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/

Workshop on Protecting and Assuring Critical National Infrastructure: Setting the Research and Policy Agenda

July 21-22, 1997

Kevin J. Soo Hoo
Kenneth B. Malpass
Kevin Harrington
David D. Elliott
Seymour E. Goodman

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

October 1997

Kevin J. Soo Hoo and Kenneth B. Malpass are Ph.D. candidates in the Department of Engineering–Economic Systems and Operations Research at Stanford University. Kevin Harrington is a Ph.D. candidate in the Department of Physics at Stanford University. David D. Elliott was Staff Director for Science and Technology at the National Security Council and then Vice President at SAIC and SRI. Seymour E. Goodman heads the Information Technology and International Security Program at CISAC and is Professor of Management Information Systems and Policy at the University of Arizona.

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.

Printed in the United States of America

ISBN 0-935371-48-6

Contents

Preface

In July 1996, President Clinton established the Commission on Critical Infrastructure Protection, 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 (telecommunications, electrical power systems, gas and oil storage and distribution, banking and finance, transportation, water supply systems, emergency services, and continuity of government), and also noted 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 critical infrastructures are owned or controlled by the government, and hence the government can, in principle, 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 adequate 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 National Security, and the Center for Global Security Research (CGSR) of the Lawrence Livermore National Laboratory (LLNL) are conducting workshops to examine many of the issues connected with the work of the Commission. In addition to the questions of vulnerabilities, threats, and possible remedies, we discuss the impact on the marketplace of possible protective actions, cost in terms of capital and functionality, legal constraints, 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. The edited summaries of the proceedings of this two-day meeting are presented in the following report.

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 July Workshop on Protecting and Assuring Critical National Infrastructure focused on three specific areas: international and legal issues relating to the control of network misuse and government roles for securing the infrastructure; economic factors, including market responses to the threat and to protection measures; and directions for future tools research in forensics, modeling, and simulation that will enhance understanding of system robustness, vulnerabilities, and security.

In addition to this agenda, the Workshop addressed the nature of public-private partnerships that could serve to coordinate the separate infrastructure protection efforts of each.

International and Legal Issues

While recognizing that efforts to address threats to infrastructure or to regulate its usage will require joint action by a number of jurisdictions, major limits exist on the degree to which coordinated international action can be achieved. This derives from the requirement that joint action will be feasible only when directed at shared infrastructure and only when it is mutually beneficial to the cooperating jurisdictions. Thus, while global communication, information, financial service, and international transportation are shared and thus presumably eligible for cooperative efforts, other infrastructures such as electric power generation and distribution, road and rail transport, water supply, and government and emergency services are less likely to be shared, even though threats to them may arise from outside national borders. Effective international action will also depend upon a common appreciation of the seriousness of the threat and the consequences of an attack.

In view of the international principle of sovereignty, pursuit of attackers will be further limited by the wide variations in criminal and civil statutes and in infrastructure ownership structures. Hence existing laws and international agreements are likely to require modification to accommodate the particular nature of cyber attacks on infrastructure. Ambiguous legal jurisdictions and conflicting institutional agendas will pose problems to be overcome.

These difficulties notwithstanding, the Workshop participants addressed international fora where joint action might be discussed and the process through which agreements could be achieved. These organizations include the International Telecommunication Union, the United Nations, the World Trade Organization, the Organization for Economic Cooperation and Development, the World International Property Organization, the G-7 Group, and Intelsat. The 1973 Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation was cited as a case where effective international cooperation was achieved to protect an infrastructure system.

While the process to achieve international agreement will be lengthy, it was noted that the threat is still in an embryonic stage and that time is presumably available to achieve the necessary consensus. It was also noted that unilateral U.S. declaratory policy on cyber security as well as U.S. initiatives leading to the sharing of information on threats and security measures could provide an important leadership element.

Beyond such steps to implement new protective measures to secure infrastructure systems, it was also noted that it is important to assess where current government policies are having the effect of weakening infrastructure systems and increasing their vulnerability to attack. Desisting in such policies is conceivably as important as undertaking new protective initiatives.

Economic Factors

The government should be very careful when intervening in the marketplace and should only do so if genuine market failures can be demonstrated. With respect to infrastructure protection two such market failures that appear to be occurring are a lack of information exchange and an underinvestment in security research and development. To deal with the first, the government should improve public awareness, encourage the use of computer emergency response teams and other information sharing mechanisms, establish training and certification programs, promote standard practices, facilitate the transfer of government technology to the private sector, and evaluate antitrust policies in light of private sector attempts to coordinate infrastructure protection efforts. The second potential failure may require direct government investment or some form of government subsidy. In these capacities, government may serve to accelerate the development of markets. The government may also have a role if certain activities, such as information gathering, analysis, dissemination, etc., involve significant economies of scale, or need a trusted intermediary.

Private insurance companies may have a role in improving infrastructure security, but their participation is currently hampered by a poor understanding of the risks, liabilities, and costs associated with infrastructure failure. If insurance is to play a role, then the market must be structured so as to avoid moral hazard, when the insured party’s incentive to reduce risk is too low, and adverse selection, when a biased pooling of risk occurs. One possible model for insurance may be similar to the Year 2000 insurance being offered by companies today in which insurance is extended only after a company has implemented certain protective measures and passed an independent certification program.

Further research is needed to characterize the private incentives for infrastructure protection, whether those incentives are sufficient to ensure the public good of infrastructure protection, and how infrastructure protection should therefore be funded. Another interesting area for future research is a careful examination of the incentives that both attacker and defender have to conduct and to protect against cyber attacks.

Tools

A premise of the Workshop was that research is needed on system security and the development of tools to assist system defenders. To this end a taxonomy of system relationships was proposed, ranging from the high-level interactions between infrastructure systems down to the interactions among subsystem components.

A taxonomy of required tools was also proposed, dealing with such fundamental assessment needs as the consequences of attacks, vulnerabilities of systems, nature of threats, assessment of risks, and identification of system interdependencies. An architecture-based methodology for the rigorous decomposition of systems was recommended as well.

A number of specific areas of R&D were identified, including a national repository for infrastructure analysis tools, models, and data; a testbed for the modeling and simulation of infrastructure systems; ways of protecting software from malicious code; the need to provide interoperability between security software; the establishment of facilities to assure the creation and distribution of trusted systems; digital signatures, smart card technology, and other ways of authenticating people and systems; and high quality commercial encryption of specified performance.

While there was substantial support for modeling and simulation to support the understanding of system vulnerabilities and the development of protective measures, there was some skepticism that adequate tools could be provided in a sufficiently timely manner to be useful.

Public-Private Partnership

The closing Roundtable at the Workshop provided an opportunity to explore ways public and private organizations might work together to address the protection of infrastructure systems. The starting point was a number of generally accepted public roles: the collection and distribution of information on real or presumed infrastructure attacks and on system protection measures; education of system operators and government decision-makers concerning the threat; measuring and assessing threats and tracking their evolution over time; R&D to compensate for market failure in infrastructure protection; assisting the development of standards, leaving primary responsibility to the private sector; assisting in the development of protection metrics, using government experience as a guide; protecting system operators against the possibility of monopoly suppliers of security products; defining what constitutes criminal attacks on infrastructure; development of enforcement regimes; and aiding in the establishment of international norms.

The participants at the Workshop suggested a number of areas where public initiatives would provide a welcome complement their own efforts. Joint efforts in the area of infrastructure architecture and the development of standards for system security have already been mentioned. These included the use of government procurements as a way of encouraging the adoption of standards; the requirement of security certification for systems related to government procurements; cooperation in establishing an “Underwriter Laboratory” for cryptography; chartering government-industry task forces such as the Infrastructure Protection Task Force, the National Security Telecommunications Advisory Committee, and the Modular Multifunction Information Transfer System Forum; and assistance with training and operating Red Teams to assess system vulnerabilities.

Purpose of the Workshop

David Elliott

The primary purposes of this series of workshops on critical infrastructure protection are to improve awareness, to create avenues of communication, and to be a focal point for analysis of this significant but embryonic national problem.

Through these workshops, the sponsors bring together people from organizations involved in information technology development, product business, network and data services, security analysis, and the community of critical infrastructure managers. The first workshop in March was a survey of many component issues. In particular, the role for modeling and simulation of infrastructure information systems was highlighted as a promising tool for understanding stressed network behavior, assessing risk, and testing proposed protective measures. Other ideas that emerged from the first workshop included the potential applicability of cost-benefit analysis, the global nature of the problem, the need for action, and the necessity of coordinated action between the government and the private sector.

The present workshop emphasized three areas for discussion in greater depth:

- International and legal questions relating to the control of network misuse and government authority for creating incentives and regulation to secure the infrastructure;
- Economic factors, including marketplace responses to the threat and to government protective measures;
- The availability of forensics, modeling, and simulation tools to improve understanding of system robustness, vulnerabilities, and security.

In addition, Bill Crowell, the deputy director of the National Security Agency, presented his insights into the likely direction of threats to the national information-based systems, and Fernand Sarrat offered his perspective as the Chief Executive Officer of Cylink, an important and rapidly growing Silicon Valley company with a focus on secure systems.

Assuring Critical Infrastructure

Robert T. Marsh

When President Clinton established the Commission last July, he appointed half of its members from involved departments and agencies in Washington and the other half from private sector infrastructure companies and organizations. The President identified eight infrastructures as critical because their incapacity or destruction would have a debilitating effect on our national and/or economic security. For just over a year now, the Commission has been working to identify and assess vulnerabilities and threats, and to develop a national policy to protect and assure these critical national infrastructures.

Critical infrastructures have long been lucrative targets for anyone wishing to do harm to a nation. This is not new. What is new and what, in part, motivated the President to create the Commission is that today these infrastructures may be attacked electronically. Because they all rely heavily on information and communications systems, they are vulnerable to other nations, which might mount an information warfare campaign; to terrorists, who might strike with a keyboard instead of a bomb; or to thieves, who might rob a bank from the comfort of home.

The Commission's first task was to characterize the eight infrastructures and to assess their vulnerabilities. Much of this research was conducted through an extensive outreach program, during which commissioners consulted with stakeholders around the country and met with more than 5,500 individuals, corporations, associations, and government agencies. They conducted simulations with Sandia National Labs and Booz-Allen & Hamilton, and created a database that is currently the most robust source of information on the critical infrastructures.

With the completion of these research efforts earlier this summer, the Commission has commenced the most important phase of its work:

- identifying fundamental issues that the Commission must address,
- deliberating options for how to answer those questions, and
- writing the final report with its recommendations to the President.

From the beginning, the Commission recognized the importance of full and open collaboration with the private sector and that the most significant challenge it faced was achieving private sector buy-in. Because most infrastructures are privately owned and operated, any solution that does not have private sector input and support will not be viable.

The Issues

The Commission first identified approximately 130 candidate issues,* and then proceeded to cull that list down to about 40 fundamental questions. For purposes of the current workshop, however, comments were restricted to the three focal subjects: Global and Economic Issues, Research and Development, Legal and Regulatory concerns.

Global and Economic Issues

As US companies depend increasingly upon the integrity of information and communications for their competitive position in the global marketplace, ensuring that integrity becomes a serious concern. The kinds of protection enjoyed under US laws and regulations may not be present in other nations. This issue looks at international mechanisms, such as bilateral or multilateral agreements, that might help address this concern. In addition, the Commission is looking at the effect of multinational companies upon US infrastructure. For example, given mergers such as that proposed by British Telecom and MCI, how can the security and availability of critical infrastructures be assured?

The second issue addresses whether market forces are sufficient to produce the necessary private sector investment in infrastructure protection. How can incentives be created to generate investment where required? Among the options under consideration are: loan guarantees, tax breaks and incentives, and grants.

Research and Development

This issue addresses the need for investment in new capabilities for protecting the information and communications infrastructure, for example, investments in technologies that detect and identify malicious code or that provide some form of global “caller ID.” The Commission is also exploring the appropriate roles of private and public investment in R&D. The range of options under consideration includes government encouragement of private sector R&D, direct government funding of R&D, and the use of the government procurements to spur R&D.

Legal and Regulatory

These issues address the need to modify existing legal and regulatory authorities as well as to introduce major new pieces of legislation. Currently, no coherent body of infrastructure law exists. Rather, bits and pieces of applicable law are scattered and decentralized.

The Commission has assembled a database of pertinent legal authorities from a broad range of sources. While not completely comprehensive, the database continues to evolve as deficiencies are identified and remedied. Furthermore, some existing regulatory measures or practices adversely affect the security of critical infrastructures. Once identified, the Commission will consider proposing options for remedial measures.

Criminal law has not kept pace with technology and, at present, may be insufficient to deter serious cyber crime. Traditional laws protecting infrastructures may be inadequate to the current threat and may even hamper the investigation of serious cyber crimes. The Commission may recommend legislation to address this concern.

* An issue being defined as an area where the Commission should be making a recommendation.

The legal and regulatory aspects of infrastructure protection raise a great many concerns, privacy and antitrust being two prominent ones. Privacy concerns stem from the inherent tension between individuals' desire to protect their privacy and organizational needs to protect their assets. For example, one state's privacy laws inhibit the screening of employees and prospective employees for sensitive positions. The Commission's recommendations may include model Federal and State legislation for dealing with privacy concerns. With respect to antitrust, some corporations have expressed concern that sharing protection and assurance information might violate US Antitrust Laws. Thus, the Commission is seeking an acceptable alternative that will enable information sharing.

The Commission is also examining ways in which the government can change its own infrastructure protection behavior. Ideally, the Commission would develop a model program that could serve as a prototype for private sector and state and local government efforts. Finally, the Commission is also exploring alternative approaches to traditional law enforcement such as the licensing of private cyber investigators.

Organizational Overview

Given that the federal government must take a number of initiatives in collaboration with the private sector to achieve critical infrastructure protection goals, how should it proceed, and what structures or organizations should it create to do those things? The Commission plans to synthesize the results of its functional analysis into a recommendation about an agency or other entity to perform the required functions. The organizational form could range from a new federal agency to a private-public corporation type of entity. The Commission's decision about organizational form will be guided by an abiding respect for private ownership and operation of the infrastructures and a recognition of national and economic security as the paramount concern.

Structure of the Report

The following is a preview of the Commission's report. Although it is grappling with many separate issues and functions, it intends to address each individually and to assemble them into an overall recommendation. At a minimum, however, those issues listed below will be addressed.

Formulating Policy. Based upon an assessment of the national risk and private sector perspectives, the Commission will propose national objectives and strategies in the form of legislation, regulations, budget requests, and enforcement measures. It will also assess existing regulations and propose ways to influence private sector participation and investments. The Commission will also address the international dimension and make recommendations for shaping the international environment.

Prevention and Mitigation. In response to education and standardization needs, the Commission will make recommendations targeted at promoting awareness and education; establishing assurance standards, certifications, and best practices; assessing the risk of system components; and improving risk analysis by transferring government information to the private sector. The Commission will also propose protection, mitigation, and research objectives, strategies, and funding. make recommendations for achieving and funding

Operational Warning (Information Sharing). The Commission recognizes the lack of understanding and information sharing between and among public and private sector actors. The Commission will make recommendations to facilitate information sharing so that both strategic and tactical warnings are disseminated, jurisdictional ambiguities (limitations of the NSA, FBI, CIA, etc.) are clarified, and all participants remain informed.

Counteraction and Incident Management. Counteractions are action that will deter, halt, or minimize an attack. The Commission will recommend plans for managing counteractions; integrating and managing law enforcement, intelligence, and military responses, and controlling misinformation.

Response and Recovery. The Commission will propose plans for responding to, recovering from, and managing the disruption of infrastructures.

Transitional Organization. The Commission will recommend an operational plan for implementing its recommendations. The plan may include measures such as redefining and extending the Commission, expanding the IPTF, creating a new office, or designating an existing agency to manage infrastructure protection.

International and Legal Issues of Infrastructure Protection: Is It a Small World After All?

Lawrence Greenberg

When the railroad was new, people undoubtedly said that it would make the world smaller. The same must also have been true for the steamboat, telegraph, automobile, telephone, and airplane. In some ways, all of those technologies did make the world smaller by enabling people to travel or to communicate across great distances. Before discussing the challenges presented by information technologies to the international system, we should examine some general commonalities and differences shared by the peoples of the world.

Commonalities and Differences

First, the world community shares infrastructures. Telecommunications and the Internet are particularly international in nature and permit people from many different countries to engage in commerce, communication, or other activities. Second, the international system of states defines the legal environment in which all countries act. Generally speaking, each state exerts exclusive jurisdiction within its territory, meaning states cannot cross into each others' territories to chase malefactors or to do anything else without permission. Although not necessarily inevitable, prohibitions against territorial trespassing appear to apply to electronic intrusions as well as physical ones. Third, states share some level of dependence upon these infrastructure systems and, presumably, some vulnerability as well.

These shared characteristics coupled with the spread of information technologies create certain challenges for the international system. Namely, malefactors, incompetence, or accidents in one country may cause damage far beyond its borders, and the faraway victims of that damage may be helpless to prevent, to mitigate, or to recover from the incident. For example, a mistake in Virginia may disrupt Internet service half a world away, as was the case on July 17, 1997, when an employee at Network Solutions, Inc. sent out incorrect network address files, causing the worst Internet outage in years.

Furthermore, individual government initiatives may be defeated by the actions of other states within their borders. This problem is most visible in the criminal law when states in pursuit of an electronic criminal require foreign cooperation, but cannot always obtain it.

The problem also applies to civil matters when one country's regulations cannot reach foreigners (who, in turn, may face incompatible regulations from their own governments), and yet those foreigners' actions may reach into that country's territory. The use of liability rules to influence foreigners' behavior may also work poorly where the foreigners are not subject to the jurisdiction of domestic courts.

Unshared characteristics also present challenges to efforts to secure critical infrastructures. The lack of universal recognition of the dangers to the infrastructure systems, especially of the cyberthreat; the fact that all nations do not share the same infrastructures; and the reality of different values, institutions, relevant actors, and perspectives make widespread agreement on infrastructure protection problematic.

Governmental Approaches to Infrastructure Protection

Government efforts to protect critical infrastructures may take four general forms, namely direct action, regulation, subsidies, and allocation of liability. For those governments outside the United States that do not view infrastructure protection (especially in cyberspace) as a significant concern, inaction may be the activity of choice. Governments, however, are not the only entities pursuing infrastructure assurance; market, technological, and societal forces will also affect the viability of infrastructure systems.

Historically, governments, which have asserted a near monopoly on the legitimate use of physical force, have defended physical infrastructures through direct action. For example, the cavalry defended the railroads from American Indians in the Wild West, the navy patrols the sea lanes, and the police pursue truck hijackers.

Rather than doing the work themselves, however, governments often prefer to tell others what to do and how to do it. Governmental regulation today touches all aspects of economic activity, including the construction and operation of critical infrastructures. Governments may set standards for safety, security, or merely the functioning of particular systems. The Federal Communications Commission allocates the frequencies that US broadcasters may use for their communications, for example, and Article 4A of the Uniform Commercial Code governs the daily electronic transfer of trillions of dollars of bank debt in the United States.

Governments may also encourage activities, in contrast to mandating them, by providing tax breaks, funds, or exemptions from regulation. For example, the US railroad companies were granted tracts of land along their routs, not only for rights of way, but also to support their development. Other potential forms of subsidy include the transfer of government-developed technology to the private sector and the government functioning as an insurer of last resort.

Concern over potential liability for damages resulting from accidents or malfunctions may influence the security measures taken by both infrastructure system operators and those who depend upon the infrastructures. Both legislatures and courts may allocate liability, and limiting liability may enable industry viability even when faced with the potential for horrendous, widespread losses from malfunctions or accidents. The allocation of liability for harms arising from system failures or accidents has been an important factor in the development of major US national infrastructures. During the 19th century, for example, US legal doctrine developed holding that the railroads were not liable for damages, such as fires, that they caused to properties along their tracks. Given the frequent, massive damage that the railroads caused, a contrary holding might have made the development of a private national railroad system impossible. Similarly, courts, legislatures, and public utility commissions have repeatedly limited the circumstances under which electric power companies may be liable for damages resulting from power outages, reasoning that broader exposure could crush the utilities.

Problems of the International System

One of the revolutionary features of telecommunications infrastructures, in particular, is the way in which they bring people together. Individuals can cheaply communicate with their counterparts in distant lands to conduct business, to obtain information, or to manipulate other computer systems. Networks may also enable individuals, groups, or states to inflict damage or to commit crimes against distant systems by willful action or by accidental system failures that spread from one country to another.

The long-standing international principle of state sovereignty, whereby each state's authority within its borders is absolute, hinders states' abilities to pursue and to act against attackers or malefactors who use the international networks as their gateways to other countries. Although the principles of sovereignty were conceived when international law contemplated only physical intrusions across national borders, governments would probably apply the principles to intrusions into computers, networks, or data banks. Thus, governments may be stymied by a conflict between physical properties and fundamental principles of international law, namely that electrons may flow through networks freely across international borders, but the authority of national government agents does not. Investigators will thus need foreign cooperation in their investigations, or they will need to operate covertly.

Historically, foreign agents have not been permitted to operate within another state's territory, without that state's permission. In the absence of international agreements, governments have no independent obligation to cooperate with one another. Diplomacy and inducements may be more important than legal argument, as foreign governments may be particularly skeptical of both US intentions and technical methods of investigation. This skepticism would likely complicate the tasks of US agents and diplomats, especially where they must determine whether a catastrophe resulted from an "accident" in a complicated system or from an attack.

Existing international law enforcement agreements may not be adequate to support an investigation. For example, treaties of mutual legal assistance, which institutionalize cooperation between countries' law enforcement agencies, generally contain exceptions that permit parties to refuse cooperation under certain circumstances; such as to protect "sovereignty, security, or similar essential interests." In the context of information systems attacks, where a country's national security interests, its technological development, the security of its financial and communications infrastructure, and the privacy of its citizens may be implicated, and where governments may not feel confident about their ability to monitor foreign (especially US) investigators' activities, some nations may not wish to cooperate. Furthermore, formal mechanisms of international cooperation, such as letters rogatory,* may be too slow to keep up with the speed of networked communications.

A state's efforts to gain custody of those who have attacked its systems from abroad are also complicated by the collision of the international state system, the international nature of networks, and the relative historical novelty of computers and networks. A country may

* A letters rogatory is a formal request for evidence from a foreign jurisdiction.

only obtain the apprehension and the delivery of an alleged criminal from a foreign country for trial under certain conditions. Most relevant, virtually all extradition treaties contain a "double criminality" requirement that mandates that an extradition request be based on an offense considered illegal under the laws of both the requesting country and the one to which the request is directed. This requirement has already hindered US efforts to try those who have intruded into sensitive US data systems. For example, when a young Argentine broke into several US Department of Defense computers, the United States could not obtain his extradition, even though Argentine police cooperated with US authorities, because Argentina had not classified such intrusions as criminal.

Those pursuing infrastructure assurance through liability allocation face similar problems. Obviously, liability rules may vary from country to country (or even within them). Furthermore, a court may be unable to obtain civil jurisdiction over the entity that an injured party may wish to hold liable, particularly as extradition does not apply to civil matters. However, if the goal of a liability rule is to hold an infrastructure system owner liable for damages resulting from that system's failure, the corporate owner of the infrastructure may have sufficient assets within or contacts with the forum country so that jurisdiction may be attainable, making liability rules effective.

Problems of Coordination

When international coordination is necessary for successful infrastructure protection policies, the number of actors involved may hinder that coordination. Virtually all countries are connected to such infrastructures as international telephone systems, the Internet, and systems coordinating international civil aviation or international financial transfers. Joint decision making can be difficult when many states must participate in decisions, many of whom may not see infrastructure protection as a problem or may have other reasons to be uncooperative.

The simplest area in which coordination may be necessary is in the development of standards, as for safety or system security. Standards work best when they are, indeed, standard. The predominant position of the United States and a few other nations in technology and business may reduce the number of states that participate in setting standards, but that number may still be significant.

The international system further complicates countries' efforts for domestic infrastructure protection because one country's policies may cripple their fellows', even unintentionally. For example, US export controls on cryptographic products may have hindered the spread of cryptography in the United States and, because US software companies dominate the international market, abroad. Governments (if there are any) who might hope to see cryptography widely used in their nations' private sectors, would find fewer cryptographic products available than they would have without US restrictions. Conversely, international cryptographic product development, combined with easy international transport of software over the Internet, may ultimately defeat restrictions on cryptography. Perhaps most significantly, various governments' restrictions on the import, export, or use of cryptography may make it harder for international standards to emerge.

Varying domestic priorities may also complicate international coordination. The uneven progress of privatization and deregulation in telecommunications, among other infrastructure-related sectors, means that countries will have varying mixes of public and private actors in their decision-making processes; where one country's PTT official may make a decision, another country may rely on executives at several companies to decide. Differing national concepts of freedom and privacy may also hinder coordinated efforts; countries' rules may differ on such matters as bank secrecy or the necessity to protect personal data. Significantly, many governments may be more concerned with regulating the content of communications than with protecting the communication networks themselves. Finally antitrust provisions, which may be enforced extraterritorially, and varying restrictions on foreign investment may create significant disincentives for private, coordinated initiatives.

International Approaches to Infrastructure Protection & Assurance

If international coordination or cooperation is desirable for infrastructure protection, an obvious potential solution is to create institutions or expand the roles of existing institutions to share information, to set policy, or even to respond to infrastructure attacks. Several candidate institutions already exist. The International Telecommunications Union (ITU) sets standards for telecommunications equipment and broadcasts, and coordinates national efforts to avoid broadcast interference. A significant characteristic of the ITU is that although its members are all states, various companies also participate in its discussions; the ITU may thus be a valuable place for governments and industry to pursue telecommunications infrastructure protection. Another institution, the International Civil Aviation Organization, has succeeded in coordinating national aviation policies to the extent that, with the exception of a few airlines, international aviation actually works. More broadly, Interpol promotes international criminal investigatory assistance and information sharing. Other existing forums where infrastructure security might be pursued include the UN, Intelsat, the World Trade Organization, the Organization for Economic Cooperation and Development (OECD) which has already issued guidelines for the security of information systems, the G-7, and even the World Intellectual Property Organization.

Through treaties or other agreements, international law can be changed to serve the needs of infrastructure assurance. An agreement that standardizes the criminality of computer intrusions, for purposes of investigation and extradition of perpetrators, may be particularly appropriate. The 1973 Montreal Convention on the Suppression of Unlawful Acts Against Civil Aviation, in which signatory nations agreed to recognize attacks against aircraft or air navigation facilities as illegal acts and to extradite or try suspected offenders, could provide a model for such an agreement. Such agreements could focus upon selected critical systems or upon computer or network attacks in general. These initiatives may only succeed, though, when broad international consensus and be established on the identity and gravity of the threat. During the 1970s and 1980s, for example, efforts to make terrorism a universal crime foundered on the rocks of ideological and definitional disputes.

Furthermore, incentives exist for countries to refuse membership in a regime against computer or network intrusions. First, some countries (including the US) may wish to preserve their abilities to use such intrusions or other attacks. Second, some nations may have ideological reasons to resist such rules, such as differing conceptions of privacy in electronic data, or distrust of any measures that appear to preserve the advantages of the developed nations. Finally, and perhaps most disturbingly, countries may choose not to criminalize certain conduct as part of a development strategy. Nations that hope to improve their knowledge base on information technologies may permit the behavior of hackers or other attackers in the hope that they will relocate to these nations.

Such “regulatory arbitrage” may actually occur. First, countries have already sought individuals or groups of foreign hackers to engage in espionage. During the 1980s, for example, the Soviet Union employed a group of German computer hackers to obtain US and NATO defense secrets. Second, “regulatory arbitrage” has taken place in other contexts. For example, the Seychelles, hoping to attract foreign (including criminal) capital, enacted an Economic Development Act that granted citizenship and immunity from asset forfeiture or extradition to anyone investing at least $10 million in the islands. Less sinisterly, perhaps, countries, states, and municipalities routinely compete to provide regulatory relief and tax incentives to attract business.

Market forces and technological development will undoubtedly contribute to the solution of various infrastructure assurance problems. Companies may compete on the basis of security or system assurance. CompuServe attempted to capitalize on America Online’s troubles last winter; and, according to news reports, shortly after one London bank was reportedly the victim of serious computer-aided theft, rivals contacted its clients to inform them that their security was much better. Furthermore competing private sector investments in infrastructures, such as the several undersea cable and satellite communications systems, contribute to redundancy and thus to robustness of the overall communications infrastructure.

Significantly, many companies today are international institutions and may promote coordination of government policies, as well as private arrangements; when Bill Gates speaks, China apparently listens, a claim that Bill Clinton might envy. Significantly, the US government now appears inclined to let the private sector set standards for global Internet commerce, and the non-governmental Internet Engineering Task Force (IETF) has had marked success in developing standards for the use and functioning of the Internet.

Questions for Discussion

Who should be responsible for protecting and assuring critical infrastructures? What are the appropriate roles for national governments and their agents (regulators, law enforcement, and national security officials), international governmental entities, non-governmental organizations, individual infrastructure owners, and those who use or depend upon infrastructures? What are the legal bases for specific policy initiatives?

Under what circumstances will international efforts for protection of infrastructures be necessary? How can the United States gain international support for such efforts in the absence of global appreciation of a cyberspace-based threat to infrastructures? How can a global appreciation of the issues be achieved? Can widespread apparent concern with cyberspace-based threats to electronic commerce serve as a useful proxy for concern over infrastructure vulnerabilities in general?

How should governments and individuals pursue those who have attacked them across international borders? How should the United States approach conflicts or inconsistencies among nations, standards, laws, concepts of rights, and policy goals relating to infrastructures?

Three important issues should inform any discussion of international and legal issues relating to infrastructure protection and assurance. First, the political dimension cannot be ignored. Convincing arguments must be constructed to illustrate the problems and to justify the implementation of any solutions. The US people, perhaps even some in attendance at the workshop, as well as foreign peoples and governments are not entirely convinced that serious measures are required. Second, institutional context and capabilities should be considered as solutions are crafted. Specifically, the legal basis for potential actions must be established, especially where governments with varying institutional capabilities are concerned. Third, the underlying values that motivate the solutions should not be forgotten. Protecting critical infrastructures is important because of the activities that they support, including, in this country, the functioning of a relatively free and open society. Other countries may have different priorities and motives. In the trade-offs that accompany any negotiation, foreign or domestic, US negotiators must recognize and respect differing values and agendas, but should not lose sight of their own.

International and Legal Working Group Report

The working group discussed a number of strategies for approaching infrastructure protection, including possible legal changes and avenues for international cooperation. The field has global implications for targets of attack, computer system vulnerabilities, and the location of attackers. However, all aspects of infrastructure protection may not require international responses, and existing international tools and mechanisms may be inappropriate for protection against cyber attacks.

Evaluation of Threats

While many infrastructures may, in theory, be subject to cyber attack from any point on the globe, in some areas the extent of cross-border infrastructure interdependence is limited. Thus, the need for an international response may be limited to those fields where cooperation is essential, such as information sharing, telecommunications, and selected cross-border utilities. Special cases might include provisions for national defense espionage and concerted efforts to combat terrorist organizations. Further work is needed to classify other specific threats that may require a coordinated response.

Internationally, the matters of infrastructure protection and cyber threats to infrastructure are not even on the agenda of most countries. The United States has the biggest problem, and thus the biggest concern, because it has the most computers, Internet nodes, etc., but the majority of countries have a very limited infrastructure and hence little interest in the problem. Thus, the international threats are still quite embryonic and developing. The United States' current position is not one in which it must implement desperation measures, but rather it is at a stage where it can plan out in some sensible way over a period 5-10 years, a strategy for securing the infrastructure.

National Security, Law Enforcement, and Private Responsibilities

Divergent viewpoints emerged on the proper roles for national security institutions, law enforcement agencies, and private organizations. To the extent that attacks are visited upon private concerns and their customers, private funds should arguably be committed to defend against attacks. To the extent that law enforcement organizations have limited resources and few technically sophisticated personnel, the efficacy of pursuing attackers across borders is questionable. With respect to national security resources, an unresolved conflict remains between defending infrastructure and expanding military capabilities in offensive information warfare.

Resource allocation issues aside, coordinated efforts between the various entities are often complicated by ambiguous legal jurisdiction and conflicting institutional agendas. Unfortunately, the highly technical and rapidly changing nature of computer crime make, a timely, coordinated legislative response highly unlikely. In the interim, however, private institutions could be formed to share information about attacks and to educate legislators about the problem.

International Concerns and Responses

Although the danger exists that some nations might recruit cyber criminals as a means of economic development (similar to the way in which the Seychelles are allegedly encouraging wealthy renegades to move there to avoid extradition), no hard evidence has emerged that such a phenomenon is occurring. A model code of computer crime laws and international condemnation of certain actions were suggested, but no consensus emerged on how either could be accomplished.

The issue of privacy is fundamental to any discussion of cyber defenses. It arises in both the monitoring of attacks, through wiretapping or similar measures, and the disclosing of proprietary information about technologies, vulnerabilities, and losses. Because certain European countries protect the right to privacy more broadly than the United States, implementing a common defense based on mandatory disclosures of information or on required precautions to be taken by firms may be problematic.

International Initiatives

Although some measures will require international initiatives or may be just much more likely to succeed with international initiative, the multiplicity of nations’ motives and agendas for governing the information infrastructure would seem to encourage strictly domestic defensive solutions. This perspective, however, ignores Sun Tzu’s admonition that a passive defense is a futile position. Thus, despite the difficulties, international agreements that would enable the United States to strike back in some way at attackers, either directly or through law enforcement mechanisms, will likely be of critical importance to securing the infrastructures.

The process by which an agreement of this nature is struck will probably be somewhat more involved than a simple round of negotiations. For example, if some sort of consensus developed among the G7 to start with a particular measure, it might, after a couple of years, issue a communiqué. In the ensuing years, the governments of other nations would have to be persuaded that the measure has merit and warrants a UN General Assembly resolution, calling for a convention. Once the resolution is enacted, a conference is held to create the convention which, in turn, must be accepted by the international community to enter into force.

Technology and Policy

Trusted systems, including encryption, certificates, authentication, etc., can provide greater assurance of protection than after-the-fact prosecution. The present controversy over NSA's key recovery proposal aside, government should encourage efforts to implement protective measures like trusted systems to safeguard the information infrastructure. Policy should, of course, be flexible so that it can adapt to the rapidly changing technological landscape and the dynamics of the international marketplace.

Redundancy and competitive loading of utilities is an important area for research and policy coordination. Just as multiple undersea cables and satellite systems provide many paths for communication, similar redundancies may be possible for the delivery of electricity, fuel, and other essentials to improve infrastructure robustness.

Independent verification is another strategy for building confidence in both hardware and software products. Vulnerabilities inherent in a product or virus-infected upgrades need to be detected and remedied before the product is distributed. Verification is also needed on a system level for similar reasons. For example, confidence in the international telecommunications system could be bolstered by rigorous red-team testing of failure modes and potential attack propagation methods.

The group briefly discussed other actions that might lead to improved infrastructure protections, including the possibility of postmarking packets on the internet, the subsidization of security features in US software products, and a US declaratory policy on cybersecurity; but information sharing emerged as one of the clearest first steps for improving security. For example, if the banking regulators in one country have evidence of attacks of a certain nature, they should be able to sound an alarm and share that information with other banks and officials. Unfortunately, institutions' inability to identify and share their information with others remains a pervasive problem. Governmental authorities might lead by example with stronger protective measures for governmental systems and with new rules for identifying information to be shared and partners with whom to share it.

Further Research

International awareness of and commitment to respond to the problem should be gauged on a country by country basis. Successful programs in each country should be identified, and the essential features shared with the international community. A list of privacy and database protection laws and regulations should be compiled, and anti-trust barriers to information sharing, coordinated research in secure systems, and forensic tools development should be reviewed.

Specific definitions are needed for terms such as computer crime and act of war for cyber attacks. A concept of civil liability for cyber attacks across borders should be developed, and a lowest common denominator for sharing information and resources should be determined.

Technical research should be sponsored to investigate the relationship between standards and diversity of systems, the best way to test end-to-end security for international networks, and statistical categories and data capture techniques to better understand the problem. Organizational research in personnel training, communication of attacks, and interagency coordination is also needed. Methods are needed to facilitate information disclosure from reluctant industries and to assure information accuracy.

Better explanations of information infrastructure security problems are needed to give the field higher priority in both public and private sectors. Export control policy for cryptographic products should be evaluated in light global marketplace realities, enforcement feasibility, and societal impact. Mechanisms, such as research grants, should be established to transfer technology from the public sector to the private sector.

Economic Aspects of Infrastructure Security

Hal Varian

The government should promote public awareness, enhance exchange of information, strengthen education and training, and promote development of secure technology. It needs to resolve the critical issue of how improved infrastructure security will be funded and to do so bearing in mind the fact that participants in a competitive industry will resist additional costs even if those costs are uniformly applied.

Nature of the Threat

In some sense computers are inherently more secure today than before, but the consequences of a system breach are also significantly greater. For example, computers enable banks to verify transactions fairly quickly and easily. In the previous workshop, however, a banker noted that banks may not verify a transaction as low as $50, reserving verification for larger sums. Once criminals discover this threshold, they will adapt their transactions to fall below the threshold and, with computers, will be able to make multiple "micro-transactions" instead. Thus, a $500,000 transaction, which would certainly trigger verification, might be executed with 10,000 transactions of $50 and thus avoid verification. The modern defense against this sort of countermeasure is profiling, where customers' behaviors are statistically modeled and suspicious behavior is investigated. Both the credit-card and the cellular phone industries have instituted very sophisticated profiling systems.

When examining most cases of computer crime, one finds that they are typically accomplished using very mundane means. A prime example is Kevin Mitnick, who achieved many of his exploits through "social engineering," tricking unsuspecting employees into surrendering their passwords or searching through company dumpsters for pages of passwords and other useful materials. Even the most secure technology is breachable if proper procedures are not in place to support that technology.

When Disaster Strikes

In case of an emergency, what mechanisms exist to allocate scarce bandwidth and power? At present, no good method exists for the Internet. For purposes of general data transmission, the Internet treats all data with the same priority, regardless of the source.* Although it may be coming in the future, priority service does not yet exist.

Who will be blamed when a disaster occurs? Will people blame private firms or government agencies? Whoever will be pilloried has an incentive today to take steps to prevent these disasters from ever occurring. The Commission's work is extremely important because it will essentially present a blue-print for comprehensive action before a serious disaster takes place. People tend to underestimate the probability of rare events, and, once something happens they overestimate the probability that it will happen again. In the event support cannot be generated to implement the plan before an infrastructure disaster occurs, broad support will certainly materialize after one has occurred.

Role for Insurance

Will private insurance providers be willing to cover major infrastructure-related disasters? The risks, the liabilities, and the costs are extremely difficult to measure. In addition, the destruction of physical capital, which prevents transactions from taking place, is qualitatively different from a delaying of transactions. The snow storms in Washington, DC, are a beautiful illustration of this point. The cost of a storm shutting down the nation's capital for day could be very large if the transactions that would have ordinarily taken place never do, but indeed the transactions do take place, albeit delayed by some number of hours or days. Thus, the real social cost of that kind of disaster is relatively small. Caps on damage disbursements should be considered quite carefully before encouraged as a means to limit insurer liability.

Careful consideration of how insurance is structured will be required to avoid two pitfalls associated with insurance. The first is "moral hazard," in which too much insurance is given, reducing the insured party's incentive to reduce risk. For example, a standard insurance policy typically carries a deductible so that the insured individual bears some cost in case a bad event happens. In this way, the deductible creates an incentive for the individual to take steps to avoid bad events. Ideally, risk should be allocated to those who are who are in the best position to reduce it. The second pitfall is adverse selection, which is the property that those who need the insurance are the ones who buy it, and those who do not need it do not buy it. The result is a biased pooling of risk in which people who actually have a higher probability than average of incurring damage are the only ones in the pool. This effect can occur when the cost of insurance is prohibitively high, so that people who are most in need of insurance are the only ones who purchase it and people who have lesser needs are crowded out. In the end the market is destroyed.

In the absence of a private market for infrastructure-damage insurance, perhaps mandatory insurance should be considered. Like unemployment and to some extent health insurance, infrastructure-damage insurance might be in the same category.

Another possibility for risk management may take the form of an insurance company guarantee. For example, a company or individual hires an insurance company that has had

* Network control information does receive a form of priority treatment on the Internet and is the only exception to the rule.

extensive experience with infrastructure-related risks, and an incentive contract is established where the insurance company pays if damage occurs, but only if certain prescribed measures have been followed. Thus, if the insurer does not provide the right advice to
manage the risk, then it will have to pay when something goes wrong. Like the Chinesedoctors who are only paid when the customer is well, the insurance company is paid for keeping its clients well. An example of this kind of insurance exists today with companies offering insurance against Year 2000 disasters. These companies have a certification program at ITAA (Information Technology Association of America) that monitors the Year 2000 defenses implemented by client corporations. The program certifies them as having done an adequate job, and the insurance company insures them after they pass the certification test.

Computer Security Education

Where do security experts come from? The field of computer security is essentially in apprentice mode. Very few universities offer classes or degrees in computer security. When attempting to construct a formal education program in computer security, two issues immediately surface: the issues of certification and of continuing education. Computer security is a field that does not stand still, so certification should be renewable. Ethical and professional standards need to be articulated and established so that the profession can develop and work effectively. Even programs that do provide training in the technologies essential for computer security (cryptography is a simple example) often omit the critically important social engineering side, which continues to comprises a significant part of the risk.

Social Incentives

Although they may have many good effects, deregulation and the accompanying decentralization of infrastructures have probably hindered rather than helped security. The infrastructure is, by virtue of its shared nature, a public good, thus its provision presents the same financing problems that the provision of other public goods presents.

Public goods are typically financed in one of three ways. The first is taxation. The second, somewhat less well-known, is to subsidize investment through credits like the R & D tax credit. A general principle in economics states that subsidies are better than grants for encouraging an activity because grants will crowd out individual activities while subsidies will encourage incremental investment in that activity.

The third method for public good finance involves tying it in with the provision of a complementary private good. For example, lighthouses in England were financed by imposing a port fee for docking at the ports. Looking at private technology, like security-related chips or components, a user tax could be built into them so that the tax could then be used to subsidize infrastructure investments in the public good. The only danger with this classic tried-and-true method is the possibility of some other source entering the market and supplying the same functionality but evading the tax used to support the public investment.

Role of Government

The government certainly has a role in public safety and law enforcement, but it also has a role as purchaser and standard setter. The fact that the most recent version of the Department of Defense Orange Book, which details standards for computer security equipment, is dated December 1985 indicates that the government is not exercising its influence in areas where it can and should.

Two trends are at odds with efforts to set standards. The first deals with closed security systems. Unlike open systems which make their techniques and strategies open to public and scientific scrutiny, closed security models are kept secret. The risk, of course, is that someone will break through the secrecy, discover the algorithms, and find a weakness. Mondex learned the dangers of closed security models when a foreign national demonstrated at a recent meeting how to take $20 worth of chemicals from any pharmacy, dissolve the protective layer of the Mondex smart card, expose all of the circuitry, and deduce the logic of the algorithm.

The other trend derives from the idea that greater diversity reduces overall vulnerability. As an illustration, if Windows-NT is the sole operating system running every server in the US and a hacker finds a security hole in it, then every US server is vulnerable to this particular attack. If, however, there are several operating systems in use, then the danger that a single Windows-NT security hole presents to the US will be significantly less.

Keeping a Secret

The current encryption policy is based on the idea of taxing strong cryptography; that is, preventing strong cryptography from doing certain things by preventing its export. An alternative policy worthy of consideration is one that subsidizes weak cryptography. For example, if the government had a particular chip or technology that performed encryption using weak cryptography and gave it away, sold for pennies, or somehow subsidized it, then one would expect to see many people using it. Admittedly, the Iraqis would unlikely use it, but people like Timothy McVeigh might. Of course, the government could adopt a combination of the two strategies, taxing strong cryptography while subsidize weak cryptography. By adjusting the tax and subsidies revenues could be raised to fund infrastructure protection.

Q & A Session

In some ways, a system of two cryptographic classifications might be beneficial to law enforcement. The fact that a person or organization is using strong encryption might arouse the suspicion and precipitate closer scrutiny from law enforcement.

Economics Working Group Report

Strong agreement was reached in the working group that the government should be careful about intervening in the marketplace. The free market is the most efficient decentralized form of organizing economic activity that is known. Recommendations that the government intervene should be made only if convincing evidence of a genuine “market failure” can be found, that is, only if a non-market alternative can clearly result in superior outcomes. Thus, a central question that the working group faced was, “What can be done to make markets provide better security/protection measures for the nation’s infrastructure?”

An important distinction should be made between the provision of private security and public security. Private security is instituted when the consequences of an attack are borne mostly by the attacked system, while public security is needed when the consequences will be suffered by others as well. In economist’s jargon, the distinction is whether or not the attack generates externalities or spill-overs. If it generates no externalities, it is a purely private attack.

Private Security

In the case of private attacks, many suggestions were made help cure the classic market failure of information inadequacies and deficiencies. The general sentiment was that the private sector is woefully ignorant of the dangers posed by inadequate security and of how to obtain the information and the skilled personnel needed to improve security. Some suggestions to solve this problem include:

Improve public awareness. This task is more difficult than it may, at first, appear. The news media generally slights tutorials. Instead, as a large academic literature shows, the news media tend to focus on “newsworthy” events, or events that are unusual and have dramatic consequences. The literature also shows that before such an event the public will tend to greatly underestimate its probability of occurring and after the event it will tend to overestimate its probability of recurring. Thus, policy must contend with both a public’s underreaction and its potential overreaction to large scale security failures.

Use CERT. Computer Emergency Response Teams (CERT) and other similar organizations serve as important foci for the pooling knowledge on security flaws and solutions.

Encourage standard practices. The development of standard practices (for example, companies implementing security patches posted on CERT within 6 months of their posting) would raise awareness and could improve general computer security practices. The standards could be propagated initially with governmental procurement contracts. In the long run, this sort of risk management is a natural role for the insurance industry. However, many believe that the insurance industry will be unwilling to assume this role until catastrophic events demonstrate the market for it.

Encourage information sharing. Following the example of NSTAC, industry-government advisory committees could be established to guide policy.

Encourage technology transfer. Relevant government technologies, such as security tools and modeling and simulation tools, developed by NSA and DoD should be shared with the private sector.

Evaluate antitrust policies . Antitrust policies may be unnecessarily hindering industry cooperation on security issues. Clearly, these policies should be reconsidered.

Encourage the training and certification . Security experts should be trained and certified. The government could initiate this process via military training programs, government procurement, government sponsorships of conferences, stimulation of the formation of special interest groups on security in professional organizations, and other routes. The market will eventually take care of the lack of security experts. In a matter of time computer science and management information systems departments, as well as the military, will routinely train security experts. The government has a valuable role to play in drastically shortening that "matter of time;" otherwise, as with the insurance example mentioned above, a catastrophic event may be required to precipitate a market response.

R&D Market Failure

An important market failure different from information inadequacies and deficiencies has to do with research and development. Pure knowledge is an example of the limiting form of an externality–one that affects everyone. Such a good is a called a public good and is characterized by the fact that it is non-excludable (people cannot be excluded from enjoying it) and non-depletable (one person's consumption of it does not diminish the amount available). To illustrate the point, if someone publishes knowledge, like a mathematical theorem, then other people cannot be kept from benefiting from it. Unfortunately, this consequence creates a disincentive to produce and publish knowledge because the producer cannot be adequately reimbursed for costs. Thus, everyone has an incentive to be a free rider.

The classic solution to the free rider problem in the production of R&D is to have the government do it or pay for it. R&D on secure technology is no exception and may provide an important role for government.

Public Security

At the outset, the group noted that private security is complementary with public security. If individual organizations have secure systems, then the public security problem is dramatically easier. Consequently, the first and most basic step in dealing with public security is to make sure that the markets for private security arrangements work effectively.

Even though the incentives may be right for private security provision, the possibility exists that the most cost-effective way of providing private security is via collective action. This collective action could be private–for example, industry organizations, or it could be public–public law enforcement officers who specialize in security issues.

Operations that involve significant economies of scale may require government action, such as, information gathering, analysis, dissemination, monitoring, profiling and snooping. Government may be also be required to place constraints on the sorts of investigative techniques that private agents can use or assume the investigative duties itself.

The government needs to make clear statements about what constitutes illegal actions, acts of war, and appropriate retaliations in the realm of computer intrusions. It should also establish effective plans for disaster recovery, including prioritization of operational infrastructure, coordination of responses, etc.

To the extent that security requirements above and beyond those instituted by the private sector are needed, government procurement policy may be needed to pay for them. For example, if these additional costs are primarily fixed costs (independent of the scale of operation) such as R&D costs, the familiar free rider problem may demand the classic solution of government funding. If, on the other hand, these additional costs are variable costs (dependent upon the number of units) then subsidies or mandated use may be necessary.

Research Agenda

No one has a clear idea about what is happening now with respect to computerized attacks, and individual firms do not have good incentives to disclose attack data. Mandatory disclosure to government agencies, along with promises of anonymity, may be appropriate to alleviate this information deficiency. This could be done first in a regulated sector, such as banking, to see how well the policy works.

A fundamental understanding of the types of attacks and the costs that each imposes is needed to prioritize investment in deterrence. Thus, simulation, profiling, and red teams are all potentially useful tools. In this regard, economics is relevant both to the attacker’s decisions as well as to the defender’s. The ability to do $10 million worth of damage via cyber attacks at a cost of $100 thousand is not very attractive to terrorists who can already do $20 million dollars damage with a $50 thousand conventional attack. Attacks must be generally cost effective from the attacker’s point of view.

Furthermore, incentives of the players must be understood and carefully modeled. For example, criminal penalties for low-level destructive cyber attacks decrease incentives for individuals and firms to self-protect. This may, in turn, make them more vulnerable to high-level attacks for which legal protection may be irrelevant. The benefits of decriminalizing low-level attacks may exceed the costs. All of this suggests interesting and important research problems in the design of optimum deterrence.

Tools for 21st Century Infrastructure Protection

Stan Trost

The entire critical infrastructure is a complex, interdependent system of subsystems. The DoD has already developed an extensive methodology and set of tools for dealing with complex systems of systems. The current challenge is to draw upon, to improve, and to develop new tools for application to the nation's critical infrastructure.

A number of approaches for improving the critical infrastructure are currently under consideration; the purpose of this section is to examine the requirements for new and improved tools. Actual research emphases will depend upon prioritization of infrastructure areas, architectural decomposition, and consequence analysis.

System and Data Architecture

Understanding the nation's critical infrastructure requires a knowledge of the system architecture and the data flows. Despite the many interdependencies, a rigorous decomposition might help identify critical dependencies. Unfortunately, such a decomposition is complicated by the infrastructure's dynamic nature and the unplanned, evolutionary method by which infrastructure formed.

An adaptable system architecture must be developed and should support a common language to enable research, operational, legal, and other communities to communicate more effectively. A method of identifying critical nodes, links, and dependencies is also required. Further, a set of standards will be required to understand data flows, communications, interfaces, and models. Although a challenging task, architecture development will simplify and standardize many other research tasks.

Tools Research Strategy

Assuming improved component and subsystem level tools are at present and will continue to be under development, the focus of new tools research should be on high-payoff technical and policy tools that will help strengthen the critical infrastructure. In all likelihood, the process described below will require full automation, constituting yet another significant research challenge.

Consequences: Beginning with the eight critical infrastructures, determine the failure scenarios with the greatest consequences and rank them in order of severity.

Vulnerability: Characterize the nature of vulnerabilities exploited in scenarios with the highest consequence severity rank, and determine the avenues of attack.

Threats: Identify the threats that can attack the vulnerabilities. Analyze the threats to determine whether their origin is a natural hazard or human induced; what their underlying causes or motivations might be; and how likely or credible the scenarios are.

Risks: Formal risk assessment methods should be used to evaluate the threats, the vulnerabilities, and the consequences to inform research efforts.

This analysis moves from consequences to vulnerabilities to threats. A complementary analysis should also be performed, starting with threats and credibility and moving to vulnerabilities and consequences.

Suggestions for Tools Research

A set of advanced, automated systems analysis tools are needed to understand vulnerabilities, risks, and consequences of a failure at the component, subsystem, or system level. Specific research questions include: to what level of detail can an automated mapping process build a high fidelity network model, if at all, and how can the specific configuration or operating condition of a subelement be automatically determined.

Security Tools

Computer communications systems are relatively immature when compared to other infrastructures. Furthermore, the complexities of software and the difficulty of validating software and hardware combinations imply an increased need for many kinds of computer security tools. Examples of needed research include more robust authentication, intrusion denial and/or detection, and forensics. Research agendas for advanced security tools are being developed in a number of forums, such as DARPA’s “Research for Critical Infrastructure Assurance” workshop, held on July 9-11, 1997, at which Indications and Warning; Intrusion Detection; and Probes, Monitors, Sensors were the major research themes.

Computer security experts suggest that the most important steps in securing systems from attack involve having appropriate authentication mechanisms that are coupled with authorization tools. Most current systems have rather weak security with the system authenticating via user-supplied passwords. Many advanced mechanisms have been developed to strengthen these password schemes (e.g., Kerberos), but they are not in routine use.

Strong authentication must come into common use, with a biometric likely forming the basis of the technology. Research is also needed in hierarchical authentication, or system certification for tiered, interconnected systems. Accompanying authentication tool research will be research in stronger forms of authorization, especially methods to authorize over multiple networks.

Separately, techniques must be developed to improve software reliability and to minimize the number of security holes. Intelligent, adaptive, protective tools need to be developed, including “smart firewalls” for adaptive and flexible network security management and intelligent software agents for detecting and tracking unauthorized intruders and security holes. Certification procedures should be developed, and synchronization of software releases should keep software security up-to-date.

Finally, research is needed on tools for intrusion detection, indications and warnings, and forensics in case of attack. Current indications and warning systems recognize known attack patterns, but they must be adapted to keep abreast of the rapid changes in attack patterns and techniques. Forensics tools are an essential element in understanding patterns and assessing future trends. Research is needed to automate these tools so that they may handle increasing volumes of data.

Intersystem Tools

Credible scenarios that result in dire consequences are the ones that require the most attention. Tools must be developed for modeling the consequences of infrastructure failure, and a ranking methodology should be developed to prioritize further research. The tools should be capable of simulating complex, highly interdependent systems for country-wide systems and of adaptively reconfiguring themselves to accommodate the constantly changing infrastructure.

Tools must also be developed to address the linkages between systems and to provide an analytical capability for systematically investigating interdependencies. As an example, various water supply systems may depend upon electricity and computers to operate remote pumps. The system may have back-up power for emergencies in the form of diesel or natural gas generators. These generators, in turn, depend upon the oil and gas distribution system to replenish their fuel reserves after usage, and the oil and gas distribution system is, again, dependent upon electricity to operate its pumps and control systems. Thus, a comprehensive analysis of attack and defense scenarios involving the water supply will require a thorough investigation of these interdependencies.

National Repository

A national repository for critical infrastructure tools, models, and data could play an important role in speeding infrastructure protection and reaction. Such a repository would contain a validated set of analytical tools and, to the extent possible, a validated set of analytical models. The repository might also house incident data; threat, vulnerability, and consequence models; data on lessons learned; and a graphical information system with location and model information of infrastructure elements. By sharing these resources, failure modes can be more quickly identified, and protective measures can be adopted to address them. The repository could also be of great value during the response phase of a national crisis.

Critical Infrastructure Test Bed

Whether employing existing commercial tools, or developing new ones, the tools need to be tested in a repeatable way. Ultimately, this testing will require a working test bed. Because such a test bed may be prohibitively expensive, development of a virtual test bed should be considered. One of the dangers of building one big test bed for everyone to use is that nobody will use it for fear of the damage that may accompany a display of their vulnerabilities, limitations, and future expansion plans. Replicable virtual test beds would obviate this privacy problem and enable researchers throughout the country them simultaneously.

Tools Working Group Report

The crux of the technical problem is to manage secure, survivable infrastructure networks, especially in situations when multiple, interdependent, accidental or intentional failures occur. This problem differs from other engineering problems in its grand scale and complexity, the strong system interdependencies, and the inapplicability of reductionist techniques. The system is also stochastic, uncertain, and unpredictable, especially when dealing with rare events like catastrophic failures.

A prime example is computer networking. Quick fixes are an unlikely solution. Instead, a long term fundamental point of view will be needed to understand in depth the problem's technical dimensions.

Need for Knowledge

At present, a dearth of knowledge exists. With the two exceptions of reports on DoD intrusions and voluntarily reported incidents compiled at Computer Emergency Response Teams, no systematic mechanism exists for preserving the wisdom and knowledge gained from previous intrusion experiences. System failure data must be collected and analyzed; experiments should be run on simulated systems; and real systems should undergo rigorous stress tests whenever possible. Methodologies must be developed to assess system failure risks; mechanisms need to be created for hedging these risks; and strategies should be established for tracking and controlling undesirable scenarios, such as the propagation of a virus through a network. Performance metrics and benchmarks for system security must be developed to facilitate standardization and communication. Research is needed to better understand the security vs. availability tradeoff, the difference between accidental and intentional failures, and whether a minimal essential secured infrastructure is feasible and practical. An attack taxonomy should be developed, as should formal methods on the technical level and methodologies for engineering complex adaptive systems. All of this knowledge should be stored in a centralized repository for preservation and sharing.

A possible coordinating organization for both R&D and repository efforts might be a private-public partnership that would be charged with redesigning the basic infrastructure architecture. The effort could be modeled on a previous private-public partnership like

Sematech, ARPAnet, Internet, etc. Basic research into the architectural framework should be directed and funded by the government, while companies should be encouraged to model specific systems for problem-solving in their particular infrastructure.

The centerpiece of the Commission's R&D effort is a national labs program that sent out teams from the national labs to talk to people in each of the infrastructures, assembled a series of working papers, and made recommendations. The effort is focused on information and communication infrastructure and a little bit on banking, finance, and electric power, but it will attempt to include all of the infrastructures. According to the study, the private sector is spending anywhere from $300 million to $600 million on information assurance R&D. Thus, any R&D recommendations should account for some kind of integration between these private programs and any government efforts. Other research efforts include a NSA study on government information assurance and a National Research Council study, which is in the first year of its two-year term.

The Commission's R&D report will cover several areas and attempt to answer the following questions: What are the research topics that require investigation? What level of R&D funding is appropriate, and how should it be split between government and private sector sources? Finally, how should the R&D efforts be coordinated between the public and private sectors?

Architecture

The fundamental technical problem is broader than the development of a set of tools. The challenge is to devise a system architecture that is the basis for both reliability and security. In the right kind of multisystem, basic structure, electronic exploitation of redundant paths would mitigate outages; heterogeneity would be tolerated to limit damage; and suspect behavior could be identified, monitored, and isolated. However, any architecture, even a well-planned one, will not be Shangri-La, with a road map for achieving perfect security.

People have been working for more than two decades to develop these kinds of architectures with little success. Architecture is more usefully thought of as an intuitive process of discovery.

A critical distinction should be drawn between macro-architecture and micro-architecture. The workshop discussion dealt with macro-architecture issues on a high, conceptual level to provide a blueprint for research. This kind of architecture discussion is to be distinguished from a micro-architecture discussion which would involve the rigid specification of an entire system, its components, their functionality and interactions, the system states, etc., and whose purpose is to lay the foundation for building a system.

The essential features of a system architecture are: predictability with some randomness, security orientation, fault tolerance, graceful degradation, robustness, and scalability. Predictability is needed to understand system behavior and failure consequences, but a degree of controlled randomness would improve security because such a feature would complicate the environment in which adversaries operate. Gracefully degrading means that when the system is stressed, it does not collapse completely; instead, its performance falls off gracefully. One technique for improving robustness is to have an integrated architecture that permits hardware and software diversity. This diversity helps prevent single point failures in which one weakness discovered in one system can be exploited in every other system. Scalability is essential to keep the architecture relevant and applicable to future computer networks as they are expected to be significantly larger and more complex than today's networks.

Tools

Although it is just one part of the solution, tool development is important. Given that the larger architecture problem has proven intractable for several years, perhaps efforts should be diverted toward solving simpler, more constrained problems. In this context that could mean solving some application problem in a particular infrastructure , for example, studying how the power grid could be used to assure power for a particular air-base operation, or trying to harden and develop architectures with some simplifying constraints.

The tools mentioned in the workshop can be classified into three categories, each group requiring different management structures, having different constituencies, and calling for different government and industry roles. The groups are: engineering-level tools, simulation- and training-level tools, and higher level analytical tools.

Engineering tools function at the most detailed level of knowledge. Engineers and computer scientists use these tools to characterize the vulnerabilities and the strengths of a system. Thus, the constituency consists of system developers.

At the next level is training where human operators interact with the system. Engineering knowledge can feed into training simulations of large-scale attacks. As yet unbuilt infrastructures can also be simulated, but the simulations should be grounded solidly in the engineering insights. Simulators, such as the DoD's Joint Simulation System, that use contemporary tools based on the common object request broker architecture–what DoD calls the High Level Architecture and the Real Time Infrastructure–can execute in real time, provide an opportunity for training under stress situations, and can teach people how to deal with attacks on critical infrastructures.

At the higher level of analytical tools and goals, the primary constituency is system operators; most of which are private sector people. Because the goal would be to engage industry, the government could provide leadership by requiring all of its vendors to participate in programs to support analytical tools research. Using data gathered from industry, the government could sponsor research efforts to aggregate and analyze the data. For example, if the government required all companies that do business with it to collect data on computer intrusions and the estimated costs of each intrusion, the data could be aggregated to better characterize the extent of the problem.

Equally important with the engineering of systems is the management of them. Management involves planning and operating systems on different scales with real-time dimensions. Tools in each of the various planning, engineering, and operations phases are presently lacking.

Modeling and Simulation

Traditional modeling and simulation differs significantly from the kind of modeling and simulation discussed here in that traditional modeling looks at problems in a universe of random events; the opponent is noise. Systems, to the extent that they are robust against noise, stay up. The workshop discussion, however, has revolved around attacks coming from a determined opponent; the opponent is not noise but is the devil. Instead of random acts, the devil will do things to exploit specific system weaknesses in sequence so as to create the worst possible consequence.

Better models are clearly needed. Essential features of systems should be abstracted, and canonical model should be analyzed to capture the dynamics of total failure modes. Paths that lead to these failures must be identified and understood as well as the evolution of scenarios that lead to failures. To the extent possible, simple problems should be tackled first.

Just as the nuclear weapons laboratories build gigantic supercomputers to conduct virtual experiments for maintaining the safety and reliability of the nuclear arsenal, so too must some kind of software-simulated environment of networks and their interconnections be constructed to better understand infrastructure vulnerabilities and behaviors. This environment may be crafted by tying together the models that corporations currently use to operate their infrastructures or by building a separate test bed like the one proposed earlier.

A great deal of work has been done in the area of modeling and simulation. The DoD, Santa Fe Institute, Nonlinear Institute at the University of California at San Diego and University of Southern California, and Electric Power Research Institute are all engaged in developing, at some level, tools for modeling and simulation of complex, nonlinear systems. The problem that these researchers are encountering is that the systems are inherently difficult to model. Typically, they compromise their model accuracy by limiting the degree to which the system will deviate from known, conservative operating points. Because the ensuing system conditions during an attack are often much farther away from the modeled operating points, the model is inappropriate for predicting system behavior under these circumstances.

One potential solution for dealing with highly nonlinear, complex systems is to redesign the systems, making model tractability a required feature of the system. Other features may be lost; efficiency may be compromised; and performance may suffer. These losses must be balanced against the benefit gained by being able to predict the system's behavior.

Concluding Thoughts

The changing landscape for many infrastructure industries, brought on by deregulation and the break-up of monopolies, has created a unique opportunity for influencing the design of systems. As these industries rethink their businesses and processes, a report from the Commission about the requirements for inherent internal system security can have an enormous, leveraged effect.

A critical distinction should be made between information infrastructures and physical infrastructures, like power and water distribution systems. Because information is generated by human beings and can be exchanged in many ways other than through a physical infrastructure, focusing on physical tools to protect the physical infrastructure that supports basic information exchange obscures the very important social infrastructure of information exchange. Any amount of security that goes into designing physical security can be defeated by a simple conversation between two people. Although this discussion has focused primarily on physical tools, intersystem security studies should also examine social information infrastructures.

Ubiquity of Information Technology in Government & the Economy

William Crowell

Forty years ago, the US had approximately 5,000 computer, no fax machines, and no cellular phones. Today, it has 160 million computers, most of which are networked or can enter the network; 40 million cellular phones; and 14 million fax machines. Information technologies (IT) are changing the structure of business, government, and society while simultaneously creating new threats to privacy, public safety, and national defense.

In the future, computer and telecommunications networks will become ubiquitous. By 2002, the number of people involved in industrial concerns will drop to 12% of the labor force, while the number involved in information work will increased to more than 33%. By the end of the decade, fewer companies, large or small, will be able to compete without network-based operations.

This shift has not yet occurred, or is only beginning, in Europe and in most of the Far East. The US has led the rest of the world into the Information Age, moving faster and farther than any other nation to adopt and integrate IT. As an unintended consequence, however, it now has the greatest strategic vulnerability, and its future is tied to a resource that it has not yet learned to protect.

IT plays a central role in the provision of government services. As pressures to modernize and to reduce costs increase, hard-to-use legacy systems will be replaced with new technologies that will enable government to do more with fewer people. The Cohen Act has unleashed the purchasing power of all government agencies—not just defense—to buy new technology.

The Desert Storm experience accelerated the military's adoption of IT. During the war, 100,000 messages and 700,000 phone calls were exchanged daily. The NSA delivered 80 tons of keying material to the desert to support the use of cryptography in the field. During that war, in each half-day NSA processed more information than it had processed in its entire 40-year history. In four months, it changed from a low information throughput to a high information throughput agency, cleansing itself of "sneaker nets" and all other vestiges of industrial-age practices.

Unfortunately, good performance standards for security in the new government systems, or even people to evaluate systems to ensure such standards, are not nearly common enough.

As a result, these systems are built on a poor foundation of security, creating serious vulnerabilities. Trusted systems are needed, and the trust must be built into the initial design.

How Vulnerable is the US to Deliberate Attack?

A need exists for an accurate assessment of the threats to networks, the level of risk, and the consequences of adverse events. Policy responses to the threats will be intimately tied to the severity of the consequences. At the low end of that spectrum are small monetary losses while at the high end is airline safety. The two ends of the consequence spectrum lead to very different policy responses.

The increasing use of IT also has led to a dramatic increase in the number of attacks on networks, and at present the common assumption that hackers are to blame is highly speculative. Because DoD has no active defense, it seldom knows the sources of unauthorized intrusions into its computers. The available attack technology is outpacing the installed defenses, creating opportunities for stealing intellectual property and disrupting military effectiveness.

Who are the adversaries? Who would want to attack US systems? Several foreign national intelligence organizations want to gather information; foreign military organizations would like to alter US military capabilities; terrorists might seek to finance their operations through Internet fraud and/or conduct Internet operations to commit terrorist acts; industrial competitors, hackers, and disgruntled or disloyal employees have varying incentives that might lead them to attack systems. Each is motivated by different objectives and constrained by different resources, technical expertise, access to targets, and risk tolerance. All can be assumed to be technically competent because the knowledge is widely available. Fifty percent of the computer science graduate students in US universities are from outside the US.

How extensive is the threat, especially the foreign component? Direct evidence is scarce. US intelligence can confirm that a substantial number of countries are working on cyber techniques and that the number has more than tripled in the last three years.

The organized threats, from intelligence and military organizations, have sought to covertly develop and test new information warfare capabilities on US networks without getting caught. How successful they have been might be inferred from tests conducted by NSA, in which 60-90% of systems it attempted to penetrate were successfully compromised, with almost no detection of these intrusions. Thus, US systems may have already suffered thousands of successful attacks for purposes of reconnaissance, surveillance, intelligence-gathering, or even weapons development, and be completely unaware.

Encryption

The net is a party line, unless security is being used. In network terms, security is about encryption, authentication, data integrity, digital signatures, and non-repudiation. Trust is about key management and digital signatures. Most of the public rhetoric is centered on encryption, but very little of it is concerned with trust.

When Netscape’s browser secures a link and joins the key with a bank, how does it verify that the public key is the correct key for that bank? Key management and certificate authorities are the glue that binds security together, and almost no attention is paid to it. The debate about encryption policy has shifted off into export controls and not into how to build a secure infrastructure for this country. Is this the right way to generate public policy on encryption? To achieve widespread use of encryption, the following systems and infrastructures must be in place: key management infrastructure, key recovery capability, law enforcement access to encrypted data, international cooperation, digital signature standards, security performance standards, and government purchases of encryption technology.

Encryption solutions must be built on top of key management infrastructures to provide trust in how they actually provide true security. This infrastructure should not be created by the government, but should be comprised of as many systems as the public will tolerate.

Key recovery capability must be possible. Encouraging weak cryptography is the wrong way to go. Strong cryptography should be used to protect important information. Strong cryptography means that the encryptor has an incentive to be able to recover information. Anybody who argues that key recovery weakens cryptography is ignoring that fact. If key recovery does weaken cryptography, it does so because of poor implementation.

Law enforcement must have access to encrypted data. The 1000 lawful accesses by court order each year, most of them at the state and local level, have resulted in 20,000 arrests and convictions over the last 10 years for the most heinous crimes committed in this country. This access is part of public safety, and the public has an expectation that it will be used as such.

International cooperation is essential. Unfortunately, inflamed rhetoric is making cooperation increasingly difficult. Every country with which Ambassador Aaron met wants to have lawful, court authorized, warranted access to cryptography, without exception. None of them, however, have agreed on how to do it. Many worry that the United States will drop export controls and overwhelm the market, forcing them to erect import controls. Ideally, they would like to find a cross-border, cooperative solution, but technological disparities complicate those efforts.

Digital signature standards, interoperability, and legal status need to be established. Digital signatures are absolutely fundamental to trust and security. No two signature systems operate together today. Seven states have passed seven different laws on digital signatures, and no leadership has come from Congress. What is the legal status of digital signatures? Key management protocols and certification authority protocols also need to be established. Incentives to get that work done are needed.

Cooperation between government and industry is needed to set performance standards, R&D agendas, and verification of security levels. The US government should not be a tester of encryption or security products. It can, however, foster a private organization to perform this function. NIST and NSA, over the next three years, will be funding and developing such a private institute. The intent is to use government technologies and funds to jump-start what will hopefully become the Underwriters Laboratory for cryptography.

Government procurement of encryption technology must be encouraged. Government has stewardship of a great deal of information, both public and private. If the government were to encrypt these without having key recovery capability, then it would run the risk of having information “electronically shredded,” violating statutes that require public access to information.

The encryption issue is not a simple public policy question with a simple solution of “end export controls and be done with it.” Many obstacles impede the use of security in networks. It demands more serious treatment than it has received, and more leadership.

Q & A Session

Key Recovery

"Key recovery" sounded better than "Key escrow" when it was invented, but it is somewhat misleading in that the key need not necessarily be divulged to recover encrypted data. In fact, most schemes under consideration today do not divulge the key at all. With respect to misuses of key recovery, no system that involves humans can be completely impervious to attacks. However, robust systems are needed that can withstand normal kinds of attacks to safeguard the United States' important information, whether defense or otherwise, to protect the nation.

Key recovery is not about providing total access for law enforcement to everything that everyone does, nor is it about whether terrorists or criminals are smart enough to use encryption well, although some of them probably are not. It is about providing some degree of protection where possible. Just because the airlines cannot protect against every single circumstance do they give up entirely on safety? When terrorists do business, they do it in several different areas: with each other, with their sponsors, and with the general public. In the first two instances, they may be able to protect themselves, but they will have a difficult time protecting themselves when doing normal business, like using a credit card, traveling on airplanes, etc. Key recovery is mostly about these transactions.

Looking at the issue of key recovery as a public policy need, what options exist to encourage it? If some industry has a market incentive to develop such a system, then government can ride on that market force. If no such force exists, then the public policy need, like public safety, must be weighed against the costs of intervening in the market. At present, the market for key recovery in communications is confined to narrow areas, but this condition will likely change over time.

Trusted Systems

Trusted systems also should imply trusted code. Currently, NSA is conducting research into methods of protecting software so that changes and errors can be detected early enough to prevent harm. Obviously, hardware assurance is much better developed than software assurance. Interestingly enough, the basic science required to protect software is public-key cryptography. By signing the software, and by having an incontestable public key to read that signature, some measure of security can be attained. Unfortunately, software invariably contains bits whose functions cannot be traced and look as valid signed as when unsigned.

The Cryptography Underwriters Laboratory venture will be provided a repository of information and a group of people trained to use that information. The level of demand for such services remains unclear. This venture is, in part, an experiment to characterize the demand for verifying system robustness and trustworthiness.

Cryptography could be very helpful in making systems more available, especially those that support the network itself. Because most availability problems relate to potential attacks through maintenance ports and holes in operating systems, cryptography, particularly through authentication, could have great applicability, provided systems went beyond the current standard of password protection. The conflict rests in the amount of inconvenience users are willing to tolerate. Transparency will make systems more convenient, but in doing so it makes trustworthiness more difficult to achieve. Some have suggested creating universal identification numbers as a partial solution, but the present administration is very, very carefully focused on a market-driven, rather than a centralized system.

The current administration is also interested in seeing the spread of strong encryption, not weak encryption, that can be used with confidence and that can protect and balance all of the nation’s interests. As of today, however, no law has been passed on this issue. Public debate is needed to clarify how strongly the public feels about the various elements of this issue.

Cylink and Its Market Environment

Fernand Sarrat

Cylink has 60% of the link encryptor marketplace for private networks, but private networks are becoming passé. Nevertheless, link encryptors are far from dead. The new area of growth is security for public networks. This new market is only 2% saturated in the US with the top three firms holding only 6% of the market share. Low barriers to entry have resulted in some 90 competitors, and the market is projected to grow from $0.5 billion in 1996 to $6.5 billion in the early 2000s, a 44% annual growth rate. The industry is just starting to hit the inflection point of growth on the technology adoption curve.

Cylink focuses on large accounts. Half of its revenue comes from bank customers and another 25% comes from the government. The government customers are non-DoD three-letter agencies, including the Department of Justice. Long-distance carriers are the new growth opportunity for Cylink, including Internet providers; 13% of current revenues come from AT&T, MCI, and Sprint. Other customers include SWIFT, a large portion of the Federal Reserve, Bankers Trust, and Citibank. Cylink also secures the backbone for AT&T's Operations and Administration division and has a contract to secure BT-MCI.

New Products and Technologies

The only established products in this market are firewalls. The market for firewalls seems mature: firewall prices went down 35% last year; 73% of the firewall market is controlled by five firms; and Checkpoint has a 53% market share.

Authentication has penetrated to only 17% of the overall marketplace, but it is growing at 54% per annum. Remote access will cause it to take off and will move it from tokens to smart cards. Europe is eons ahead in smart card technology. Another important technology in developing the smart card market is elliptic curve encryption, as it will enable vast improvements in performance.

Other new, rapidly growing markets include the enterprise solution market (133% growth per year), secure e-mail (68% growth per year), and virtual private networks (VPNs) with 64% growth per year. These markets are very immature and are about to take-off.

How to Get Companies to Invest in Security

To get companies to buy security products, a vendor must understand what customers want and the market dynamics.

What Customers Want

Security is a nuisance for a corporation because it requires investment and offers no clear value return in many cases, so corporations tend to minimize investment in securing their business. The value proposition Cylink offers to its customers is simple: cost reduction in communications lines and increased market flexibility can be achieved through security.

The complexity of security also inhibits its adoption. If security can be made easy, and not time-consuming to deploy, then the benefits received from it will outweigh the inconvenience and companies will use it. For many industries, this point has not been attained. Manageability, scalability, and ease of use are the keys to expanding the security market.

Market Dynamics

The early adopters of security were banks, government, and now the telecommunications companies. This beachhead of early adopters is important for getting further growth. Because of acquisitions in the financial community, the use of security should spread from banks to insurance companies and other firms in the financial services markets. Similarly, the telecommunications companies should provide a springboard into Internet service providers.

What Government Can Do to Make the Market Work Better

One of the worst possible outcomes would be for standards to be set by people who, by virtue of patent ownership, extract an unreasonable price from other vendors or have arbitrary licensing and royalty policies. Such a scenario will hinder the spread and adoption of security. The government should prevent monopolies from arising through patent dominance. No patented key recovery system should become the standard. Some of our competitor's patents rest on Cylink patents, but Cylink has not sued because it hopes elliptic curve usage will soon take-off, making it easier for everybody to enjoy security.

The government approved three key recovery schemes. One company is licensing. Another dropped theirs, deciding to join Cylink's instead. Although patenting and licensing was a very attractive option, Cylink decided to throw its scheme into the open market. Its reasoning was that it could make money by selling tools based on that standard, but above all else it wanted to see the standard adopted. The Commerce Department said to other companies that if they adopted Cylink's key recovery scheme, they would receive the same favorable treatment that Cylink is getting with respect to exports. That kind of government action is helpful.

The Commission can facilitate a move to higher levels of security. It can encourage government R&D dollars be spent in critical areas, specifically in developing technologies that enable authentication, encryption, key standards, smart card technologies, and elliptic curves. The Commission can also encourage the use of subsidies like R&D tax credits over taxes. Tax breaks ultimately benefit the end user, while taxes are borne by the end user, so they tend to favor subsidies as well.

The government should favor incentives over regulations. Security certifications that must be passed for firms to be able to do business with the government or industry are pretty strong incentives. Similarly, the standards that the government promotes through deployment and purchases are much more likely to become de facto standards as opposed to standards which are merely declared.

Q & A Discussion

Cylink believes that financial institutions are incurring substantial losses as a result of cybercrime. Specifically, the four major Swiss banks had all taken big hits before implementing security. Today, they are so tight with security that virtually every link out of a Swiss bank is encrypted. In El Salvador, one of the major banks lost roughly $5 million in a fraudulent electronic transfer.

Modeling and simulation tools present a daunting challenge. They would be extremely valuable if they could be constructed in a timely fashion, specifically, before technological change made them obsolete. The complexity of the system being modeled and its dynamic nature make many skeptical as to the feasibility of modeling tools, but these reasons do not justify giving up before even trying.

Roundtable Discussion

William Perry

The following four fundamental assumptions underlie the Roundtable Discussion. First, the threat to US infrastructure, and, in particular, to the communication networks, is serious and will get worse. Second, the stakes are high and will only get higher as society becomes increasingly dependent upon the networks. Therefore, the vulnerability to organized attack is increasing, and a potential for a real catastrophe is developing. Third, the protection technology for the networks is expensive and inconvenient. Fourth, the will to act is generally lacking because the solutions are expensive and inconvenient, and because the division of responsibility remains unclear. These issues raise the unpleasant possibility that a catastrophe will be necessary to force the US to act.

Focusing now on actions that can be taken today, a Presidential Commission has been established to recommend action at the national level. In this roundtable, the discussion will focus on the proper role of the government in this area and specifically how it should fulfill that role.

Roles of Government

One role of government is to provide information and education. Specifically, it should be measuring and assessing the threats in some detail: both the real threats that have occurred and the potential threats that may materialize. Assessments have been episodic in nature, rather than the systematic effort needed to measure the threat. Once the threat is assessed, the public should be educated about it, and information should be provided to incentivize industries to protect themselves, to develop protection technology and systems that they can sell as products, and to work cooperatively with government.

A second role of the government is to support research and development, whether done in government laboratories, contractor funded, or incentives to contractors. Defense R&D uses all three techniques successfully. R&D should be directed toward new protection techniques, models and simulation, and providing a basis for Red Team analysis. Small teams need to be set-up to look critically at the networks and to find ways to break into them; then government and industry can formulate measures to reduce the vulnerability.

Other meaningful tests need to be constructed and performed. No single industry can do this alone; it must be done or supported by the government. To be most effective, the government should turn to industry and provide organization and incentives, as it has done in defense research and development.

The third area for government is developing standards. The first steps in this area are to require reporting of incidents, to maintain a knowledge base that will serve as a repository of knowledge on the field, to establish performance metrics, and to work with industry to develop standards. Standards have been set in other fields for decades, and they need to be systematically set in this field as well. An organization needs to be established in which the industry and government will systematically and regularly work together on the development of standards. Standards should not be developed in isolation or only once, but should be developed in a continuing process.

A fourth role for government is protecting the market against monopoly, in particular, against a monopoly in protection techniques. As alluded to by other speakers, the presence of monopolies in the market for protection techniques could seriously hamper private efforts to secure the infrastructure.

A fifth role has to do with the legal aspect of this problem: defining what is a criminal action, formulating laws to sanction a criminal action, and developing an enforcement regime for these laws. Very little has been done in this area compared to other criminal actions. If successful laws and regimes can be demonstrated on a national level, then the US can play a significant international role in this problem. International norms need to be established, and US law enforcement needs to cooperate with other law enforcement agencies in other countries, just as it does in dealing with transnational organized crime and in trying to control drug traffic. The institutional models exist, they just need to be applied to this particular problem.

The last issue is partly a legal issue and partly an issue of standards: working with international agencies for common carrier agreements. The ITU is the best case here.

One final point regarding the framework for the proper role of government in this problem is that a public/private partnership focused specifically on infrastructure architecture should be developed. The partnership could, of course, also deal with broader issues in this area, and is a very interesting and important idea.

John Gage

Where there is power, there is going to be attack. The infrastructure system developers never thought that they would be linked, nor did they think that they would be attacked. If one were to examine the infrastructure closely, he would see that although it appears to work well enough, it is a cobbled mess of components. What can the government do?

The government can do something about the cross-infrastructure communication problem among the infrastructure providers such as sewer, water, power, and rail. Whether or not they have a way to communicate with each other is unclear. The government needs to do an assessment across infrastructures.

The government can provide a Red Team mentality, can create the tools of Red Team attack, and can make those tools available for private industry to use. Privacy is key; most companies will want to go through and audit their own systems.

A role exists for the federal government to set an example for acquisition policies that are thorough. Techniques for catching Trojan horses in both software and hardware need to be developed so that industry and government can check their acquisitions for unexpected surprises before they do damage.

Government can encourage the establishment of social norms by promoting an awareness of computer security and attacks. A taxonomy of attacks would be extremely valuable in expediting communication between people when an attack has occurred.

A testing facility is needed to stress test systems. Both Japan and the United States are using Malaysia as a test case because they are incapable of testing the systems inside their own countries, primarily due to the web of laws, liability, and regulations that entangle such efforts.

Sun is currently redoing its operating systems because, in part, of security concerns. At present, state-of-the-art 1985 operating systems like UNIX and Windows NT run the banks, the trading floors, Desert Storm, Command and Control, and soon, the air traffic control system.

Stephen Lukasik

First, the government should look carefully into the trends within each infrastructure system that are currently diminishing the robustness of those systems. Second, the government should look very carefully into the interdependencies among infrastructure systems for presently unforeseen consequences. Third, on the threat side the government should think broadly about the larger objectives of the infrastructure attacker. Understanding the attackers' motives will help set some overall perspectives, and, perhaps, priorities.

A very interesting book, *Normal Accidents*, talks about things that break and how they break in unexpected ways. The author analyzes many systems and incidents, including the Three-Mile Island disaster, and characterizes systems in terms of their coupling, or interactions. The worst state of affairs typically results from tight coupling in which the systems have complex interactions and relatively limited buffering and redundancy. The power grid is a primary case in point. As deregulation encourages generation capacity growth and greater economic efficiency, the generating and transmission systems will be run closer to their natural limits, making them less able to handle system stresses.

The Internet is a totally new infrastructure that is, in its own quiet way, linking pieces of society that have never been linked before. So, while it is a technical and business opportunity, and even a social opportunity, it may also be building in unforeseen problems in various other social systems. For example, electronic commerce, health-care delivery, and news collection and distribution are just the beginning of a long list of systems that are being linked by this network, and these linkages may have unforeseen consequences.

David Friedman

The workshop has been contemplating two very different classes of threats: routine computer crime and the information-equivalent of a nuclear attack. The Commission appears to be primarily driven by the latter problem. Unfortunately, the latter problem is a purely hypothetical one as nothing like it has occurred.

The evidence for its existence is that the NSA reports that it could use computers to penetrate systems and cause significant damage. So two questions worth thinking about are the economic questions from the standpoint of both the attacker and the victim. Do these new technologies provide cheaper, easier, better ways to cause damage? And, from the victim's perspective, how much personal injury will the damage really cause? These infrastructure attacks may not be the equivalent of a nuclear attack at all, but rather a form of harassment, intent on slowing down actions.

The computer crime kind of problem is one that can be handled. Viewed as an ordinary private-good problem, it is one in which the targets have incentives to defend themselves. Certainly the government can help in these situations by not hindering the targets with legal rules, but it should basically stand aside and let the market function. In general, complicated decentralized systems are dealt with best by using markets, and the markets are dealing with the problem, even though some people may have a false perception to the contrary.

These two problems are related in that the basic response to both of them is the same, namely harden systems to prevent intrusions. To the extent that people have a strong private incentive to harden their systems, public protection can be achieved.

One of the striking facts about this problem is that nobody knows to within even an order of magnitude how much computer crime is taking place. If the government were to gather some hard numbers to quantify the problem, then firms could make informed decisions about whether to take any precautions.

Research on information warfare is totally speculative today because it has not happened. The fact that the infrastructures are complicated systems belonging to and controlled by several different people makes management of them problematic with a top-down approach. Once again, the clearest answer is for government to refrain from direct intervention and work on information collection, production, and distribution.

The government can, in the process of managing its own house, generate information, share protection technologies, and influence private sector investments. If the research at DoD yields effective tools that prevent hackers from breaching DoD computers, the government should share those tools. Given that the government writes regulations, buys goods, passes laws, etc., it ought to perform these functions in such a way that it encourages rather than discourages private investments in protection.

Should the government actually force or pay people to do things? One serious drawback to mandates of this sort is that they tend to lock into position the current dominant approach, in essence freezing the system. An extensive economic literature has been written on the way firms use regulation to benefit themselves under the pretense of benefiting the public, and any new regulation, no matter how well-intentioned, may end up a political football rather than an effective protection policy.

Roger Pajak

The banking sector is said to be a very murky component of the infrastructure, and this description is an apt characterization. Bankers, financiers, and people in the finance area often refuse to admit that a problem exists. They are very reluctant to admit that anything in the way of penetrations or intrusions occurs because they are extremely concerned about customer and client confidence, which is the bottom-line consideration. Also, the banking sector considers itself very confident, very tight in the way of anti-terrorist precautions and procedures. They claim that because they have several redundant controls damaging system penetration is impossible. Although these security systems can handle almost any cyberspace intrusion from a teenage hacker threat to perhaps an organized-criminal threat or even a rudimentary terrorist threat, they cannot handle an organized attack perpetrated by a rogue state. That juncture is where the financial community believes the government has a role: to serve as a firewall between it and an attack coming from a rogue state.

The Infrastructure Protection Task Force (IPTF), has a mission in public awareness and education. It interacts with finance and banking organizations and seeks to define a unified approach to meeting the threats in cyberspace. Among other things, it is working on the so-called yellow pages directory of the government, which will be an on-the-shelf compilation of all of the government WATS offices, operations centers, and response teams in the computer area that respond to any kind of a cyberthreat or intrusion. It is also attempting to generate a handy 911 number where a firm can call for help when a threat or intrusion is being perpetrated against it.

Red Team simulations have been a useful tool for testing Treasury systems. A number of intergovernmental exercises and war games have been conducted to test infrastructure systems, including those in the banking and finance sectors. Treasury has also formed a Treasury Terrorism Advisory Group to quickly disseminate threat notices, analyses, and intrusion reports to its constituent units: the Bureau of the Mint, Bureau of Engraving, the Financial Management Service, and the Comptroller of the Currency. The Treasury Department is also attempting to coordinate with the intelligence agencies, primarily NSA, to continue Red Team approaches in the testing of systems, particularly with respect to classified e-mail systems, connections between Washington and other cities in the United States, and between Washington and US attaches abroad.

General Discussion

Red Team Strengths and Weaknesses

The strength of a Red Team is that it does an excellent job of identifying a very large, very broad set of potential problems, potential issues as well as potential solutions. The objective is not to prove that penetration is possible, but to analyze a broad range of possible avenues and advise management as to what fixes should be done first. Extensive application of the approach may also help to build a catalog of quirks and attributes in hardware or software that enable penetration, and understanding the sum total of those could be very useful. Because Red Teaming tends to display system vulnerabilities in a dramatic fashion, it is very good for raising awareness.

Red Teaming, however, is not a panacea. A number of serious weaknesses are inherent in the Red Team approach. First, Red Teams, while good at raising awareness, do not always lead to improved overall security. Often, management is quick to agree that a problem exists after the Red Team has cracked a system, but then assumes the problem is fixed when the one point approach is fixed. ARPA experienced this problem in the early ‘70s. Greater thought should be given to structured ways of designing computer systems, secure channels, trusted code, and trusted processes. Red Teams may be very good for getting management’s attention, but they may not achieve better overall security.

Second, Red Teams usually produce a list of system vulnerabilities that is too long and cumbersome. When this list is given to the system administrators, they have difficulty deciding which items to address because they lack the resources to address them all. Also, Red Team tactics are not necessarily representative of the kinds of things that are likely to happen, thus skewing the perception of a system’s level of security. Red Teams are a useful tool for identifying weaknesses, but a management layer is also necessary to determine which risks should be reduced, and which ones must be accepted.

Finally, Red Teams tend to focus on technological vulnerabilities, and as has been mentioned before, human-factors and social-engineering are often a major source of security holes.

Red Teams are just one means of identifying exploitable weaknesses, which constitute vulnerabilities; but vulnerabilities often do not translate into a threat. In a military context, when the threat is poorly defined, immature, unknown, or below the level of the intelligence community's attention, it is difficult to be convincing. One approach is to demonstrate the effectiveness of the military's offensive techniques if they were directed at US infrastructures. Currently, NSA has an information operations technology center that is technically separate from NSA but overseen by the NSA director. It is where NSA, the Defense Department, and others throughout government join together to examine the tools of information warfare.

Red Team Industry

As a marketing tool, IBM created group of "ethical hackers" to perform Red Team exercises on any companies willing to be tested. The companies were asked to identify where their strongest interest lay in protecting a particular area of their network, and the team invariably cracked it, often within a very short period of time. IBM now cannot find enough good hackers to do that work. One possible role for government could be to help build an industry that does Red Teaming very effectively, perhaps with expertise drawn from NSA. Analogous arrangements in the physical security realm exist where the government sends in teams which do effectively in the physical security regime what is being recommended for information network security.

A very vigorous Red Team business is already thriving in the private sector. Large business organizations tend to be the primary customers. These Red Teams test firewalls, perimeter security, and connections to Internet. Although successful so far, these businesses still worry about liability and damaging people.

The market has provided a highly decentralized form of Red Teaming in which a company effectively places a bounty on its product. Apple has run its "Crack-a-Mac Contest" for quite some time, basically offering money to anyone who can break into its computer and obtain certain information. As a means for fundraising and keeping its cracking skills sharp, perhaps NSA should enter a few of these contests.

The Commission will recommend using the SEI model to help encourage the growth of such an industry. Originally, the SEI went out, backed by government funding, and assessed the software capability of various firms, rating them 1 through 5. They also advised as to what had to be done to raise a company's level. The SEI's services would later be transitioned to industry with the FBI training the assessors of private industry, soliciting proposals, and then certifying these groups as being able to conduct assessments equivalent to the quality that SEI provided. The Commission is developing a similar scheme for NSA on the assumption that NSA has a lead in Red Team techniques and technologies because of their experience with offensive and defensive aspects of information operations, and these assets can be best utilized by transferring them to the commercial sector and letting private enterprises perform the Red Team exercises.

Legal Issues

Regarding the legal impediments to greater use of Red Teams, legislation is currently before Congress to revise the Computer Security Act of 1987, yet again. At present the law provides for Red Teaming, but modifications in several areas to existing regulations and laws would be helpful and might encourage the use of Red Teams. These changes would not necessarily involve granting more authority, but involve clarifying authority instead.

Liability laws must be also changed to permit the assessment of vulnerabilities without increasing liability. At present, a strange set of incentives exist which encourages people to remain ignorant of their security problems by creating liability if security holes are demonstrated and for budgetary or personnel reasons are not patched. In addition to changing liability laws, the government could also set standards of best practice so that people will know what their legal obligations are to avoid liability.

Returning to the legal questions raised in previous sections, much of the work suggested goes beyond the bounds of the authority and charter of the Commission. However, an opportunity for forging an answer may lie in forming an organization for data structures similar to the National Security Telecommunications Advisory Committee (NSTAC). It could be an industry-government partnership and could be given the charter and legal authority to act. It could be a form of watch-dog to insure that the marriage between industry and government remains healthy with regard to sharing vulnerability information.

Government-Industry Partnership

The government has a history of setting standards known as “mil specs,” which at the time they were created performed a very useful function, but then they became encrusted. After a number of years they actually became counterproductive because they did not adapt to the changing times. The Defense Department is now moving toward using industry standards for the same purpose, or developing standards in conjunction with industry. These moves are just one example of a government-industry partnership and also demonstrate that a partnership has a place in the standards area as well.

The government’s work with the programmable modular communications system (PMCS) to try to put together an open-architecture standard for wireless is another good example of government-industry partnership in the area of standards. About a year and a half before PMCS the government reached out to industry, and industry formed a forum for open architecture radios called the “Modular Multifunction Information Transfer System Forum” (MMITS Forum). It brought industry and the military in a cooperative venture with the Defense Department.

Standards

The government definitely has a role in setting both technical and procedural standards. The high-tech industry has an established practice of setting standards to which the industry conforms and then develops compatible products. Before any standards are developed, however, a fundamental understanding of the problem and the possible solutions that the differing proposed standards will foster must be obtained, typically through research. Government can help the standard-setting process by promoting this underlying research.

The government should also figure out ways to drive de-facto standards rather than to impose rules or guidelines. The government could learn by looking back at the standards that have been established, the manner in which they came about, and whether they promoted or hindered industry growth. Future battles will likely be fought over secure e-mail standards, control of payment standards, and key recovery.

The Commission certainly believes that standards are needed. It also believes that they ought to be generated primarily by the private sector but in collaboration with the government. For example, the North American Electrical Reliability Council (or NAERC) is moving from voluntary standards that it imposes on its membership, which includes all of the electrical industry, to mandatory standards. To make this transition, they may need some government backing, perhaps in the form of government purchases of electricity in which it insists that the supplier meets the Council’s standards. The government has leverage with everybody who supplies it, and the Commission is looking at similar ways in which government purchasing power can be used to promote standards.

Program

Workshop on Protecting and Assuring
Critical National Infrastructure:
Setting the Research and Policy Agenda

Wattis Room, Littlefield Center
Stanford University
July 21-22, 1997

Monday, July 21:

8:00–8:20	Continental Breakfast
8:20–8:30	Welcome – *Michael May* Program and Logistics – *Seymour Goodman*
8:30–8:50	PCCIP Progress Report: Issues and Options – *Tom Marsh*
8:50–9:10	Discussion
9:10–9:20	What are we trying to do? Framework and continuity with the last workshop – *David Elliott*
9:20–9:45	International and Legal Issues of Infrastructure Protection: Is It a Small World After All? – *Lawrence Greenberg*
9:45–10:00	Discussion
10:00–10:30	Break
10:30–10:50	Economic Aspects of Infrastructure Security – *Hal Varian*
10:50–11:10	Discussion
11:10–11:30	Tools for 21st Century Infrastructure Protection – *Stan Trost*
11:30–11:50	Discussion
12:00–2:00	Luncheon Speech: The Trust Implications of an IT-based Infrastructure – *William Crowell*
2:00–2:15	Breakout Goals and Logistics – *Seymour Goodman*

2:15–3:45	First Breakout with Parallel Sessions on the Three Focal Areas – Chairs+: International/Law: *Paul Edwards/Richard Hundley/Richard Gronet* Economics: *Edward Zajac/David Friedman/Kathleen Bailey* Tools: *Edward Feigenbaum/ Edward Zeitler/Nick Bambos*
3:45–4:15	Break
4:15–5:30	Second Breakout with Parallel Sessions on the Three Focal Areas
6:00–8:00+	Dinner Speech: Trends in Information Security – *Fernand Sarrat*

Tuesday, July 22:

7:30–8:00	Continental Breakfast
8:00–9:30	Three group reports. Presentations and short discussions – Chair: *Ronald Lehman*
9:30–9:45	Break
9:45–11:45	Roundtable/Synopsis – Chair: *William Perry* Panel: *John Gage, Stephen Lukasik, David Friedman, Roger Pajak*
11:45–12:00	What next? – *Goodman and Lehman*
12:00-1:00	Box lunch. Informal discussions.

Points of contact: Seymour Goodman (650)725-2704,
Banani Santra (650)723-6501 in the CISAC IT Program
administrative office,
or David Elliott (650)854-1827

Participating Commissioners:

Robert (Tom) Marsh is Chairman of the Presidential Commission on Critical Infrastructure Protection (PCCIP). He is Chairman of the Board for CAE Electronics, Inc. and for Comverse Government Systems Corp., and serves in various senior capacities for other companies. He is a retired 4-star general whose last assignment was as commander of the Air Force Systems Command.

Mary Culnan is a Commissioner from the private sector, where she had been Associate Professor at Georgetown University's School of Business. Her primary interests are in information privacy and electronic commerce.

Peter Daly is the Commissioner from the Department of Treasury. Before joining the Commission, he was senior Advisor in the Office of the Assistant Secretary for Management and Chief Financial Officer. His specialty is electronic money policy issues.

John Davis is is the Commissioner-designate from the National Security Agency. At NSA, he has served as Director of the National Computer Security Center, Deputy Chief of the Research & Technology Group, and Chief of Microelectronics.

David Jones is the Commissioner from the Department of Energy, where he directed an organization responsible for developing, promulgating, and analyzing DoE-wide safeguards and security policy, procedures, and standards.

Stevan Mitchell is the Commissioner from the Department of Justice. He is a trial attorney with the Criminal Division's Computer Crime Unit. He has litigated cases, conducted investigations, drafted legislative proposals, and participated in international efforts to curb illegal uses of advanced technology.

Paul Rodgers is a Commissioner from the private sector, where he last served as executive director and general counsel for the National Association of Regulatory Utility Commissioners.

Frederick Struble is a member of the PCCIP Banking and Finance Team and the Economics Team. Prior to joining the Commission, he served as a member of the Federal Reserve Board for 25 years. While there, he was responsible for developing and implementing policies for the supervision and regulation of banking organizations.

Nancy Wong is a Commissioner from the private sector, where she had been the Manager for Information Assets and Risk Management at the Pacific Gas and Electric Company.

The principal participants and organizers:

Kathleen Bailey is a Senior Fellow on the staff of the Director of LLNL. Previously she has served as Assistant Director of Arms Control and Disarmament Agency, and as a Deputy Assistant Secretary of State in the Bureau of Intelligence and Research.

Nicholas Bambos is Associate Professor of Engineering Economic Systems and Operations Research at Stanford University. His specialties are modeling and simulation and computer security.

William Crowell is Deputy Director of the National Security Agency, where he acts as the Agency's chief operating officer, guiding and directing strategies and policy, and serving as the principal advisor to the Director. He is also principal technical advisor to a cabinet-level committee charged with developing the national policy on encryption.

Paul Edwards is assistant professor in the Science, Technology and Society Program at Stanford. His studies include a history of the impact of the information technolgies during the Cold War.

David Elliott was Staff Director for Science and Technology at the National Security Council and then Vice President at SAIC and SRI. He is now "retired."

Edward Feigenbaum is Chief Scientist of the U.S. Air Force. Before that he was Professor of Computer Science at Stanford University, where he is best known for his work in artificial intelligence, and especially for expert systems.

David Friedman is Professor of Law and Economics at Santa Clara University. He has a special interest in the law and economics of Internet commerce.

John Gage is a founder of Sun Micosystems and Chief Scientist. His interests span a wide range of public policy issues including encryption, export controls, and electronic commerce.

Seymour Goodman heads the Information Technology and International Security Program at CISAC at Stanford and is Professor of MIS at the University of Arizona. He studies the international dimensions of IT and related public policy issues.

Lawrence Greenberg was a counsel with the NSA and Wilson, Sonsini, Goodrich & Rosati, and is now General Counsel for The Motley Fool, Inc. His principle interest is in IT-related law.

Richard Gronet is Section Leader for the Proliferation Assessment Section, International Assessments Division at LLNL. He has held executive positions responsible for intelligence and policymaking at the Departments of State and Defense and ACDA.

Richard Hundley is Acting Director of the Acquisition and Technology Policy Center at the RAND Corporation. His recent research has centered on the emerging security challenge confronting society in "cyberspace."

Ronald Lehman is Director of the Center for Global Security Research at LLNL. Previous positions include: Director of the U.S. Arms Control and Disarmament Agency, Assistant Secretary of Defense (International Security Policy), and Deputy Assistant to the President for National Security Affairs.

Stephen 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.”

Michael May is Co-Director of CISAC and a Professor of Engineering Economic Systems and Operations Research at Stanford. He is Director-Emeritus of LLNL. He studies a wide variety of national and international security issues concerned with energy and weapons of mass destruction.

Roger Pajak is the Senior Advisor for Counterterrorism at the Department of the Treasury and is Treasury's representative on the Critical Infrastructure Protection Task Force.

William Perry is a former Co-Director of CISAC and has held several very senior positions with the Department of Defense, recently stepping down as Secretary of Defense. He has a long and distinguished history of involvement with American high technology industry in many capacities.

Fernand Sarrat has been CEO of Cylink, Inc. since November, 1996. Prior to that, he was with IBM for 22 years, where his last position was General Manager for Network-centric Computer Marketing and Services.

Stan Trost is Director of the Center for Advanced Information Technology at LLNL. He was formerly head of electronics engineering there, and chaired the IEEE Committee on Communication and Information Policy.

Hal Varian is Dean of the School of Information Management and Systems at the University of California, Berkeley. He also holds appointments in the Haas School of Business and the Department of Economics. He studies IT-related economic issues.

Edward Zajac is professor of economics at the University of Arizona. He was formerly Director of Economics for AT&T, and continues to specialize in the economics of regulation of the telecommunications industry.

Edward Zeitler is Senior Vice President of Charles Schwab, Inc.

List of Participants

Name	Affiliation
Janet Abrams	PCCIP Staff
Robert Anderson	RAND
Ken Arrow	Stanford
Kathleen Bailey	LLNL
Nick Bambos	Stanford
François Bar	Stanford
Paul Baran	Com21, Inc.
Dave Bernstein	Stanford
Tom Berson	Anagram Laboratories
Matt Bishop	University of California at Davis
Stewart Brand	GBN
George Bunn	Stanford
Jean Camp	Sandia
Piper Cole	Sun Microsystems
Guy Copeland	CSC and ITAA
William Crowell	National Security Agency
Mary Culnan	PCCIP
Peter Daly	PCCIP
Fred Davidson	PCCIP Legal Staff
John Davis	PCCIP
Les Denend	Network General Corp
Paul Edwards	Stanford
Dave Elliott	NSC/SAIC/SRI (Retired)
Ed Feigenbaum	Stanford
David Friedman	Santa Clara University
John Gage	Sun Microsystems
Dee Goodman	CISAC Staff
Sy Goodman	Stanford and Arizona
Lawrence Greenberg	The Motley Fool

Adrienne Griffen	PCCIP Staff
Dick Gronet	LLNL
Kevin Harrington	CISAC Staff
John Heimann	Oracle
John Hiles	Thinking Tools
Don Howe	National Security Agency
Richard Hundley	RAND
Anita Jones	University of Virginia
Dave Jones	PCCIP
Andy Kuchins	Stanford
Jim Kurtz	PCCIP Staff
Ray Leadabrand	Leadabrand Associates
Ron Lehman	LLNL
Karl Levitt	University of California at Davis
Herb Lin	NRC
Ted Linden	MCC
Stephen Lukasik	DARPA/FCC/Northrop (Retired)
Ken Malpass	CISAC Staff
Tom Marsh	PCCIP
Mike May	Stanford
Tom McInerney	BENS
Steve Mitchell	PCCIP
Joe Mitola	National Security Agency
Kathryn Moir	BENS
Martin Morf	Stanford
Peter Neumann	SRI
Donn Parker	SRI
Roger Pajak	US Treasury Department
William Perry	Stanford
Paul Rodgers	PCCIP
Michael Rostoker	Kawasaki Microelectronics
Jeff Rulifson	Sun Microsystems
Banani Santra	CISAC Staff
Fernand Sarrat	Cylink Corp
Jim Schindler	Hewlett Packard Lab
Donald Scott	GTE
Jeannie Seelbach	TRW
Wayne Shotts	LLNL
Howard Shrobe	MIT/DARPA
Ron Skelton	EPRI
Kevin Soo Hoo	RAND
George Spix	Microsoft
Fred Struble	PCCIP
David Swanson	Edison Electric Institute
Stan Trost	LLNL
Hal Varian	UC Berkeley
Dean Wilkening	Stanford

Prescott Winter	National Security Agency
Nancy Wong	PCCIP
John Woods	TRW
Edward Zajac	University of Arizona
Ed Zeitler	Charles Schwab

Center for International Security and Arms Control

Stanford University

Please send orders to: Publications, Box P, 320 Galvez Street, Stanford, California 94305-6165. Enclose check payable to Stanford University. Add $2.00 postage and handling for first item ordered ($5.00 for overseas delivery), $1.00 for each additional item. Foreign orders must be in U.S. dollars and drawn on a financial institution with branches in the United States. California residents, add appropriate sales tax.

Center reports, working papers, and reprints

NEW Herbert L. Abrams. *Can the Nation Afford a Senior Citizen As President? The Age Factor in the 1996 Election and Beyond*. 1997 (28 pages, $6.00).

Herbert L. Abrams and Dan Pollack. *Security Issues in the Handling and Disposition of Fissionable Material.* 1993 (27 pages, $5.00).

Assessing Ballistic Missile Proliferation and Its Control. 1991 (181 pages, $14.00; summary, $3.00).

Andrei Baev, Matthew J. Von Bencke, David Bernstein, Jeffrey Lehrer, and Elaine Naugle. *American Ventures in Russia.* Report of a Workshop on March 20-21, 1995, at Stanford University. 1995 (24 pages, $7.00).

NEW Michael Barletta, *The Military Nuclear Program in Brazil.* 1997 (38 pages, $8.00)

David Bernstein. *Software Projects in Russia: A Workshop Report*. 1996 (28 pages, $7.00).

David Bernstein, editor. *Defense Industry Restructuring in Russia: Case Studies and Analysis*. 1994 (244 pages, $14.00).

NEW David Bernstein, editor. *Cooperative Business Ventures between U.S. Companies and Russian Defense Enterprises*. 1997 (332 pages, $18.00).

George Bunn. *Does the NPT require its non-nuclear-weapon members to permit inspection by the IAEA of nuclear activities that have not been reported to the IAEA?* 1992 (12 pages, $4.00).

General George L. Butler, Major General Anatoli V. Bolyatko, and Scott D. Sagan. *Reducing the Risk of Dangerous Military Activity*. 1991 (39 pages, $6.00).

Irina Bystrova. *The Formation of the Soviet Military-Industrial Complex*. 1996 (28 pages, $6.00).

NEW Jor-Shan Choi, *A Regional Compact Approach for the Peaceful Use of Nuclear Energy—Case Study: East Asia* (65 pages, $9.00)

Cooperative Security in Northeast Asia (text in English and Russian). 1993 (17 pages, $4.00).

John Deutch. *Commercializing Technology: What Should DOD Learn from DoE?* 1990 (10 pages, $4.00).

John S. Earle and Saul Estrin. *Employee Ownership in Transition*. 1995 (53 pages, $10.00).

John S. Earle and Ivan Komarov. *Measuring Defense Conversion in Russian Industry*. 1996 (40 pages, $7.00).

Lynn Eden and Daniel Pollack. *Ethnopolitics and Conflict Resolution*. 1995 (21 pages, $5.00).

David Elliot, Lawrence Greenberg, and Kevin Soo Hoo. *Strategic Information Warfare—A New Arena for Arms Control?* 1997 (16 pages, $3.00).

Anthony Fainberg. *Strengthening IAEA Safeguards: Lessons from Iraq*. 1993 (64 pages, $6.00).

NEW Geoffrey E. Forden. *The Airborne Laser: Shooting Down What's Going Up*. 1997 (20 pages, $6.00)

James E. Goodby. *Can Strategic Partners Be Nuclear Rivals?* (First in a series of lectures on *The U.S.–Russian Strategic Partnership: Premature or Overdue?*) 1997 (26 pages, $6.00).

James E. Goodby. *Loose Nukes: Security Issues on the U.S.–Russian Agenda* (Second in a series of lectures on *The U.S.–Russian Strategic Partnership: Premature or Overdue?*) 1997 (20 pages, $6.00).

James E. Goodby. *NATO Enlargement and an Undivided Europe* (Third in a series of lectures on *The U.S.–Russian Strategic Partnership: Premature or Overdue?*) 1997 (16 pages, $6.00).

NEW James E. Goodby and Harold Feiveson (with a foreword by George Shultz and William Perry). *Ending the Threat of Nuclear Attack*. 1997 (24 pages, $7.00).

Seymour Goodman. *The Information Technologies and Defense: A Demand-Pull Assessment*. 1996 (48 pages, $9.00).

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*. 1997 (48 pages, $8.00).

NEW Yunpeng Hao. *China's Telecommunications: Present and Future*. 1997 (36 pages, $7.00).

John R. Harvey, Cameron Binkley, Adam Block, and Rick Burke. *A Common-Sense Approach to High-Technology Export Controls*. 1995 (110 pages, $15.00).

John Harvey and Stefan Michalowski. *Nuclear Weapons Safety and Trident*. 1993 (104 pages, $12.00; summary $2.00).

Ji, Guoxing. *Maritime Security Mechanisms for the Asian-Pacific Region*. 1994 (25 pages, $5.00).

Leonid Kistersky. *New Dimensions of the International Security System after the Cold War.* 1996. (34 pages, $8.00)

Amos Kovacs, *The Uses and Nonuses of Intelligence*. 1996 (68 pages, $10.00).

Allan S. Krass. *The Costs, Risks, and Benefits of Arms Control*. 1996 (85 pages, $8.00).

Gail Lapidus and Renée de Nevers, eds. *Nationalism, Ethnic Identity, and Conflict Management in Russia Today*. 1995 (106 pages, $12.00).

George N. Lewis, Sally K. Ride, and John S. Townsend. *A Proposal for a Ban on Nuclear SLCMs of All Ranges*. 1989 (13 pages, $5.00).

John Lewis and Xue Litai. *Military Readiness and the Training of China's Soldiers*. 1989 (37 pages $9.00).

Stephen J. Lukasik. *Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure*. 1997 (40 pages, $7.00).

NEW Kenneth B. Malpass et al. *Workshop on Protecting and Assuring Critical National Infrastructure*. 1997 (64 pages, $10.00).

John J. Maresca. *The End of the Cold War Is Also Over*. With commentaries by Norman M. Naimark, Michael May, David Holloway, Arthur Khachikian, Daniel Sneider, and Renée de Nevers. 1995 (60 pages, $8.00).

Michael May. *Rivalries Between Nuclear Power Projectors: Why the Lines Will Be Drawn Again*. 1996 (20 pages, $7.00).

Michael May and Roger Avedon. *The Future Role of Civilian Plutonium*. 1994 (22 pages, $6.00).

Michael May and Roger Speed. *The Role of U.S. Nuclear Weapons in Regional Conflicts*. 1994 (24 pages, $5.00).

Michael McFaul, ed. *Can the Russian Military-Industrial Complex Be Privatized?* 1993 (60 pages, $6.00).

Captains Moreland, Ota, and Pan'kov. *Naval Cooperation in the Pacific: Looking to the Future*. 1993 (21 pages, $4.00).

Robert F. Mozley. *Uranium Enrichment and Other Technical Problems Relating to Nuclear Weapons Proliferation*. 1994 (64 pages, $9.00).

Thomas Nash. *Human-Computer Systems in the Military Context*. 1990 (32 pages, $6.00).

Wolfgang K.H. Panofsky. *Do We Need Arms Control If Peace Breaks Out?* (lecture). 1990 (9 pages, $4.00).

M. Elisabeth Pate-Cornell and Paul S. Fischbeck. *Bayesian Updating of the Probability of Nuclear Attack*. 1990 (24 pages, $6.00).

William J. Perry. *Defense Investment: A Strategy for the 1990s*. 1989 (43 pages, $9.00).

Scott D. Sagan, ed. *Civil-Military Relations and Nuclear Weapons*. 1994 (163 pages, $12.00).

Scott D. Sagan and Benjamin A. Valentino. *Nuclear Weapons Safety after the Cold War: Technical and Organizational Opportunities for Improvement* (text in English and Russian). 1994 (25 pages, $5.00).

Capt. Alexander Skaridov, Cmdr. Daniel Thompson, and Lieut. Cmdr. Yang Zhiqun. *Asian-Pacific Maritime Security: New Possibilities for Naval Cooperation?* 1994 (28 pages, $5.00).

Song, Jiuguang. *START and China's Policy on Nuclear Weapons and Disarmament in the 1990s*. 1991 (29 pages, $5.00).

Konstantin Sorokin. *Russia's Security in a Rapidly Changing World*. 1994 (95 pages, $10.00).

Roger D. Speed. *The International Control of Nuclear Weapons*. 1994 (59 pages, $11.00).

István Szönyi. *The False Promise of an Institution: Can Cooperation between OSCE and NATO Be a Cure?* 1997 (34 pages, $6.00).

NEW Xiangli Sun. *Implications of a Comprehensive Test Ban for China's Security Policy*. 1997 (24 pages, $7.00)

Terence Taylor. *Escaping the Prison of the Past: Rethinking Arms Control and Non-Proliferation Measures*. 1996 (65 pages, $10.00)

Terence Taylor and L. Celeste Johnson. *The Biotechnology Industry of the United States. A Census of Facilities*. 1995 (20 pages, $7.00).

MacArthur Consortium Working Papers in Peace and Cooperation

Pamela Ballinger. *Claim-Making and Large-Scale Historical Processes in the Late Twentieth Century*. 1997 (52 pages, $7.00).

Tarak Barkawi. *Democracy, Foreign Forces, and War: The United States and the Cold War in the Third World*. 1996 (40 pages, $6.00).

Byron Bland. *Marching and Rising: The Rituals of Small Differences and Great Violence in Northern Ireland*. 1996 (32 pages, $6.00).

Charles T. Call. *From "Partisan Cleansing" to Power-Sharing? Lessons for Security from Colombia's National Front*. 1995 (60 pages, $7.00).

David Dessler. *Talking Across Disciplines in the Study of Peace and Security: Epistemology and Pragmatics as Sources of Division in the Social Sciences*. 1996 (40 pages, $7.00).

Lynn Eden and Daniel Pollak. *Ethnopolitics and Conflict Resolution*. 1995 (21 pages, $5.00).

Daniel T. Froats, *The Emergence and Selective Enforcement of International Minority-Rights Protections in Europe after the Cold War*. 1996 (40 pages, $7.00).

Robert Hamerton-Kelly. *An Ethical Approach to the Question of Ethnic Minorities in Central Europe: The Hungarian Case*. 1997 (34 pages, $6.00).

Bruce A. Magnusson. *Domestic Insecurity in New Democratic Regimes: Sources, Locations, and Institutional Solutions in Benin*. 1996 (28 pages, $6.00).

John M. Owen. *Liberalism and War Decisions: Great Britain and the U.S. Civil War*. 1996 (22 pages, $5.00).