Others can claim jurisdiction over specific functional or geographical parts of infrastructure. Like fractals, the closer you look the more complicated it becomes.

Because of the peculiarly diverse and distributed nature of infrastructure systems, the Commission has probably assembled an unusual, and possibly unique, collection of information on the subject. Besides the technical, legal, historical, and management information, the Commission's files are likely to be a goldmine of who knows what about a myriad subjects. Databases have been created and others have been identified. What will happen to this material, whose value will grow as the nation attempts to address this difficult problem at hand? One is reminded of the closing scene of *The Raiders of the Lost Ark*, where the Covenant of the Ark, crated and stenciled, is slowly moved down the aisle of an endless government warehouse, to be again lost. One hopes that this is not to be the fate of what the Commission has assembled.

The Commission would be expected to pass its files on to the ONIA, if and when that organization is established. ONIA could decide to divest itself of this paper burden that could be more voluminous than its space will support and than its staff can use effectively. But the need for a national "corporate" memory will remain.

Furthermore, the material is likely to be quite useful to the engineers and scholars who will choose to work on this problem. One would hope that one of the things that will be done, with such funding as may be made available to pursue remedies to the problem of infrastructure protection, is that the Commission's collection will be transferred to an academic or not-for-profit setting, with funds to catalog and maintain it under the supervision of an information specialist. This would provide yet another easy way for the federal government to take an important step in the information sharing the Commission so fervently advocates.

The Global Context

The rugged individual, the isolated tribe, the self-sufficient nation are fading as social realities, to be replaced by a growing interdependence at all levels of human organization. Separateness was always difficult to sustain and what remains vanishes by the day. Replacing small clusters of human activity connected by links of limited capacity is an already vast but still growing web of globally integrated enterprises. Infrastructures provide the links between individuals and between their organizations. Progress in improving the human condition is made possible by the effectiveness of collective efforts enabled by these infrastructures.

The growing complexity of global infrastructures derives from sophisticated organizations combining hierarchy and distributed control. Powerful information technologies aid in the design, manufacture, and control of both the infrastructures and the activities they support. Because society finds itself, in some cases, operating near the limits of its ability to control these systems, it finds itself facing two difficulties. On the one hand, complex systems will behave in unexpected, unintended, and often disastrous ways. And on the other hand, to the extent that catastrophic consequences can be induced, society finds itself hostage to the systems on which it must depend. Should we fail to understand and control the behavior of these systems, we will by the same token limit the potential of human enterprise.

Thus, the issues with which the Commission has concerned itself, while initially having national security concerns as their basis, are far more general. At their focus is the robustness of the national and global economy. To the extent that the Commission's recommendations are implemented, they could have far more significance than simply providing enhanced security to the United States from a new "threat." They would provide an important opportunity for the nation to exercise global leadership in understanding and controlling the adverse consequences of the technologies on which we all rely.

Glossary

CGSR	Center for Global Security Research, Lawrence Livermore National Laboratories
CISAC	Center for International Security and Arms Control, Stanford University
CRADA	Cooperative Research and Development Agreement
DARPA	Defense Advanced Research Projects Agency
FCC	Federal Communications Commission
FERC	Federal Energy Regulatory Commission
GPS	Global Positioning Satellite
INFOSEC	Information Security
IW	Information Warfare
KMI	Key Management Infrastructure
MITI	Ministry of International Trade and Industry, Japan
NERC	North American Electric Reliability Council
NIST	National Institute for Standards and Technology
NRC	National Research Council
NRIC	Network Reliability and Interoperability Council, Federal Communications Commission
NSC	National Security Council
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications Information Administration
ONIA	Office of National Infrastructure Assurance
OSTP	Office of Science Technology Policy
PCCIP	President’s Commission on Critical Infrastructure Protection