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

March 10–11, 1997

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

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

July 1997

Kenneth B. Malpass is a Ph.D. candidate in the Department of Engineering–Economic Systems and Operations Research at Stanford University. Kevin J. Harrington is a Ph.D. candidate in the Department of Physics at Stanford University. David Elliott was Staff Director for Science and Technology at the National Security Council and then Vice President at SAIC and SRI. Kevin Soo Hoo is a Ph.D. candidate in the Department of Engineering–Economic Systems and Operations Research at Stanford University. Seymour 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.

Printed in the United States of America

ISBN 0-935371-47-8

Contents

1.0 Introduction

In July 1996, President Clinton established the Commission on Critical Infrastructure Protection, with a charter to designate critical infrastructures and 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 gives examples of critical infrastructures (telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government), and also notes 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 recognizes 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 by security specialists at infrastructure organizations, research companies, and the national laboratories. The results of this two-day meeting are summarized 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

2.0 Executive Summary

In July 1996, President Clinton issued an executive order creating the Presidential Commission on Critical Infrastructure Protection (PCCIP), commissioning a one-year study of actions needed to protect critical national infrastructures. The order initially identified eight critical infrastructures to be considered with regard to both physical and cyber threats:

i Telecommunications
ii Electrical power systems
iii Water supply systems
iv Emergency services
v Transportation
vi Banking and finance
vii Gas and oil storage and transportation
viii Continuity of government

On March 10–11, 1997, the Center for International Security and Arms Control at Stanford University and the Center for Global Security Research at LLNL hosted members of the PCCIP and sixty representatives from industry, universities, and national laboratories to evaluate the issues. The workshop limited its focus to organized information technology based threats and needed responses. These threats include terrorism, organized crime, and state-sponsored attacks. A second workshop is planned for July 21–22, 1997.

Conclusions from the March workshop:

Real vulnerabilities exist. The amalgamated nature of large infrastructure systems (especially older "legacy" systems, new systems with bugs, lazy organizational policies, and interfaces between different systems) opens the door to many types of penetration. The increasing interlinking of all computer and telecommunications control systems raises the specter of cascading system failure, not only in the United States but globally. Broader agreement is needed on priorities and probabilities before action will gather broad support. The most pressing need is an agreed-upon delineation of exposure and the priorities for effective response.

Devastating scenarios can be imagined, but reality checks are needed to maintain perspective. Many events have occurred to guide analysis of this topic, including software glitches, natural disasters, carelessness, and accidents. Organizations have response teams for emergencies, and they run practice drills to prepare for things that have happened in the past. Very little preparation has been made for unprecedented situations, however, and new thinking and new mechanisms are required.

Industry participants advise cautious, cooperative steps. While the general problem is of concern, any discussion about specific vulnerabilities or responses met with a range of opinion as to how big the problem is and whose problem it is. With most infrastructures owned and operated by the private sector, no plan to address the problem has a chance of succeeding without the active participation of industry.

Roles and responsibilities are a central area needing agreement. Responses to "organized threats" require cooperation from privately owned infrastructure companies, technology vendors and system integrators, law enforcement (at every level of government), national security and intelligence organizations, and transnational institutions. No agreement exists on the responsibility for alerting others, acknowledging losses, protecting interdependent systems, or paying for responses before, during, and after an attack.

Cooperation is needed at all levels of government, here and abroad, to formulate necessary responses and to coordinate information sharing, law enforcement, deterrence, and pursuit of attackers. Infrastructure is developing worldwide similarities. Information technologies for infrastructure are increasingly standardized in hardware, software, equipment, and vulnerabilities. Attackers are connected globally to targets. A difficulty is that information attacks can be launched on a low budget by independent organizations, small groups, or even individuals. Law enforcement, intelligence, and private groups in many countries each have fragments of the whole picture. Issues of company defensiveness, military and commercial secrecy, national pride, fear of panic, and fear of imitation are involved.

Past examples of government/industry responses to other threats were surveyed and may yield useful insights to guide the work of the Commission. The National Security Telecommunications Advisory Committee (NSTAC) was cited as an example of successful cooperation in the telephone industry.

Legal institutions are as yet largely untested as a tool for improving protection and allocating risk and loss among participants. Many speakers voiced concern that mandates could not achieve the necessary level of preparedness and investment in training and systems to protect critical assets. However, no clear consensus emerged as to what incentives would be effective, how much they would cost, or who is to provide them. Tax incentives and regulatory changes were touched upon, but at this early stage no plan has been articulated. The role of the judiciary was compared with the role of legislation in addressing new technologies and problems. The courts can respond to specific situations, assess liability, and signal how responsibility for action will be imputed to institutions. Although legal institutions tend to respond to events rather than anticipating them, they can evolve effective mechanisms for adjusting the rules of the game.

The insurance system of liability and risk-based premiums could play a leading role in communicating to industry the value of prevention. The insurance companies have been hesitant to write information-loss policies, however. There are at least three barriers to making this coverage a prime vehicle for encouraging "best practices" by all businesses:

i Lack of actuarial experience with information losses,
ii Difficulty or lack of experience in placing a value on information-driven losses, and
iii Lack of accepted industry-wide best practices for protecting information in storage, in transit, and in use.

The government was urged to subsidize insurance, like flood insurance, together with a private-sector effort to determine “best practices” for IT security and to base insurance coverage on those practices.

Better statistics are needed. More attention should be given to assembling accurate and well-defined statistics on current hazards faced by infrastructure assets. Organizing these data in a consistent manner will facilitate risk assessment by industry, insurance companies, law enforcement, and the defense establishment. Information sharing is made easier and more meaningful if standards for reporting attacks and losses (both direct and indirect) are agreed upon. These tasks are complicated by (1) the absence of clear lines of institutional responsibility for such information gathering, and (2) the fact that system security is in a continuous state of change and hence past statistics may provide only limited guidance for the future.

Modeling and simulation can be important tools and test beds to assist in understanding stressed-system behavior, the effectiveness of proposed protective measures, cost-benefit trade-offs, and vulnerabilities, and to explore for unexpected interactions of large networked systems.

Priority areas are telecommunications and electrical power distribution. The reason for this is that all infrastructures share these core infrastructures in order to operate. A case study of IT-based telecommunications would benefit all infrastructure operators and responsible institutions. Finance and banking have unique, and high priority, vulnerabilities as well.

Educational efforts are required to include the public, business, standard-setting bodies, state regulatory officials, and research organizations in the process. An awareness of the long-term dynamics of the problem is necessary to develop appropriate responses. Since this is a largely undefined policy area, education is necessary to motivate action from government, industry, and the public at large. Infrastructure owners are a logical starting place, along with IT professionals.

Technology is not the long pole in the tent. The critical tasks are awareness, understanding of network complexity and interdependence, education, training, and organizational commitment.

Analytical categories were described to allow further work to be systematized and coordinated. One approach, developed in detail in a companion publication to this report (see Stephen J. Lukasik, *Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure*, CISAC, May 1997), structured responses according to:

- Types of infrastructure
- Information subsystems subject to attack
- Strategies for protection: prevention, damage limitation, and reconstitution
- Nature and scale of attack
- Responsibilities: public, private, and cooperative
- Priorities for public initiatives
- Minimizing government intervention

3.0 Summaries of Proceedings

Assuring the critical infrastructure: A public/private sector challenge

R. Tom Marsh

The Commission's mandate is to assess the vulnerabilities of, and threats to, the nation's infrastructure, to identify the relevant legal and policy issues, to recommend national policy and strategy for protecting the country from both physical and cyber attacks, and to recommend regulatory and policy changes necessary for implementation.

The ancient Roman government built fifty thousand miles of roads, and these roads subsequently became its undoing when attacking barbarians used them to invade Rome. Then, as now, a nation's infrastructure could be used to topple it. Increasing channels of communication may be used to facilitate terrorism and also to penetrate its cybersystems, especially by insiders. With our increased reliance on IT throughout the economy, increased interdependence of infrastructure systems, and increased vulnerabilities of the various infrastructures, we are on the road to catastrophe. The tools available to exploit these vulnerabilities are increasing exponentially, and are available to amateurs. Infrastructures are also becoming more vulnerable to state-sponsored terrorism—vulnerability is increasing across the spectrum of threats, from the least supported hacker to the most organized terrorist.

While offensive tools proliferate, there remains a serious lack of tools to detect and defend against cyber attack. We need warning of possible attacks, real-time identification of attacks as they occur, and ways to respond. Technology is a bigger part of the problem, and will be a bigger part of the solution, than we at first thought.

The interdependency of infrastructures has almost become their defining characteristic. With interdependence comes growing complexity, creating a need for new risk models. Can the marketplace anticipate and manage these risks? Will some form of government action be required? If so, how? Should the government create tax incentives for increasing infrastructure assurance? Should government underwrite assurance efforts, perhaps through interest-free loans?

Many legal questions arise in this new environment. Who should pay if service is interrupted? How does the deregulation of certain infrastructures affect this question? If infrastructure providers are liable for a lack of assurance, should assurance standards be established to determine such liability, and who should establish them? If they are mandated, who should enforce them? Will this provide openings for insurance? Should new regulations be adopted to increase the degree of assurance, though tight regulatory environments seem to discourage private-sector investment, such as with public utilities?

Information sharing about these problems is needed between government and the private sector. There is a great danger in sharing information, but a greater danger in not sharing it. While we need to protect classified information and private-sector information involving reputation, consumer confidence, and liability, the challenge of the Commission is to forge a partnership between government and private industry. To do this, we need to raise the awareness of industry leaders. Whatever we do, we will be seeking private sector buy-in of our findings and recommendations, as the quality of these recommendations is only as good as the buy-in from the private sector that we achieve.

The capability to do damage: Perspectives on vulnerabilities and threats
Brenton Greene

The sources of vulnerabilities to infrastructure may be summarized under seven categories:

i New technologies
ii Interdependencies
iii Complexities
iv Deregulation
v Single point failure potential
vi Information access
vii Globalization and foreign ownership

New technologies are creating new or expanded vulnerabilities via common operating systems, open architectures, and large software packages with millions of lines of code and minimal ability to identify a few bad lines of code or who wrote it.

Gas and electric utilities are vulnerable to interdependent system failure, especially with systems whose availability is taken for granted. For example, gas utilities are vulnerable to disruption by intrusion into their control systems via the public switched network, a system they are taking for granted and for whose security flaws they have no special expertise. Such companies are five to ten years behind the telecommunications companies in implementing security measures. The failure of the electric power grid in the Pacific Northwest and California in the summer of 1996 was a failure combining system interdependency and system complexity. Perhaps a small investment in a better control system might have prevented the large costs of systemwide collapse. As deregulation decreases the profit margins for utilities, fewer resources are available for security investment, resulting in limited private sector buy-in; therefore, a more compelling case must be made to these companies that they should make such investments.

"Single point failure" exposure already exists in several systems, and the information for how to exploit systems at such points is widely available. It is possible to purchase local exchange routing guides and CD-ROMs that list all the telecommunication switches in the U.S. Two sites listed in the latter show that a car bomb attack on either could disable all telecommunications in New York City until the physical damage to the wiring and buswork can be repaired or replaced. Ninety-five percent of DoD communications are sent on insecure, public networks that have not been evaluated for the possibility of denial of service. The international submarine cables can easily be cut by a trawler, and the locations of where these cables come ashore are given regularly to mariners. On land, it is possible to cut just a few cables and deny service to major U.S. cities. [Peter Neumann added that the ARPAnet in the 1980s and the 1990 AT&T collapses were both single-node failures that propagated globally and, although accidental, could have been triggered intentionally if someone desired to do so.]

The trend toward globalization of ownership of IT corporations signaled by the British Telecom/MCI merger also tends to globalize the vulnerabilities, and points to the need for bilateral or international security standards and extradition and jurisdictional agreements on those security standards. The increasing points of vulnerability include common technology worldwide, interfaces between dissimilar systems, and the problem of large systems being dependent on the weakest link in the chain (shared access by many people and systems).

Ray L. Leadabrand

Hardware disruption technologies are potentially as devastating as software (hacker) disruption methods. The Commission should not neglect conventional electronic warfare techniques, or new technologies such as ultra-wide band (UWB) radio frequency (rf) impulse signals. The latter capabilities were discussed in detail.

UWB rf signals have carrier frequencies of 50 to 2,000 MHz but are on the order of one rf cycle in length. This very short pulse can have very high peak power (in the megawatt range). Because of fundamental Fourier transform limits, the pulses also have very wide bandwidths, which can be several GHz. Power Spectra Inc. (PSI) holds a patent on a technology called BASS (Bulk Avalanche Semiconductor Switch) that can be used to generate these UWB signals. BASS is based on the discovery that solid-state chips of gallium arsenide (GaAs) will become a short circuit in a few picoseconds when illuminated by a diode laser. When such chips have 10–12 thousand volts momentarily placed across them and this laser-diode activated “switch” is put in a simple rf circuit, the avalanche of current that flows when the chip becomes conductive produces on the order of a megawatt of rf power. A single BASS module is about 2x2x6 inches in size and weighs less than a pound. To function it requires only a trigger generator and a battery. The modules can produce repeated UWB pulses with a pulse repetition frequency (PRF) of tens of kHz. PSI has also licensed Russian “Thyrister” technology with smaller peak power (100 kW) but with higher PRFs of 100 kHz. These modules are even smaller: ½x½x2 inches. If these individual switches are put in an antenna array and triggered with precision timing, the combined pulse produced can have peak power levels of up to one gigawatt. They can be phased, analogously to a phased array antenna, so that the beam can be steered over a 60-degree angular cone. With gigawatt peak power capability, it is possible to disrupt electronic apparatus at some distance.

UWB signals disrupt electronic equipment by garbling internal electronic signals with the spurious signals they introduce into the data stream, causing the system to malfunction in unpredictable ways. The disruption may last only while the UWB signal is present, or in more severe cases system rebooting may be required to restore operability. UWB signals may be more disruptive if their pulse repetition frequencies correspond to the internal clock frequencies of the equipment. Their wide bandwidth appears to enhance their capability to match an internal frequency spectrum that will disrupt the hardware.

Export of this technology is currently not prohibited, as there are potentially beneficial uses for it, including high-penetration radars, covert communication, and law enforcement uses such as the disabling of the electronic systems of automobiles being pursued by police. Because terrorist groups can afford to purchase these transmitters, close monitoring of the international proliferation of this technology should be encouraged.

Peter Neumann

To a first approximation, every computer in the world is connected to every other computer in the world. The security problem posed by global connectivity is made worse by the near-universal use of “garbageware,” software that is riddled with security holes: Java, Active-X, Microsoft Word, Web browsers, Web servers, operating systems, database software, firewalls, and networks are examples. We have nothing but weak links in the chain of software making up the nation’s information infrastructure.

Vendors are not producing software with adequate security, and the government doesn’t do a good job of procuring software: the FAA air traffic control system, which took a decade of work, just went down the tubes at a cost of billions of dollars; the NCIC 2000 fingerprinting system just went down the tubes at a cost of millions of dollars; the IRS tax modernization system just went down the tubes at a cost of $4–6 billion. The vendors are producing “garbageware,” lowest-common-denominator systems, but the government is no longer in the position to purchase custom software that overcomes these problems. As a result we have a situation in which both the government and private industry seem unable to produce good software systems with good security measures.

We have so far been lucky not to have seen attacks on infrastructure that could create large-scale disruption and denial of service. Most software attacks so far have been fairly benign and perpetrated by teenage hackers trying to prove that they can break things. Large-scale disruptions produced accidentally, such as the 1980 ARPAnet collapse and the 1990 AT&T long-distance telecom collapse, could both have been triggered intentionally had someone desired to do so (and both were single-node failures that propagated globally). Other systems look like accidents, or attacks, waiting to happen: a security analysis for a pipeline company some years ago showed that the same maintenance password was used on every node in the entire network, and used by every other maintenance person who worked on that network nationwide. The telephone switches until recently had the same problem; they were using the same maintenance password, and “the kids” knew the password and were getting into the system.

Recent problems have shown up in encryption systems: well-known security analyst Ross Anderson tricked a smart card into revealing its keys, and a recently discovered attack on a particular implementation of public-key cryptography showed that the private key can be derived as the difference between a slightly faulted version and the correct version, with the difference having the private key as a factor. There are defenses to these threats. Research is important for risk assessment and for education. Cryptographically generated one-time passwords would go a long way toward solving network security problems.

In summary, significant risks exist and need to be addressed. Our defenses against isolated attacks and unanticipated events are inadequate; our defenses against large-scale coordinated attacks are even more inadequate. Cryptography is an absolutely essential ingredient in achieving confidentiality, user authentication, system authentication, information integrity, and nonrepudiability. The U.S. encryption export policy has generally not been sufficiently oriented toward improving the infrastructure, in that it has been more concerned with limiting the use of strong encryption. U.S. encryption policy has acted as a deterrent to better security.

Potential technologies for improving security and aiding law enforcement
David Cooper

Suppose a disgruntled opponent of the National Ignition Facility (NIF) at LLNL tries to break into the computer network at LLNL to redirect the powerful laser beams it uses to ignite nuclear fusion in such a manner as to destroy the facility. He finally succeeds in breaking in because a new employee uses the password "enterprise"—one of the ten or twelve most commonly used passwords. An expert system comprised of genetic algorithms, AI, and neural nets detects the break-in by noting the unusual pattern of computer use of this intruder and alerts the computer security officer, who then drops him into a high-fidelity virtual facility that mimics the NIF control system, while tracing back to determine the identity of this intruder and making his arrest.

How realistic is this? Replace the NIF with any large financial institution, and the goal of vandalism with that of theft, and it is clear that this is a realistic threat. In such a case, it is clearly worthwhile to create a system similar to that proposed for the NIF's security.

Other questions: Can such technology be developed? Should we be seeking such a sophisticated level of threat response? Do we have the will to commit the necessary funding? Will we allow our computing environments to be so fully monitored? What level of operational control must we sacrifice? What performance penalties must we pay, in computing and networking? Are the legal hurdles to doing this surmountable? Will we need international buy-in?

No matter what your opinion on these issues, we all admit that the world of networked computing is fragile and vulnerable. Most systems have little or no protection, and such protection is misunderstood and underappreciated. It is difficult for system administrators to stay ahead of the intruders into their systems, and the losses are already staggering (estimates for 1995 are $10–50 billion, and this is probably conservative). There is constantly increasing pressure to minimize and reduce system costs. This is accompanied by growing system size, complexity, and user dependence, and such users are increasing their demand for more access and services while resisting attempts to require the implementation of security measures.

To make meaningful progress toward implementing a structured, coherent security and protection program, widespread cooperation and determination will be needed. Any viable program must address the following elements: deterrence, detection, response, and pursuit.

Deterrence: Most protection efforts to date have focused on this. Methods include authentication systems, firewalls [Peter Neumann says no "good" firewalls exist, but Cooper thinks that significant progress has been made in improving these], data access controls, system usage monitors (expert systems could be used to do this), encryption, and system vulnerability scanners. Many of these tools exist, but the vast majority of computer systems and networks do not utilize them, jeopardizing their own systems and all interconnected ones as well.

Detection: There has been recent interest in this, and some products have been developed. These include virus scanners (drawback: about ten thousand viruses are known to exist, the number is growing all the time, and scanners only catch the old ones), network scanners that look for strange activity, hacking signatures, and forensics (user profiling and system usage profiling that sets off alarms if unusual patterns are detected). Other than virus scanners, there has been little interest in utilizing these tools. Some interesting R&D is being done with artificial intelligence, neural nets, and genetic algorithms, but current results are mostly embryonic, and these approaches appear to lack upward scalability and portability.

Response: Most response is administrative rather than technical; little technical research has occurred. It is difficult, for example, to drop an intruder into a virtual system mimicking the real one without the intruder detecting this. Resources will need to be invested in response technologies if we are to move beyond the current mind-set of getting the hackers out of our systems or preventing them from intruding to actually being able to catch them. This is insufficient because the intruder will simply target other systems or return later after further study of the original target's vulnerabilities.

Pursuit: Is it our goal to catch intruders? If so, we must develop sophisticated tools for tracking them. We must agree to allow footprints in our systems to be explored, especially if they are using the system as a gateway to another system. There is little automation of this process at present, and human-intensive, manual efforts are replete with legal ramifications, some of which may be unsolvable. Certifiable network source addresses are essential, requiring standardization of these. Little technical work has been devoted to pursuit; the goal is usually limited to just getting the hackers out of the system and keeping them out.

There are a variety of technical needs. One such is technology for securing legacy systems that are large and complex, and thus expensive to replace with newer, more secure systems. Technologies that can be applied in an incremental or evolutionary way, and that can be implemented "late in the game," are most marketable and appealing, although the ideal is to design security into a system before it is built, instead of "retrofitting" it later. With many systems, it is already late in the game, implying that more demand for such solutions exists. For new systems, system engineering and integration are the keys to success in designing protection systems.

The elements of a protection program include technology, but an exclusive focus on technology would be an error. Organized cooperation in response to incidents is also vital. While we are justifiably operating in the parochial interests of our own organizations, the threat is global, and if we are establishing local policies, procedures, and technical responses without coordination with the rest of the community, the problem will not be solved. If some banks are more secure than others, the insecure ones will get most of the attention of the hackers. Some kind of collective action may be needed to get us out of this incentive trap.

We must increase awareness on the part of corporate personnel managers who are currently oblivious, in the main, to the threat to their systems posed by disgruntled insiders. A large fraction of insider computer mischief is promulgated by employees who continue to have access to computer systems after being given notice of termination. This practice must be changed.

How do we get there from here? It will take a lot of money, time, and unprecedented cooperation (perhaps even international cooperation). An effective protection program will impact computer communications and productivity. The bottom-line questions we must ask are: Can we afford to do it? Do we have the resolve? Can we afford not to do it?

Q: Most of the evidence of cost is anecdotal. Are there any hard numbers?

A: Off the record, a San Francisco chief information officer said his bank lost $100 million in 1996, but is proud that no headlines were seen to this effect.

Q: Did this executive initiate a program to stop this problem?

A: Yes.

Q: Most of these loss figures are squishy and somewhat self-serving. What is the solidity of the $50 billion loss figure for the last year?

A: Only as solid as the figures reported by the FBI. These do not include the costs due to disruption.

Audience comment: No loss figures of computer crime are valid. They are nonsense. We should stop using these figures.

Q: Experience shows that security needs to be built in from the beginning; retrofits are not easy or successful.

Audience answer: SSL was a retrofit and is successful. Firewalls aren't 100 percent effective, but are an efficient element in a comprehensive system of computer security.

Q: Part of the problem can be solved by encryption. The Israelis account for 55 percent of the security products sold in the U.S. Why aren't they, or someone else, selling Netscape plug-ins that implement encryption? Why hasn't PGP, Inc. sold a plug-in for Netscape?

Audience answer: If they can't export it, there is reduced economic value in making the software.

Counter: Then why don't the Israelis, who are not bound by U.S. export restrictions on encryption, sell such products? Export restrictions don't explain the current market dynamics.

Comment: One of the reasons there is not more demand for security is that the risk is small and is absorbed by large entities. For instance, the risk of using one's credit card over the Internet with no security whatsoever is nearly zero because the credit card companies absorb the cost.

Options for government roles and actions

Stephen Lukasik

[Editor's Note: Dr. Lukasik's presentation is available in a companion publication to this report titled "Public and Private Roles in the Protection of Critical Information-Dependent Infrastructure," available from CISAC. The abstract follows.]

A conceptual framework for addressing the protection of infrastructure systems subject to attacks on their information subsystems is presented. This includes treating the types of infrastructure systems, possible strategies for their protection, and the nature and scale of the attack. Three components of a protection strategy are identified: preventing attacks, limiting the damage in an attack, and ensuring rapid reconstitution of the target system following an attack. The paper includes a discussion of public and private responsibilities for infrastructure protection and the identification of a number of areas where public initiatives might be effective. These are ordered roughly in terms of the cost and difficulty of implementation. In addressing the subject, the analysis is from the perspective of minimizing government intervention in privately owned infrastructure systems.

Some early thoughts on information security in the new global information business environment

William Miller

William Perry has said, “We might say that in the nineteenth century the wealth of California came from the gold in our mountains; today it comes from the silicon in our valleys.” I would expand on that thought to say, “Nationally, the wealth of the nation is moving in the direction of software and information content. Software is high value-added for manufacturing, finance, transportation, communications, retailing, and even warfare. Excellence in software provides the greatest comparative advantage for individual companies. The battlefield of the computer industry today is the area of networks, and networks are much more about software than hardware.”

Computer industry observations:

First-to-market advantages are stronger than bug-free or perfectly secure software.
Individual company custom software has been replaced by collections of software packages. Companies are finding it more efficient to adjust their systems to the software packages than to customize the software and re-customize it when changes are made. First-to-market advantages for packaged software are so enormous that software producers will always make the trade-off in favor of time-to-market over quality. The successful companies then have rapid feedback and correction techniques to perfect the software after it is in the field. The returns to scale are enormous, and time-to-market is critical. “Get there first” is the production model. Software producers do not use the cumbersome software engineering procedures that would slow down the race to be first to market.

The packaged software business has been growing rapidly, driven by Microsoft, Borland, and many others. Embedded software creates the most employment, and the service side is growing commensurately. More software is now purchased from abroad. More is coming in from Japan and elsewhere. They’re getting caught up in networks and the Internet. There are a lot of young, inventive Asian entrepreneurs, and they are a growing part of our market. In Japan, custom software was a big business. Now, system integrators such as NTT Data, Daiwa Research Institute, Amoura, Fujitsu, etc., are combining packaged software for companies.

An international protection effort is needed because of global sourcing and distributing.
Networks reach the whole world and support the new business paradigm of global sourcing and distributing. Databases may be distributed around the world and may be accessed from almost anywhere. Making these networks secure will take an international effort. Every business is moving to Jack Welch’s General Electric strategy: go to any part of the world where conditions are best for any portion of your business.

Author Kenichi Ohmae describes the impact of technology on business: “...there is not much evidence to support the notion that economic activity in today’s borderless world follows either the political boundary lines of traditional nation-states or the cultural boundary lines of what Huntington calls ‘civilizations.’ But *there is plenty of evidence that it does follow information-driven efforts to participate in the global economy.*”

This trend is changing all institutions, including governments, around the world. Open economies are raising transnational issues, globalism begets regionalism, and new definitions of sovereignty are needed. One model is “Hanseatic capitalism,” which is influencing

China, Mexico, Eastern Europe and the former Soviet Union, and the high-performance economies in Asia. These are examples of information-cooperation economics.

The new economy has a corollary: regions have become more important. They can have a comparative advantage. Some regions have pockets (clusters) of economic activity connected to other clusters. Webs of regions. Networks are building from region to region. Japan, as a nation, is slow to change, but prefectures are developing clusters and linking to other regions. “We’re sovereign,” says a Japanese governor. JETRO promotes Hanseatic League-like relationships. The Council of Lubek generated rules for the League, and most of our commercial law derives from those rules. We need something like the Council of Lubek. We need practical relationships, with practical rules for intellectual property, taxation, and perhaps security.

The danger to information networks from cyber terrorism is just as great internationally as domestically. Because of the economic and information network interdependencies, we need to provide the same means of protection domestically and internationally. Every product, every component, is the best you can get from wherever you can get it, whether within your company or not (like a great hockey team). What is required is a willingness to reach out and get technologies. This leads to greater interdependence. The new economy is based on “web industries” (relationships) and alliances. That makes security a much more difficult problem.

Software protection requires incentives, not mandates.
Software is fragile and needs protection. I do not believe that protection can come by fiat. It must come from incentives, purchasing requirements, testing, and correcting the imperfections. It is important to protect the information business in this country (software is a plurality of our exports). A command and control system won’t do it. The self-correcting incentives and motivation of another system are required.

Strong encryption is needed worldwide to protect the world financial system.
To secure the world financial system, the highest level of encryption is needed worldwide. Network security cannot be done by one nation alone. Money can disappear on you so fast. The trick is to penetrate and you can create a huge ripple. Financial systems are probably the least secure; they need maximum protections, maximum encryption. If we permit the maximum encryption in the U.S., but not internationally, we have protected only a fraction of the system.

The energy systems we use are vital.
Energy is important. The continuity of the energy system is important for information systems. The risk here is not people blowing up the system—it is overload. With deregulation and competition, people need to get a higher level of utilization to be competitive. This will lead to more outages, more overloads, and the risk that problems will ripple through the system.

Growth
Information appliances are proliferating. The new computer industry ranges from PCs linked in enterprise networks to electronic chips embedded in everyday items. Industry uses standard components to add value through networking. The standardization and interlinking of electronic devices increases their vulnerability to attack. Encryption is not the only

issue, but it is one of the most important issues. Look for interdependencies. A national system of security won't do it—it's got to be international. If the Net Computer (NC) comes into being, as Oracle is predicting, there will be databases elsewhere, distributed databases for everything, so a national system won't protect us.

Regis McKenna said in 1978, "The network is the system." Scott McNealy adopted this as his motto for Sun Microsystems. Today's industry has computers linked to devices (old); this is being replaced by information appliances that are networked (new). There are now many sites hooked to the Internet (exponential growth); that's where the action is today. The Internet works better in the United States because telecommunication is cheaper here. Japan is too expensive in telecommunication, and there are differential tariffs, sometimes quite sizable, between countries. This will need to be resolved.

Government-private issues

The short list of key issues falls under these headings. Each is a conference in itself.

- Regulation/deregulation: telecoms, domestic and global
- Taxation: domestic and tariffs
- Privacy
- Security: the business environment and the need for military and police (physical) security
- Telecom mergers

Q: Major new government systems that failed to work include those of the IRS, the FAA, and others. How can large government systems be made to work?

A: How do we get out of this problem? The devil is in the details. The Social Security Administration has been successful with packaged software. But don't use packages right away. Wait for it to be debugged. Have a testing program. Wait until it's ready.

Q: What about attacks from abroad? What about state-sponsored attacks?

A: The world is becoming interdependent. Major trading partners are not likely to attack us. The PCCIP must be concerned with protection in other countries. Look for the same things you would in the domestic situation: terrorists, fraud—it will be the same internationally. For example, look at CommerceNet, which has over two hundred members, of which forty are international companies. They develop standards for electronic commerce on the Internet. They are very dependent on the United States for both trade and investment.

Q: What should the PCCIP focus on?

A: They should cover the major threats to system integrity: natural disasters, systemic overload, malignant amateurs (hackers), and the possibility that a nation-state can sponsor attacks on infrastructure. In between the latter two extremes is the criminal element. Focus on incentives and systemic encouragement to do things.

Utility deregulation is going on—the government would have to re-intercede if they want to use command and control. They can put incentives on reliable energy (the government is a big buyer) so they don't press the capacity limits. There is a need for more capacity for fluctuation.

Q: What about other government policies?

A: A big thing the government can do for software reliability is to wait until software meets measurement standards. Don't impose production controls. Just set standards they must meet for the government to buy. If there were measurement standards, companies would comply. It would be more profitable. Singapore did a clever thing. They automated the government first. For trade debt, you can get permits electronically. This takes forty-eight hours on-line, but it takes three weeks for a piece of paper.

Lessons from other government efforts to shape civil actions for national security purposes
David Elliott

The importance of critical national infrastructures to safety and well-being, plus the perception that threats may originate outside the U.S., tend to raise assurance to a national security problem, and the executive order for the PCCIP speaks in these terms. Several broad-gauge lessons may be learned from earlier examples.

Prevention of airline hijacking
In the early '70s, this was a major problem, creating problems with foreign relations with certain countries, and affecting national image. The authority of the FAA to mandate an existing solution was clear, but airlines delayed imposition of it for two to three years because they contended that screening would be unacceptable to the public and the cost would be prohibitive. The debate also turned on responsibility; the airlines contended that screening was a police matter, and actions dealing with foreign relations and national security were the federal government's province. Government viewed this primarily as a safety issue and did not want to start the precedent of paying for mandated FAA safety measures. Other solutions were studied, but were not feasible. Airlines had considerable power in Congress so legislative action was unlikely, and the FAA was hesitant to mandate new regulations on an industry the administration was moving to deregulate. (A clear analogy to electric power and short-haul telecommunications can be made here.) Eventually screening was implemented, hijacking was dramatically curtailed, the cost was considerably less than the airlines had estimated, and the public embraced it.

Lessons: This case involved an immediate, not a potential, problem. The nature of the threat was understood, an immediate solution was available, the airlines did not have an alternate solution, the costs were substantial but manageable, government authority to mandate the solution was in place, and the international community was prepared to cooperate. The problem was eventually solved, but why wasn't it a "slam dunk"? Two lessons can be inferred. Firstly, industry and government do different cost-benefit calculations. In this case, industry looked at near-term costs, cost risk, competitive position, customer relations, and liability. The government weighed public welfare, the political and foreign-policy costs of inaction, and its commitment to deregulation. These two concerns led to different conclusions. A second lesson was that by framing the problem in national security terms, the government elicited not the patriotic acquiescence it might have expected, but rather a strengthened industry view that, as a national security issue, the solution and its funding were government, and not private sector, responsibilities.

Keeping bombs off aircraft

This is similar to the preceding problem, but with a much different outcome. Again, potential steps to minimize the problem existed. These have only very partially been implemented, however, and the prevention of the placement of bombs on aircraft remains a goal, not a fact. Why? (1) The frequency of occurrence has remained below the threshold at which the public demands action. (2) The airlines say with reason that the proposed remedies would radically alter airline operations as we know them today, and the costs would be insupportable. (3) It is hard to measure the effectiveness of a remedy for infrequent events, and credible circumvention scenarios weigh against the implementation of costly solutions.

Lessons: (1) It is difficult to impose costly remedies to major but immature problems. (2) The risk of liability may be less of an industry driver than one might expect. (3) The government must be prepared to participate, and perhaps take responsibility for, the funding of solutions to problems of this magnitude.

Post-nuclear-attack telecommunications

Key to the strategy of the U.S. government plan for recovery in the event of nuclear attack was the availability of a core telecommunications system to maintain the continuity of government. AT&T was the central player in this effort. Meanwhile, other parts of the government were planning the breakup of AT&T and deregulating telecommunications, also with a national purpose in mind.

Lessons: Coordination of fundamental policy objectives between government agencies is iffy. Conflicting actions can result if coordination is inadequate.

Telephone espionage

The Soviet Union deployed equipment at extraterritorial locations to intercept telecommunications over leased lines carried over microwave links. The government had adequate authority to force some technical or operational remedy, but it did not do so for various reasons, including the fact that the new competitors to AT&T were in their infancy, and their viability could be affected by this government action. Finally, though concerned about an outraged public reaction, the government announced, without fanfare, that leased lines could be insecure and consumers should not assume that privacy exists. The collective reaction was indifference.

Lesson: Public support can provide the necessary political basis for action, but the public is more inured than the government might expect and obtaining support is difficult without marketing the hard evidence of a serious problem.

Civil defense

The U.S. government took extensive steps to protect the public from nuclear attack. The impediments to the policy were the magnitude of the problem, cost, multiple jurisdictions, and fact of an unmobilized society. The program failed when the threat outran any practical remedy, and what remained of the program was palliative at best.

Lessons: The government must seek solutions to the infrastructure assurance problem with implementation timescales less than the timescale for significant threat evolution, assuming such can be foreseen. Modifying large systems is slow, so we should look for incremental remedies that have a cumulative effect rather than for grand solutions.

Export control

This is a long-established concept, and bureaucracies exist to enforce it. The Cold War was largely a technology race. Technology transfer limits were internationally agreed to, even though companies with global markets lost revenue. The strategy was basically effective.

Lessons: The U.S. should take the lead to obtain international cooperation in seeking infrastructure assurance. Since the threats are not yet as evident, it will be more difficult to obtain agreement, so efforts to seek international cooperation should be started soon.

Preventing access to nuclear weapons material

Prior to the Indian nuclear explosion in the mid-1970s the U.S. was strongly committed to growth in nuclear electric power, the reprocessing of spent nuclear fuel, and the development of breeder reactors to make nuclear power self-sustaining. The government was also moving to privatize the fuel cycle, and had orchestrated industry’s investment in new facilities and technologies for this purpose. Abroad, the U.S. was a leader in supplying nuclear fuel and reactors, and it encouraged a large safeguarded nuclear program in most other states. The Indian nuclear explosion caused the government to reverse most of the key elements of its previous policy. Fear of nuclear weapon proliferation dominated all subsequent thinking in the nuclear arena, and because of interrelationships, changed our national energy policy as a whole.

Lesson: This is an example of the wrong way to accomplish an objective. Moreover, it was decided—and this is the real lesson—on very specific grounds with little consideration of the broader framework of issues of which it was a part.

Application of these lessons to the Commission’s task: Summary thoughts

1. It is important to comprehend industry’s calculus of cost-benefit. It will help us understand the limits to what can be achieved by cooperation and incentives, and how best to frame new regulatory authority that is effective and acceptable.

The above comment is directed primarily at the value of understanding the economic thinking of the infrastructure owners, since they are the Commission’s main private sector constituency. But there are others. As the Commission and the infrastructure owners explore the possibilities of new or modified approaches to networks, giving more emphasis to protection and reconstitution, the economic perspective of system builders and component producers must also be factored into the equation. Responding to the new market will require investment on their part too. However, this will not be seen as a usual market but one that exists, at least in part, because of government intervention, and one in which the government will have some continuing role. The willingness of system and product companies to make investments, in direct terms as well as lost opportunity costs, will depend on how the market is structured.

The nuclear materials example is a case in point, though the level of investment at risk was greater. The government wanted to transfer the nuclear fuel cycle to the private sector. That negotiation proved to be difficult and long because of the uncertainty created by the government’s continuing, but necessary, presence in the market. Industry wanted economic and legal assurances to guard against future government changes in policy or specifications that would obviate its investment. Ironically, the government validated industry’s concern by its subsequent actions.

This conundrum may at some point appear on the Commission’s agenda.

2. Reaching consensus on remedies to manifest threats has been a challenge. It will be even harder to define agreed actions to protect latent vulnerabilities against less evident threats, i.e., threats which go beyond those that infrastructure organizations can foresee. Mutual education and compromise will be required.

3. Liability exposure may be less of an industry driver than one might expect. This observation is pertinent because it has been suggested by some that the discipline of potential liability and insurability may lead the affected companies to take appropriate, efficient protective measures. Yet infrastructure organizations may be less motivated than most by the liability issue because their irreplaceable role in our socioeconomic life will lead the government, when pressed, to provide some form of immunity.

4. With the rapid change in systems and technology, the nature of the cyber threat is likely to evolve rather quickly. Therefore, incremental protection that can be implemented in a relatively short time should be emphasized.

This thought is aimed more at the agency that implements the Commission’s plan because it is there that specification creep in the name of optimization is likely to occur.

5. If national security is the reason for industry making expensive changes, the government should be prepared to pay some (perhaps much) of the bill.

6. It is important to understand the policy objectives of the government agencies (including state agencies) that traditionally deal with the critical infrastructure organizations, to lessen the chance of later conflicts.

The structure of the Commission, with representatives from different governmental branches represented, should take care of this problem, but don’t take this for granted.

The immediate question is whether mandated actions that may be seen as necessary by the Commission are consistent with the ongoing process of deregulation of the electric power and regional telecommunications industries.

7. Public understanding will be useful when undertaking an initiative of this magnitude. Does the Commission want to recommend to the President that the administration sell the public, including Congress, on the idea of the vulnerability of critical infrastructures as the price for getting support for remedial actions, and risk inviting attacks on these systems by doing so? Care must be taken not to undercut public confidence while trying to generate support by publicizing critical infrastructure vulnerabilities and threat scenarios.

Start early in trying to obtain the cooperation of other countries in finding common approaches to reducing infrastructure vulnerabilities and in controlling threats.

Judging by the preliminary assessment done at CISAC of the French perspective, the U.S. may not be on the same page as other countries.

Q: What would have happened in your examples if we had done nothing?

A: In the case of airline hijacking, that was tried and it only increased to the point that aircraft were being hijacked at a rate of one per week.

Industry Panel: Perspectives from the community of system users, network providers, and hardware and software producers on what government can do to persuade industry to invest in infrastructure protection in the future. What might work? What would not?

Sy Goodman introduced the industry panel:

- *Guy Copeland*, Computer Sciences Corporation, panel chair
- *Bill Firesheets*, Bank of America
- *Jeff Rulifson*, Sun Microsystems
- *Barry Leiner*, Microelectronics and Computer Technology Corporation
- *Bill Eyres*, retired IBM director of corporate security, now an entrepreneur
- *Bill Murray*, Deloitte & Touche
- *Nancy Wong*, PCCIP commissioner from the private sector, PG&E San Francisco

Guy Copeland

The topic has buried within it the premise that we need to do something more than what the competitive environment would cause us to do anyway. The premise is that we do need some motivations. Does industry believe there is something that needs to be done? Do we see a threat that requires us to respond over and above what the competitive environment would cause us to take?

Bill Firesheets

I have been Bank of America information security manager for the last seven years. Before that I was in data processing; and before that I specialized in military encryption technology.

On the business side, we see the same names on this program as on other programs, and we are hearing the same alarmist message we have heard for the last seven years. That does not sell well with CEOs or with banks, who, after all, are in the risk management business. We expect to lose some money. We don’t really lose it, we know where it is, it’s just a problem to get it back.

In the banking industry, we have what we call “security in depth.” We move $350 billion of money transfers a day; we treat the security of those transfers as a high priority. At the other end of the risk spectrum, for a credit card payment system for a corporation that represents a profit margin to a bank of $85,000 per year, we’re not going to spend $5 for each of 15,000 employees to protect that.

In the banking business, the biggest motivating factor is trust. The bank can lose $25 million, and that would hurt us, but the bank wouldn’t stop. Losing our customers would cost us more than anything else.

We have heard it said that banks don’t share information. That’s not true! We have a long history of protecting information as an asset. Examples of that include network security programs, the American Bankers Association’s X9 Financial Standards, and message authentication coding. The new buzzword for this is “digital signatures” for electronic commerce, but this is not a new concept. What we are looking for are cost-effective ways to implement it.

We don’t say anything in the newspapers, because our lawyers prevent that. We don’t say anything about Citibank’s security problems because the lawyers have put a corporate-wide clamp on it. My guess is that it was an inside job. At least *USA Today* said so.

We need real solutions, not over-engineered things. Encryption in many cases is overkill. Security is cost-determined, and if we forget that, we’ll let the two ends of the risk spectrum drive us. Both banks and their customers gauge their level of risk and act accordingly. Customers give us their credit card numbers over the phone, but they won't do it over the Internet. Banks might not verify a $50 transaction, but they certainly will verify a $500,000 transaction.

What I'd like to see the government do is bring together all the solutions that are out there. Often the solution is there, but people just don't apply it. If the problem is operating systems with common passwords to common user IDs, then just change them.

When are we going to see some tangible fruit coming out of all these task forces and commissions? It is helpful just having a high level President's Commission pull together what's already out there and what's available, and synthesize it, and private industry and the government have to work together to accomplish that.

There have been two roles the government has played that have been vital to infrastructure development. One is organizing and stimulating, helping the community get together to set standards, etc., and doing it in an unintrusive way so that government itself is not mandating or setting standards. The government has done very well in this with the Internet, for example. The other role is long-term research. As industry has been forced by economic realities to pull its time horizons in, the long-term research creating the long-term technology base that industry can actually use has been an important role of the government. While I'm a firm believer in industry and market forces as the primary mechanism, I really do believe there is a role for government in terms of leadership, in terms of research, in terms of helping.

Jeff Rulifson

I manage an advanced development lab where my mandate is as much to bring in the best from around the world as it is to do things internally. From that perspective, there are four observations I would like to add to the discussion:

1. *Market pressures trump system reliability*. Early in my career, I worked for a start-up, and I was under pressure to put a product out. It had way too many bugs in it. While meeting with the company board about the problem, one of the founders decided to "handcuff an engineer to it and ship it." That's what we did. The market pressure to ship something is that great.

2. *Technology won't solve everything.* I have a fear that there is a belief that if we had better authentication, if we had better encryption, if we had AI systems for detecting intruders, we could put a technological paint over our systems. These are wonderful things that we should add. But if you want to steal Visa passwords, the hard way is to get them from the Internet. The easy way is to steal a laptop that has them on its hard disk. It's not a technology authentication issue. If you want to break into Web servers, get a source license of Sun code. Look at the networking software, go to the bug list, figure out exactly what you're going to do and then do it. That's what the real hackers do. It's not a matter of cracking passwords. There's a huge amount of legacy software that got built with thousands and thousands of man-years without any regard for these issues. It's not going to go away. We have no choice but to undertake a long, tedious "revving" (repeatedly making revisions) of the infrastructure with the goal of making it secure, being able to protect it, and making it secure against itself. Bugs in a system will bring it down when under overload just as surely as a premeditated attack. Technology won't solve that problem.

3. *Government should not set standards.* The government does not understand what industry means by "standards." What government envisions as "compliance or performance

standards" is actually a mandating of algorithms and processes. Industry is willing and enthusiastic to go along with performance standards. Sun promotes open standards aggressively, but as soon as the government gets into the business of designing and prescribing encryption algorithms or key escrow policies, you'll have an extreme problem with industry. Technology is moving so fast that prescribing standards is a foolish thing to do anyway.

4. *Learn how to gain industry's trust.* I've been a part of the negotiation that has gone on with government over export control and encryption policy over the last few years. If the government wants a cooperative relationship with industry, it should seek to understand how its interaction with the private sector led to a substantial breakdown of the trust between industry and government. If you're going to start an initiative of working with industry again on these issues, you need to look hard at that, and how to not get into that situation again.

Barry Leiner
I've been with MCC for about a year and I'm starting up a West Coast laboratory to try to give MCC better access to Silicon Valley expertise and give the companies in this area a better way of interacting with MCC.

Before MCC, I was with ARPA/DARPA, and I was responsible for the Internet and other information infrastructure and for distributed information technology R&D. I started my career doing vulnerability analysis for navigation and communications systems and for the vulnerability of wire-guided missiles. The combination of vulnerabilities, security, and distributed information infrastructure is of great interest to me.

MCC is a consortium of forty large companies and organizations that focuses on consortial pre-competitive R&D. Our typical activities are projects with six companies and the government. These range from new technologies to studies to standards to architectural work that allows exploitation of technology. To choose a project, we do a quick and dirty study, so we can take an area of interest and refine it so that it makes sense.

We just launched a study in the area of security. The focus is on the use of technology to support distributed, federated, secure operations. We ask what approaches can be taken to take advantage of the secure technologies that are available to create a flexible, secure, distributed operation that allows for effective cooperation among a defined set of organizations, while protecting the internal data of each organization, with changing patterns of cooperation and competition.

There are a number of biometric technologies being used for authentication. What is the architectural approach that will allow each organization to integrate biometric technologies and yet support a shared trust model between organizations?

We've been talking about infrastructure as if it were a monolithic thing. All infrastructures are multiple organizations cooperating with each other. For example, the airline industry needs uniformity. The Internet is a set of independent organizations and networks that cooperates according to a set of rules. Each organization does its own thing. The survivability, robustness, security, reliability, and invulnerability depend on each organization. If you get access to a cooperating network, you get access to all of it if you don't have protections.

Bill Eyres
I just finished my first thirty-year job with IBM. Most of that was spent in security, with the last dozen or so years as a security director representing a variety of business units.

We have fought with the same issue with which the PCCIP is now faced: How do we get senior management in the private sector to listen to these issues and to take action on these issues? The role of the security manager is not that much different, in this respect, from the position in which the Commission now finds itself. What we have learned over the years is what Bill Firesheets said, that management wants to do the right thing, they want to do it in the right way, but they are sitting there waiting for the right set of information that will allow them to make the right decisions. If you criticize them for making bad decisions, you are really criticizing yourself for providing them with inappropriate information, or for not providing them with any information at all.

The right approach for the Commission, and for those of us in security, is to get the information right and get it to the right folks promptly. One of the issues we have dealt with for fifteen or twenty years is the theft of computer components: chips, microprocessors, disk files, etc. We have taken steps to prevent that. We get the police involved. We've tried to correct it, but we haven't moved one step closer to a solution in twenty years. In fact, the problem has gotten an order of magnitude worse. Theft has been the growth industry in Silicon Valley and everywhere electronic components are made.

A group of security directors were commiserating on this issue. They said, "The right way is to approach the problem fresh with real data." Each professional has a ton of anecdotes. Estimates ranged from $2 billion to $8 billion in 1995 and $200 billion by the end of the millennium. No one knows how good these data are. We commissioned a study by the RAND Corporation for $500,000 to answer this question. The output of the study includes:

1. How many thefts occurred? What were the dollar losses?

2. What other costs are involved? Examples: If the company's inventory of the stolen components is low, it must be replenished at a premium. There are also warranty losses.

3. Recommendations for senior management, law enforcement, policymakers, and the security industry on how to prevent this kind of crime in the future.

Similarly, we don't know what the losses are in the infrastructure business. It does a lot of harm for us to throw around numbers that are inaccurate. I would rather see us say: "I don't know, but we'll find out."

What is the relationship between the security community and law enforcement around the world? We have done much of our work with the public/private sector on a tactical basis. To improve the relationship between the public and private sector, we need to join together on strategic solutions, not just to make the case and get the bad guys, and then go back to doing something else.

Even in the best of times, planning for emergencies and responses and running scenarios requires the support of top management. In Silicon Valley, running earthquake scenarios, and getting management to buy into it, was a fairly easy thing to do in late 1989 after the earthquake. As time has passed, the half-life of that interest has been exceeded. We are at that point or have passed it right now. The lesson in this is that if you get management revved up on a particular point, but fail to nurture it, you will lose their attention in a very short period of time. A corollary to this is that if you go to them with the wrong set of risks, their concern will evaporate very quickly. It's like selling an earthquake scenario in Rochester, Minnesota. The issue faced by the PCCIP is how to maintain the level of knowledge and concern that is there.

Bill Murray

My clients include Bill Firesheets' banking competitors worldwide, insurance companies, manufacturing companies, and telecommunications companies. Bill Firesheets' remarks reminded me of a talk last year at the RSA Data Security Conference in San Francisco, by Jim Barksdale, the CEO of Netscape. He said, "Security is to the Internet as safety is to commercial aviation. But with the Internet, we are where aviation safety was in 1937, when the DC-3 came on-line. Now, if you hold safety constant at 1937 levels, and you allow traffic volumes to grow to today's levels, you would be killing people at the rate of two 747s a day. Under such conditions, would you fly?"

If we are to enjoy the promise that the Internet holds for us, that the global information infrastructure holds for us, there is a certain level of public trust and confidence that is essential and that must be maintained. In the information technology security business, we are on a threshold. We are moving from a world in which what we did was not very important, except to the enterprises where we worked, to a world in which everything we do with computers and communications becomes part of the global information infrastructure for the twenty-first century.

Infrastructure is public. However it is financed, it is shared and used by all of us. One of the problems that we have in industry is that management does not understand that risks they took five years ago only impacted them, but if they take them today, they not only put themselves at risk, they put their neighbors at risk, and they put the public trust and confidence at risk.

General management wants to do things right. They understand what's right in the main line of their business. In this computer security area, they require a great deal of help in order to be in a position to understand what they ought to be doing. This is not a technology problem, in spite of the fact that technology is its origin. It's a management problem. In spite of what Peter Neumann told you this morning, it's not a product problem.

This is not because people didn't do things right. It's not because they didn't build the right features and properties and functions into their products. It's not because they don't have the right characteristics. They are under pressure to move things to market. I spent fifteen years at IBM trying to ensure that IBM's products had the right features and functions and properties in them. The problem arises not because of the characteristics of boxes, but because of the way we put the boxes together. If you look at the government for the last six months, you see that four servers have fallen to attack. There are a lot of ways of looking at this. One way to look at it is that, of the 1,600 Web servers that are out there, 1,596 have not fallen to attack. The government is under constant attack. They no sooner add a server to the network, than it is attacked—within hours. If you leave a server under attack for a long enough period, they will fall over. The likelihood of penetration increases with what I call "Murray's WAIST":

Work
Access or connectivity
Indifference to detection
Special knowledge
Time to corrective action

Building these things is not rocket science. Building secure Web servers is not rocket science. Building secure general-purpose systems is rocket science. Once I have decided on an application, I can make it secure. I take out all of the functionality that Jeff [Rulifson of Sun

Microsystems] worked so hard to put in there. I take out the editors and compilers and command interpreters and I operate my box as a single application, a kernel-only system. I do not operate my box as a general-purpose system that we have been trying to make secure for thirty-five years, when hardware was the expensive component.

This is not only a U.S. problem. This is a global problem that must be addressed on a worldwide basis. I've got to tell you that, from my clients' perspective, particularly those who are international banks, this is being complicated by the ambivalence of the U.S. federal government on the topic of cryptography. If we don't get that resolved, then we limit the use of the single most important tool that we have to have to put boxes together.

Nancy Wong

The electric utility industry is still paying a high level of attention to earthquake risk. It varies from industry to industry. In utilities, such as gas and electricity, attention to natural disasters that hit us year after year (different ones) will keep our attention at very high levels. Until one and a half years ago, I was responsible for the telecommunications and computing infrastructure line organization within an electric and gas utility. That industry is undergoing deregulation in a very intensive way. I was the manager of a very large department (over seven hundred people) with over 100,000 square miles of territory. You have no time to breathe. You barely have the time to keep up with the changes to prepare your company to be competitive in a deregulated world. You pay attention to the next thing. It's difficult to look ahead and identify what might happen to you two years ahead. Several industries are now undergoing these conditions. The question is, Who is interested in protection, and what is going to be the incentive, under conditions like that?

Here is the private-sector view of priorities: bottom-line financial measures and customer relationships; public perception and public confidence in a business.

Management deals with what they know or can forecast with some degree of credibility. They assess risk against their business objectives. What they don't know, they ignore, and will accept the risks. What they do know, they will assess the economic return (tangible, or intangible, if it relates to customer relationships), and invest appropriately for their business. IT companies are concerned with their intellectual capital, so they are paranoid about information security. At PG&E, I was reassigned from line responsibility to create a department to look at information assets, which includes information security. That's quite an investment on behalf of a company that is counting its pennies to prepare for deregulation. Our auditors brought to senior management's attention that our systems are our business, in a competitive deregulated world. Our information assets need to be managed as assets, very similar to how our material and our financial assets are managed. This approach to investment is similar to how we would invest in a power plant or substation or service office. We ask ourselves what is the lowest level of investment that brings the highest level of return in coverage. We would be looking at what is an expense in terms of our business, what is the risk, because we are in the risk management business. What would be the cost of protection to manage that asset that is commensurate with the asset's role in the business, and what would be the consequences if we did not put the protection mechanisms in place.

I have some thoughts on regulation and legislation. The pace of change is accelerating in business, sometimes driven by technology, but sometimes driven by customer expectations. Competitiveness is based on cycle time responses. How are regulation and legislation going to keep up?

Coming from a highly regulated industry, I can tell you that changes in regulation and legislation move at a glacial pace. Meanwhile, the market and the industry is moving away from us. It is a truism in parts of the electric industry—it does not matter what the legislators and the regulators decide, the market will start driving the changes in the electric and gas and oil industry. If we as a company do not pay as much attention to what is happening in the market as we pay to the regulators, we will have lost the battle.

We have to be careful in that boundaries have been dropped between countries. We need to consider impacts on competitiveness of individual companies and the global competitiveness of American companies in general. The largest company in our industry is Enron; PG&E used to be the largest publicly owned gas and electric utility in the United States. Within the last six months, Enron and another company have become numbers one and two. These companies have far fewer anchors to the past. They do not own as much infrastructure as PG&E. That may be a harbinger of what may happen in our industry. The question we have is: What level of protection is appropriate to balance these issues in our industry and in the country in general?

Guy Copeland and Panel Discussion

Q. What's happening with NSTAC?

I serve on the Information Security Exploratory Committee and also on its steering committee. The charge for the committee is to decide whether or not industry is going to take up the challenge posed to us by the National Security Telecommunications Advisory Committee (NSTAC) to form an Information Systems Security Board, to be an authoritative source of information systems security information, evaluation, training, and so forth, for the private sector. We are separate from government. Government is not helping us.

NSTAC, when they approached us on this, cautioned us that there would be no role for government, other than to be a spur. They have put their proposal forward, and are now letting the private sector address their proposal. We are engaged in doing that right now. We are trying to determine three things:

1. Of the missions that were proposed for this board by the NSTAC, which ones are being partially or completely fulfilled by existing organizations in the private sector?

2. Recognize the needs to be satisfied.

3. Is there a consensus in the private sector that says there is an advantage to us all of having an Information Systems Security Board, and is there sufficient support within industry to form that kind of a body?

That's the status. The exploratory committee hopes to report by August 1997.

Q: How did NSTAC decide to branch itself out of the telecommunications industry into transportation, financial industries, and that sort of thing? Why did you stop there?

A: We're not looking at all of those industries; we're looking at their use of telecommunications, networking, and information systems (requested by the President in 1995).

In 1995 it was asked to expand. In July of 1996, Clinton established the PCCIP to seemingly enter the same field. It's either a disconnect or the NSTAC wasn't what he wanted.

Q: The urgency is less evident... Even to the student of this whole activity, as we've heard at this workshop, the need for urgency is unclear. People aren't saying, "Hey, let's get on with this, the problem is really pressing.” The government sociology on this is all but clear to me. I was wondering if it is clear to you?

A: NSTAC should seek consensus with the PCCIP, in a joint effort to seek infrastructure protection, as opposed to divisionally working in corners. We have a national mission as a national organization, so let’s build consensus. NSTAC groups are working closely with the PCCIP. The NSTAC is a subset of what the PCCIP is looking at. They can be supportive of, and cooperative with, their efforts.

Q: You gave me a needle-like answer. Is there a shotgun answer? Are there those in industry who say, “go examine your own problem and don’t bother us,” or, to put it more charitably, “the private sector can handle this—we don’t really think the government is the right entity or has the right people to worry about this”?

A: Within the Information Assurance Task Force, we have, since 1995, been conducting risk assessments, after we set up a risk assessment methodology. We conducted a study of the electric power industry. We visited many companies, some of the associations for those industries (EPRI), some of the vendors, and some of the consultants. We are doing a financial services risk assessment and a transportation assessment, and beginning the identification to narrow down the scope, because transportation has many different modes: air, land, sea, and intermodal, and intelligent highway systems coming up fast (the IEEE is active in that area). The PCCIP and the Infrastructure Protection Task Force (created by the same executive order and headed by the FBI) are trying to use in-place mechanisms to enhance communications between government and industry.

Lessons from the electric power industry: the threat information is missing. There is a lot of anecdotal information, but it varies across the board, and the reaction varies. There is no evidence of intrusions causing outages. Only rumors, but no evidence whatsoever. We had evidence of employees not using procedures properly for electronic devices causing outages, but that was not intentional.

Q: With so little hard evidence, what is the best approach to take?

We engage in a constant cost-benefit analysis, including risk management, trying to identify what will enhance the bottom line of the business, what will improve the customer perception, and what will enhance their reputation and differentiate their product from others. *There is not deregulation, there is re-regulation.* The rules get more complex. They sometimes break up their companies, without communications within the company. For example, transmission services cannot share information with their retail distribution entities.

The electric power industry is very regulated. They tend to be very skeptical of folks who arrive from government and say, “I’m from the government and I’m here to help you.” That’s not unique to electric power—everybody in NSTAC views it this way, based on long experience with regulation. What they don’t want to see is more or additional regulation as the solution in this area. What they do want to see is improved communication and the opportunity to establish mechanisms to allow that communication and to do it in an environment that protects them from antitrust concerns. NSTAC can do that as an advisory body to the President because it has the advantage of being able to communicate with each other and with bodies within the government, and that’s very beneficial. For these reasons NSTAC is sometimes cited as an example of a useful approach to deal with these issues.

Q: Are industry leaders as concerned as they should be?

A: We found that there is a hunger for information: What is the real threat? Can you give me hard data (not anecdotal)? Can you give me some real measures (even samples) of what is occurring on the network? There is a desire to share information about intrusions:

- How they occurred.
- How they were discovered.
- How they were reacted to.
- What the response was.
- What they've done to protect their system so it won't happen again.

The desire is to share the information with each other and with the government (federal, state, and local—they're all involved in these activities). It's the local government that is of the most interest to these infrastructure entities—they are performing a public safety function.

There is great difficulty in sharing current-incident information when it relates to a prosecution. The interesting cases with current technology are being chased by the FBI; they can't tell you what they've learned because that would jeopardize the case they are trying to bring. So you hear things in the background—attacks in Florida on 911 service—but you never hear the details. By the time you hear the particular problem, the technology has moved beyond that and you should be worrying about new issues as well. Financial services institutions are at a higher level of concern for security than the electric power people were. People rob banks because that's where the money is. They put more emphasis on protecting their systems because of that. On a scale of concerns, intrusion is relatively low. Paper checking is the source of most fraud that occurs in banking and other financial services in the U.S., and that is a couple of orders of magnitude higher than intrusion-related losses. Credit card losses are next on the scale. The major credit card companies do a quarter of a trillion dollars of business every quarter in the U.S.; a small percentage of fraud is a lot of money. Cellular fraud is quoted at higher figures than banks acknowledge.

Q: What is NSTAC going to do?

A: NSTAC attempts to get at addressing the issues rather than defining them. Our NII Task Force defined the concept of an Information Systems Security Board and tested it with a variety of infrastructure companies (non-NSTAC members). This is similar to the Financial Accounting Standards Board (FASB) for the information security area, establishing the principles and the methodologies for evaluating systems to see whether or not they are being implemented and used at a sufficiently safe level for the application for which they are intended. NSTAC cannot implement anything.

Through our outreach process, the private sector recognizes the significance of this, and has established its own information security exploratory committee hosted by the Information Technology Industry Council in Washington, D.C., including some sixty companies and associations. This has broad representation, including the automotive industry group, the American Bankers Association, the American Bar Association, auditing companies, most computer manufacturers, systems integrators, the manufacturing sector, the services sector, etc.

From the system integration point of view, Computer Sciences Corporation is seeing the security business increasing. People come to us and say, "We've just been hit. Help!" or, "We've just been audited! We've been told that our information security is poor and we need your help to correct that." A major national restaurant chain had a hacker floating around in their system and they took it down for a couple of days. With Just-In-Time, taking down the central computers is very costly to the bottom line.

NSTAC is looking at legislative and regulatory activities. The Telecommunications Reform Act of 1996 mostly ignored security. Networks now have to provide interconnection with any other network at any technically feasible point. The FCC thinks that "technically feasible" should include security issues as well as other issues. Presently there are very few requirements to get into the business. Just buy a license and set yourself up as a broker, don't own any of the equipment, except a computer for billing because you want to collect money. That makes it possible for folks with less than a desirable background to get access to the system and to get access to the sensitive control systems of those networks. The PCCIP should look at this. It is of great concern within the telecommunications industry.

Q: Does Congress understand these concerns?

A: They spent more time in that bill focusing on the Communications Decency Act provisions than on any security provisions. Other things show that Congress needs education and awareness training from industry as much as anybody. For example, there is a draft bill in Congresswoman Jackson Lee's office (Houston, TX) that proposes that all the manufacturers and distributors of modems or other computer communications devices have to put a warning on their system to alert the user that when they connect to a network they may be exposed to harmful things, such as viruses, people trying to get into their system to steal data, and perhaps their kids might be exposed to things they shouldn't see. The intent is for home computers, but it covers everyone in the industry.

A regulation approach that focuses on technology is shortsighted. I'll touch on encryption as an example. Any regulation that touches on key length is at great risk. There is an algorithm using elliptic curves that offers considerably greater strength for the same key length as does the DES algorithm. A 56-bit key length using the elliptic curve algorithm would be orders of magnitude more difficult to break than would a 56-bit DES. A prescription based on key length doesn't make sense.

Within the Information Technologies Association of America, there is also a critical infrastructure protection group. They are trying to put together the focal point for a large number of IT companies. The ITAA is probably the largest of the representative associations within the IT industry within the U.S. The ITAA is getting ready to hold the World Congress for the IT industry in 1998 in Fairfax, Virginia, with 1,400 companies and thousands of regional associations.

Q: Are there things that government could do to motivate industry along these lines?

A: (Bill Firesheets) Guy Copeland has a paper out on the idea of using insurance to motivate business, using the flood insurance model as a way to approach it. Government underwrites flood insurance because it is so potentially catastrophic when it does occur that businesses wouldn't underwrite it themselves. The insurance companies sell the insurance, and government steps in for major floods. Insurance in general has not been available for business protection or losses due to information losses, damage, or loss of integrity, or potential liability for consequential damages, because of IT. The insurance industry hasn't had actuarial experience; they couldn't put a value on it, and have been unable to establish a basis, even though they see it as a potentially lucrative area. One of the questions is, could it possibly work on the flood model, where government could underwrite it at least for a period of time, until it could get the experience basis necessary?

This idea has been around for about five years. They always say, “I will insure you if you meet these minimum levels of security standards.” I already meet them, so I don’t need their insurance. Where is the added value? It might be a mechanism whereby the industry achieves a level of security, along the lines of accounting standards.

I suggested that NSTAC look at auditing standards more for security standards. Funding of insurance at the national level always envisions government taxing more. Somebody’s got to fund it. Government doesn’t pay for anything. We as taxpayers pay for everything. The government just dispenses the money. From a big corporation point of view, what we’ve seen with the FDIC is that we pay a lot of money but we are doing more than is required. The Commission needs to bring more small business owners into the fold. I don’t know any small business owners that are represented here today; they’re all big corporations. I’ve found that as you go down the food chain, the less emphasis there is, there isn’t capital, there isn’t the need, they expect the big guys to do it for them. The tax code could do some of this, such as expensing security investments. B of A will spend $29 million on a contingency plan. Over the last seven years we’ve spent over $300 million building and operating our contingency backup. Being able to capitalize the expenses, or carryover allowances, so it won’t hit earnings in one quarter would help. Another possibility is development and implementation credits.

We developed a money laundering system that we gave to the Treasury, but the IRS didn’t see it as worthy of the R&D credit as Congress had intended. For over a year, we have had two IRS agents sitting on our premises reviewing the information that it took Ernst & Young over a year to collect. We’ve got a problem that the Commission might address. We need to know how the IRS is going to interpret it or we’re never going to get any credits.

Legal approaches and issues

Lawrence Greenberg

Three approaches have been used to deal with the special problems posed by infrastructure protection and assurance:

Governmental

Legislative, law enforcement, and national security actions fall under this category. Who within the government(s) (international, national, state, and local) is empowered to act? Within the U.S., the federal government is constrained by the Interstate Commerce Clause of the Constitution; it is insufficient to justify federal action merely on grounds that the problem is large, unless the courts determine that Congress has the power to act because of the impact on Interstate Commerce. When does an adverse event become a national security matter, and when is it merely a law enforcement question? How can legislation be kept from becoming outdated by the rapid evolution of technology, and how can the differences between legal and computer security language be bridged to avoid statutes being struck down by the courts for vagueness?

Regulatory

One possible solution to the problem of inflexible, vague, and dated legislation is vesting power in regulatory agencies, which tend to be more nimble than legislative bodies (although perhaps not nimble enough). However, regulatory agencies are not always welcomed by the industries they regulate nor are they necessarily effective at solving problems. Also under this rubric are government mandates, perhaps enforced by regulatory bodies, and government-created incentives for private parties to protect or create infrastructure.

Private sector

Since companies can compete on the privacy, reliability, and security of their networks, software, etc., market forces might drive at least those infrastructures subject to competitive pressures toward providing greater security. When America Online proved to be an unreliable Internet access provider, CompuServe took advantage of the situation by marketing their competing service as more reliable. Clearly, the market is not a panacea for system assurance, but it will be part of the solution.

Tort litigation and liability insurance also falls under this category. If someone can be held liable for damages resulting from system failure, those victimized by such failure can sue for damages. The costs incurred from such suits will force either an improvement in system assurance or the purchase of liability insurance. An advantage of using the tort system in this way is that it puts the burden of system assurance on those with the greatest knowledge about the system's problems and on those who are best able to spread the costs of improving assurance across the system's users and beneficiaries. Another advantage of the tort system is that the service providers' liability reflects the level of available security technology. Also, such responsibility for system failure, improvement, and cost-sharing arises organically from legal and corporate structures that currently exist; nothing need be done at the legislative, governmental, or regulatory levels to make this happen. The obvious disadvantages of this system include reliance on piecemeal, state court action to set tort standards, likely requiring considerable time for a workable structure to take form; large transaction and overhead costs, often necessitating collective legal action to make progress if individual damages are too low to be worth any single person's or company's trouble to sue; and potential deterrence of infrastructure development in jurisdictions that favor plaintiffs.

Tort law is concerned with defining duty and proximate cause: what duty did the defendant have to keep from injuring another or the plaintiff have to avoid the hazard, and what were the results of the failure to fulfill such duties? These definitions will need to be reexamined in light of developments in information technology. Before the advent of railroads, people who engaged in ultra-hazardous activities were generally held liable by the courts for any damages they caused. A shift in legal doctrine occurred when courts realized that if railroads were held liable for all the damage they caused, no railroads would be built, since the damages were potentially so great that no one could be forced to bear them. Because of this change, individuals and communities who depended on railroads developed other means of protection against railroad-related damage, and insurance tended to grow in parallel with the growth of railroads.

Q: Liability may extend downward from those who own the networks to those who build the networks and even those who build the components of the networks. So how can liability be effective?

A: The good side of litigation is that it is a mechanism to represent society's broad concerns without going through the process of legislation through the results of multiple jury decisions. However, liability could drive important endeavors out of existence or prevent them from arising. An example of this is the small private plane manufacturer that was driven out of business by liability issues. The questioner's argument, however, can be made very strong.

Q: You left out a discussion of the contract mechanism. Could you discuss this?

A: Contracts are good because they allow parties to mutually agree on what is fair. Contracts are limited in that people can be damaged beyond those who are signatories to a contract. Example: A crashing plane injures both those who are riding in the plane who have a contractual relationship with the airline, and those on whom the plane falls who have no such contract. In the latter case, liability pertains, but contracts do not.

International legal issues

David Keyes

With the exception of vulnerabilities arising from system interdependencies, all threats are currently criminal acts under U.S. law.

The ineffectiveness of export controls for strong encryption is analogous to the ineffectiveness of regulations against exporting British weaving technology; it diffused from England to New England anyway. Export controls can at best slow down the technology transfer from West to East, but the time and cost required to move technological ideas around the world are negligible barriers.

In dealing with terrorist threats, the U.S. government decided to broaden its information sharing with the international, federal, provincial, local, and private sectors. Target hardening and denial of sanctuary to terrorists are now international policy objectives. Multiple government agencies cooperated to bring this about. Interpol was persuaded to change its constitution from refraining from investigating religiously motivated acts to investigating acts that were criminal without regard for motivation. Analogous mechanisms must be found to pull together an international consensus against cyber crime and information warfare (IW).

Words mean different things to different nations, and even to different U.S. government agencies. The Russians thought that the rule of law and probable cause meant that the fact that a person had long hair, Levis, and no shoes was probable cause to knock down his door at any time of day or night, just to see what he is doing.

Is it possible to launch an international investigative agency for cyber crime? According to the Germans, this will happen when there is a universal application of the Napoleonic Code and a French national is in charge of every national police agency in the world. The French respond that Europeans have a certain sensitivity to Germans carrying guns and coming uninvited into their countries. Clearly, the possibility of launching such an international agency runs aground on the shoals of national interests.

The best progress can be made through bilateral agreements and mutual legal assistance treaties, rather than broad multilateral agreements. Just as the private sector in the U.S. is often unpersuaded by the case for immediate action, other countries do not always respond immediately to new perceptions of threats. One can make this case if one is clever; if you give foreign governments a tip that people are defrauding the local government's telephone carrier in states where telecommunications are nationalized, they will have a wiretap up in no time, because it is tax fraud, but it's not a criminal activity as far as the police are concerned. We should expand international information sharing, collaborate on joint models for investigative activities, and collaborate in intelligence exchange, but this must be bilateral rather than multilateral.

Commissioner Keyes recommended the following steps: “Identify strategic and tactical indicators of cyber attack or intrusion. Fund development of the technology to monitor them. Integrate private sector and state and local government into federal warning systems.”

Dinner Speaker
William Owens

The subject that you have gathered to discuss is enormously important. The world has changed. If you look at the world’s one hundred largest economies, fifty-one are companies and forty-nine are countries. You find that Mitsubishi is larger than Indonesia, that Ford is larger than Turkey, that Daimler-Benz is larger than Israel, and SAIC is larger than Chad. The world includes many truly multinational companies, and information is a large part of what is going on with them. Many other changes are occurring, like the Soviet Union disappearing, and many other countries trying to come together to develop markets. China is going to be, I believe it is her destiny to be, the world’s largest economy. How important IT is for all of that!

Information technology as the solution to global problems
I am here to talk to you about some of my views about information technology. SAIC started a list of the world’s great problems. We have had several seminars, and have developed a list of eleven. We’ve had seminars on the eleven problems, with experts and Nobel Prize winners. The issues include energy, and food, disease, and the environment. There are some common elements of the eleven problems, and the most common is information technology. That was the most significant observation that we had. If you really want to help solve the world’s great problems, then information technology is the way to do it.

Systems integration
Outside this country, there is still tremendous technology, whether in Japan, or Korea, or China, but if you talk about systems integrating these technologies, whether it be software or hardware or telecommunications, or transportation vehicles, you find that systems integration knowledge is a talent that is almost purely American. The man who started talking about *systems of systems* in articles he wrote a few years ago is Bill Perry. Systems of systems is the answer to many of the challenges we face, not only in terms of developing systems for solving the world’s problems, but in terms of the key to protecting ourselves, the topic of the seminar here. We have something to contribute, as a nation. It comes primarily in IT and systems integration. It is terribly important that we get focused on what to do about both the problems and the issues that face us, like the one we are facing here.

Systems must communicate
For thirty-four years I was in the Navy. My last operational tour was as the commander of the 6th Fleet in the Mediterranean. For two years I did that. Whenever I was on the aircraft carrier, and we would be going by an Army base, or an Air Force base, I always tried to contact them on the radio. For thirty-four years I tried that, and I never got an answer. Was that because I was a Navy guy, or we couldn’t figure out what frequency to communicate on, or the protocol was wrong, or the security didn’t work in both directions? For thirty-four

years, I never talked to an Army person unless it was an exercise. The analogy is strong for civilian systems. Systems of systems for the electrical power distribution grid, or the pipeline grid, or the banking system, strangely come together in interesting ways. I don't think anyone understands.

We are at the stage, in this infrastructure business in the United States, of "Who understands?" *Maybe* there are experts on Internet security, or banking security, or Internet commerce, or the pipelines and how we keep them running, or the electrical distribution grid (frankly, I doubt that there are), then surely there are no experts on the whole bag of tricks, the system of systems that makes up this enormously powerful future for us as a country, and as a world, in terms of solving world problems. Frankly, I salute you for getting this conference together to talk about these things.

How to address hard problems

I had three precepts for approaching difficult problems for the military. First, you have to have the right people talking together. I thought that was four-stars, and the Secretary helped me to set up an aura around the JROC that was OK (not blessed by many people, but OK), so we had four-stars meeting together. The second element was, spend the right amount of time. When do you think about the strategy of where our country is going? Where do the senior leaders get together to think about these things? We in the JROC got together for one full day every week across fifty-two weeks of the year. We sat and we talked about the details, the boring details, of all of the systems. What frequencies does it transmit on, what is the protocol, why is that protocol better, what is the security code, why doesn't the Air Force system interlink with the Navy one? It was boring. You don't come to an understanding unless you have the right people, the people at the top, that's what you people represent, and that you have the right amount of time, and the third thing is talking about the right thing. For us, it was war-fighting: the right people, the right thing, and the right amount of time. That applies here as well. For this important capability that we have coming to us, how do you then defend against those who would go after it, how do you defend a system of systems?

Thank you very much.

Q: In Australia last November, I met with the Australian Defense Research establishment people in Canberra, the chief defense scientist, and he had a big staff there and we talked. One of the younger people said that the United States is moving so fast, with so much money and smarts, that our allies won't be able to fight with us.

A: People around the world in militaries, perhaps in business too, worry a lot about how fast America is going, and how will they ever be able to communicate, keep up, do business, or do war-fighting with us. I think there are some exciting things that are possible now. In the U.S. military, global command and control systems (GCCS) is the counterpart of a disk operating system in a computer. It allows you to put everything together on a variety of computers, and to interact with each other like you do on the Internet. A lot has happened with object-oriented computer systems, so you can take legacy systems and encapsulate them and get them on a net in a strange new way, or C++ software, or SEI level standards for software, and we have an ability now to bring a surrogate GCCS or a surrogate Link 16 to bear, which could be a lot cheaper.

Q: As you build toward interoperability with other countries, and as you bring more commercial software and hardware into your programs, how do you avoid compromising security? One of the things we talk about on the Commission is, how safe or how vulnerable are our systems? Our concern is that as we go interoperable internationally, we create problems and processes for ourselves that are simply different. How can you cope with that problem in the military?

A: You mean because they'll come back into our system and retrieve information? That they'll know about these kinds of things? It seems to me that the world has changed a lot. The close-hold, covert information is a thing of the past. I'm not saying we should go out and share this with every country in the world. For NATO, allies, we have very little that we have to hold back. We are the superpower, but we also want to be the superpartner, as part of our leadership. There are multilevel security schemes on the same net that are possible in software that are good answers to this problem. The multilevel security commercial software on my Compaq computer that I bought a week ago has 128-bit encryption. You can buy that for $2,100. It comes up on the screen, "Are you a U.S. citizen?" And I answer, yes. And then it asks, where do you live? They walk you through three frames, and I'm not sure they proved you were a U.S. citizen, but the next thing you know you're on-line at 128-bits of security, which is a tough problem for decryption.

Q: The evolving cultures outside of the United States, the fragments of the former Soviet Union, are concerned that the United States is formulating a plan for using electronic warfare or information warfare against them. Won't that place this country in a larger threat environment, even though we are involved in such activities as Partners for Peace (PFP)?

A: If you go to the Pacific, to Japan or Korea, what is going on? They never talk about the Russians any more. Their defense budget is down by 80 percent or so. Their challenge is how to buy enough oil to lubricate tanks. How they can get more than two or three hours of flight time a month for a pilot. Ours get 22 or 23 or 24 hours per month. They have profound difficulties! But we need to treat them as partners. PFP is underreported in the press—this is a very important program. We need more of the Nunn-Lugar stuff to build the confidence together. Bill Perry has been central in this effort.

You have two choices, to do it or not do it. I can't think of a single reason why we don't want to proceed to do it as best we can. I don't believe any of our allies or enemies around the world are going to not do it because we don't do it. It is important that we get on with it. If we have an approach to a system of systems, with redundancy, I don't think that anybody can ever beat us. We'll stay so far ahead of the train that they will never beat us. Sure, they may get some capability, but they are going to do that anyway. We should get on with it.

Setting priorities
Willis Ware

My views are judgment calls. They are not based on a lot of analytic study, because in the large the analytic basis does not exist.

Where is the country? To a large extent it is in the jawboning phase. It is trying to figure out an advocacy process to support this issue.

The Commission's goal is to strive for a peacetime posture that will keep the country safe, stable, and reliable while avoiding situations that might cause us to drift into a military or political confrontation. The wartime situation is another subject for another place, another time, and another commission.

Any technologist who is reasonably informed can construct scenarios that would be devastating if they were to occur. We are in a sort of offense-defense game with situations that have already occurred, with natural threats, software glitches, carelessness, and accidents. Most organizations have emergency response teams for these situations, and run practice drills, so they are in reasonable shape *for situations as they have occurred in the past*.

The country's first order of business should be to prevent physical attacks to infrastructure. These make the kind of political statements that terrorists want to make, and are therefore the most likely thing and the first thing to happen, and are the easiest to pull off.

Cyber attacks are a long-standing computer security issue set in a new and more expansive threat environment. The computer security issue took about twenty years to get going, and progress was stimulated by NSA initially. However, it is still seen as moving slowly in the private sector, because the private sector either absorbs the cost, does not perceive the risk, or thinks the cost of security exceeds the risk of loss. The critical information protection issue will be a replay of this history; it will take a long time to get it moving.

Technology is not the long pole in the tent. There are R&D and new products that will be required, but we are not exploiting what we have available now. We need protection mechanisms for the insider threat; we are not dealing with that well today. Network security has also not been adequately addressed. Devising intrusion detectors is not an easy job; you can make a detector provided you can define the event you want to detect. If you are looking in a steady stream of traffic and asking, “Is there anything wrong?” then an intrusion detector has to know what normalcy is. Then there is the Ed Feigenbaum problem: information workers are proliferating, and we must increase their trustworthiness, supplemented by technical measures.

The long poles in the tent are awareness, understanding of system complexity, understanding of network complexity and interdependence, education, training, and organizational commitment.

The Commission can make a big contribution if it can give structure to this issue, and give reality to it, and a sense of timing to it. The sky is not falling in, but we cannot afford to dawdle, either; we may be wrong in our judgment, and things may happen much more rapidly than people believe. We will be prudent to get on with working the problem, but not in a panicked way. It will be difficult to recommend a timeline, but some sort of timeline is warranted.

The government may need to stimulate investment in this issue the way it stimulated computer security in the ’70s and ’80s.

The Commission should prioritize the eight infrastructures within its purview with an eye to the commitment of and competition for financial resources.

The PSN (public switched network) is the most important, and energy sources are next. These need first-order attention. The other areas are downhill from here—either they are much less critical, or are in much better shape, or have fall-back manual techniques, or are not completely automated, or are cognizant of the threat. Don’t ignore them, just don’t put them at the top of the list. Get on with the infosec job. Do it against the measure of what the lawyers call the reasonable or the prudent man.

Pick electrical power over gas and oil. The electrical industry has a more visible, more complex, and more extensive network. The electrical industry is being forced into a new world by deregulation. They are being forced to intercommunicate, transmitting power over leased lines, and in general are facing a more complicated operational future.

The PSN would be good to do a case study on. The PSN knows how to respond to natural disaster, and they do it all the time. The telecommunications companies have mutual assistance pacts, so they know how to move assets and resources from place to place as events occur. Some redundancy is already in the system. Telephone companies have been hit by hackers, have awareness of the issue, and have some experience dealing with the problem. Most of the dimensions of the problem with these two are already known. Everything we need to examine is present in these two examples. We should not lag on getting on with the infosec problem.

How do we know when we are well-enough off? I don't know the answer. We need to develop metrics that we and other countries can use to make judgments with respect to the national welfare.

Audience comment: Engineers only test against known metrics, and the level of robustness simply has not been specified. Some of it can only be tested in the field.

William Joyce

Threats

The predominant assessment by conference participants is that there is a serious lack of data regarding threats. One way to get some data is to learn what we can from natural threats, which are a serious danger in their own right, and provide a useful laboratory to learn about potential threats and vulnerabilities.

A lack of reliability in our infrastructure, and the lack of confidence that such unreliability would engender, is itself a threat. The lack of reliability of infrastructure in the Third World creates a lack of stability and confidence. We need to remember that people do business in the U.S. because we have an infrastructure that works; we must keep it that way.

Vulnerabilities

The Commission is very concerned about vulnerabilities created by system interdependencies and the vulnerability of legacy systems. Maintaining legacy systems has both advantages and disadvantages. While having them around certainly proliferates vulnerabilities, it also increases infrastructure complexity, which creates robustness of a certain sort.

We do have a people problem. The fact that security products are available but not used, and that passwords are used carelessly, are symptoms of a consciousness problem. The Commission must work to raise consciousness, especially in regard to using security measures that are not burdensome.

Solutions and priorities

We do not want to be alarmist in dealing with the public, but we need public buy-in. If we can get public pressure behind solving the infrastructure problem, implementing solutions will be much easier. It's harder to operate when you are ahead of the game. As we seek the support of businesses and consumers, we must be sensitive to the fact that infrastructure protection cannot consume the bulk of most players' attention. The public needs an advocate of some kind in this process. While we don't want to see the establishment of another federal entity, such advocacy needs to be institutionalized.

As we seek solutions, we must also be sensitive to international constraints. The values, concerns, and perspectives of other countries are not always the same as ours.

It is essential to accurately gauge what mix of government mandates and market incentives is acceptable to the private sector. Liability exposure on the part of business is apparently less of a driving force than the Commission first thought. However, there may be some room for federal mandates similar to those ensuring environmental protection. Requiring security specifications in the federal government procurement process may also help. The government needs to share more information with the business sector; business leaders expect to be informed if intelligence agencies know of actual threats to private infrastructure.

There is a need for more formal education for security engineering, and there is a need to combine this with performance engineering. The processes of engineering, especially systems engineering, are extremely significant and need to be emphasized more in relation to the tools of engineering.

The idea of designating a minimum essential infrastructure has an element of "circling the wagons" to it. We may not want to go that route, but instead take a layered approach, designating some infrastructures as critical and others as noncritical.

There is much diversity of views within the government as well as outside, but we are starting to develop a consensus to work these problems.

Roundtable: What do we think we know and don't know? Where do we need to concentrate our attention?

Participants: *Ed Feigenbaum, Charles Giancarlo, William Owens, William Harris, Stephen Lukasik, William Perry*

Ed Feigenbaum
Feigenbaum gave the conferees a pop quiz on security awareness. Of the people in the room, 100 percent had sent and received e-mail. Seventy-five percent had received an encrypted message. Thirty-three percent had sent an encrypted message. Twelve percent encrypted the contents of their hard drive (an advance, since in most audiences no one has encrypted his hard drive contents). Feigenbaum observed that because most people do not care about security, as evidenced by the statistics, and the software industry is highly responsive to its customers, the software makers do not care about security.

The U.S. citizens are the U.S. government's best customers. In the event of a major information catastrophe, such as a major loss of personnel records, Social Security records, banking records, or a major loss of access, what would the "customers" think? What would be their perceptions? The perception would be that the government, not private industry, had failed to adequately protect the infrastructure and to plan for the catastrophe. The public would blame the DoD and the FBI, not IBM, AT&T, Merrill Lynch, Sun Microsystems, or H-P. Because citizens do not pay these private companies for protection, they have no expectation of protection. However, citizens do pay their government for protection and thus maintain an expectation of protection. Ironically, most people in the DoD do not want to touch this problem with a ten-foot pole, because it smacks of the military doing something within the borders of the United States. The private sector, both on rational and emotional grounds, must come to terms with the federal government's role.

The problems for the U.S. posed by IW are potentially severe, and the opportunities for offensive warfare are impressive. The Defense Science Board has twice studied these issues in the last three years, and admonished the DoD for slow action on its first report. A scientific basis is missing for the work that is being done by the few groups that are now working on this. As with any new technology, the early stages of IW development have been marked by much tinkering. At present, on a ten-point scale, IW research would get a 10 for creative thinking and tinkering and a 1 for science. The ARPA program that began this fiscal year to do science is the one notable exception.

We have no "science of malicious systems and software." Where are the universities in this area or this conference? One of the consequences of minimal university participation is a lack of "out-of-the-box thinking" on this issue. Collaborations, like the one between the Santa Fe Institute and the University of New Mexico, in which human immunology lessons are being applied to the design of defenses against malicious code, are the exception. More joint research of this nature is clearly needed to widen the scope of research and to bring more people and perspectives to bear on the problems of information security.

Information system defense and attack is still an empirical art, not a scientific domain. How one gets better is by doing, by exercising and training all the time, constantly improving the state of the art. Our military defense forces know this. They almost never fight, but they exercise all the time. Their exercises are very realistic—when they practice dogfights against MiG-29s, the planes are flown as if they had the parameters of the MiG-29, and they are flown by the best pilots. However, in the information warfare arena, realistic attack exercises are hardly ever done. For example, when at the Blue Flag training facility (an Air Force command and control center mock-up), Feigenbaum suggested an exercise to one of the commanding generals in which the trainers would throw in a three-second power glitch. The fellow running it "went through the roof." "No way," he said. "That exercise costs $10 million and we won't get up again for two days and you'll ruin the whole thing." They did let the information warfare specialists in on the Red Flag training exercise (the fighter exercise), with the instruction that they could observe but should not disrupt the exercise. So they didn't, but an hour before the initial briefing, the air intelligence people stole the air tasking order off the computer and then walked into the briefing with it. The general was furious.

Lesson: We almost never practice information attack.

Recommendations:

- "Government, be bold." "Private sector, cooperate, don't consternate."
- NSF, DOE, DoD should fund the creation of a science base for information protection and attack. Research spending is a comparatively trivial amount of money—one-tenth to one-hundredth of one percent of the cost of the end product.
- University researchers should focus on the problems discussed at this workshop and should help everyone else to think innovatively about these problems.
- If the DoD, FBI, and intelligence community claim that information is the fifth dimension of warfare, they should practice and train as if they believe it.
- The U.S. is just barely ahead of the game. This is just-in-time policymaking.

The U.S. must train the way it fights and fight the way it trains.

Charles Giancarlo

I am an expert in data communications devices, a relatively narrow specialty compared to the breadth of expertise of some of the panelists.

Cisco is responsible for about 80 percent of the data communications equipment of the Internet, and over 80 percent of Fortune 500 companies base their intranets on Cisco Systems equipment. Cisco is the largest supplier of firewalls, and has the largest Internet commerce site. Hence it is very concerned about security. Security in networking, firewalls, security monitoring, etc. is among the hottest areas of venture capital and investment—several companies in this field have recently gone public with great expectations of their future profitability.

We were having so many attacks by hackers (many of them overseas competitors, trying to get into our network to steal Cisco technology) that three years ago we completely disconnected the network from the outside world. It was that severe. We completely redesigned the network before reconnecting it. Sun, H-P, Microsoft, and Intel have all had similar experiences.

Cisco recently announced an Internet and networking security alliance with these companies, focused on creating security standards for the Internet and between computers. Of the customers Cisco sells to, banks are the most security-conscious, due to SEC and Federal Reserve regulations, as well as their own choice. U.S. banks assume the risk of customers passing credit card numbers over the Internet.

Security is important to technology companies, because of their Internet commerce sites and their need to provide customers with information about their shipments, orders, engineering, debugging, configuration issues, etc. Both of these activities give customers access to a part of the company's system, creating the need to secure the rest of the system against intrusion, from hackers trying to do mischief and from competitors trying to steal intellectual property.

Likewise, individual customers will have an increasing need for security with the advent of new technologies allowing persistent connections from home computers to the Internet, rather than the current dial-up technology. People value their privacy and will not want to have the same computer on which they run Quicken and store their financial records connected to the Internet without some measure of security to protect their personal information. Within two years networking capability with virus detection, firewalls, and other security features that will protect home computers will be commercially available.

Industry needs to see a consistent government policy on encryption standards worldwide. The current policy is not consistent with the reality of a worldwide market in which capable foreign competitors are not held to the same export rules as American companies.

Cisco sees the security business as a billion-dollar market opportunity, and hence sees a lot of market pressure to create security protocols and security products. We don't know all the ways that hackers will defeat any given protection, and this will have to be tested over time. We don't know how best to coordinate efforts across industry, and we don't know what the government is going to do, and this creates uncertainty in industry. Cisco hears about every failure with our products, from whatever source, natural, hacker, bugs, etc. Customers perceive these as important problems and they create pressure to decrease vulnerabilities.

What can government do?

- Create awareness.
- Create an environment for discussion and for standard-setting.
- Seed technology.
- Create a much larger security market through its own procurement.
- Review progress and give attention to neglected areas.

William Owens

Who are the employers that will hire the master's and Ph.D. students who are expert in this area and are now looking for work? What is the business that will hire these people? We are working to develop a master's program of study with the University of California that is much more relevant to the needs of business than the current UC programs.

The National Defense University started research on "fifth dimension warfare," or more accurately, information technology that infuses the other four dimensions. As more has been learned about this fifth dimension, the very structure and organization of the military today have been called into question. If God were designing the military today, He might have information specialists, a joint-strike organization that puts weapons on targets, and a seize-and-hold service that captures territory, rather than the traditional divisions of the military found in the United States today.

Modeling and simulation of warfare is a vital component of military training today. However, despite having spent nearly $4 billion, the United States still finds it difficult and, in fact, does not do it very well. The JSIMS, the Joint Simulation System, is a new billion-dollar program in the DoD that will be completed around 2002. JSIMS will model the kinds of warfare that the United States expects to conduct in the future. Modeling these new kinds of warfare is clearly considered quite important, but equally important is the modeling and simulation of U.S. infrastructure systems. A few hundred million dollars put into an effort to better understand and model the infrastructure would be a reasonable investment. Much more sophisticated and detailed models of the electrical, telephone, pipeline, and other systems is needed. Such models will help to demonstrate threats, to understand the systems, to stimulate discussion, and to answer questions about the potential effects of deregulation on the infrastructure. Until this work is done, policy design will be based on instinct and intuition rather than science and understanding.

The military is conducting some IW simulations at the Joint Battle Center in Norfolk, VA, where systems are put together in one place, demonstrated, and then put to the test. These simulations cost approximately $20 million per year. The systems usually involve a little bit of networking, a little bit of sensor data input, and communications. In the tests, Red Teams try to break into the systems, attacking the encryption schemes, software switching, etc. trying to find their vulnerabilities.

As a historical note, the NATO networks in Europe at one time had only about three or four nodes, run by Deutsche Telecom, through which all military communications passed. Thus, compared to that level of vulnerability and dependence, today's PSN is a much more robust system.

William Harris

Lessons learned from my experiences and observations in the transportation industry:

Component standardization was necessitated by the railroad systems' interdependence and interoperability, identical to the problems faced with infrastructure assurance. The railroad solution was not created at the behest of government, although government later became involved when it decided to set safety standards using the industry-agreed specifications to make their standards compatible.

The adoption of new technologies illustrates how the legal environment can dramatically affect research and development. New wheels better withstood fatigue, so the industry mandated that whenever a wheel wore out, it would be replaced with a new wheel. The cost of replacing all train car wheels at once was excessive, and the wheel manufacturers lacked the capability to manufacture enough wheels to do so. However, after an accident took place, the railroad was found guilty under tort liability of not having used the best possible wheel, even though the wheel that broke was a qualified wheel under industry specifications.

If this ruling were allowed to stand, railroads would have a powerful incentive not to conduct any further research into better technology, because they would be forced to replace all existing equipment with any newly developed technologies immediately and completely to avoid tort liability. Fortunately, the ruling was overturned.

The advent of information technology is helping to improve the physical infrastructures. With railroads, it could be used to prevent an overtaking collision (positive train separation) by continuously sensing the distance to the car in front, with onboard computers calculating the stopping distance of the train. Such a system would be much more efficient than current practices. Public traffic systems already employ the intelligent transportation systems. This technology is also quite timely because the U.S. has been underinvesting in public transportation for about twenty years; the number of lanes available has fallen well behind the demand, causing traffic jams. The Texas Transportation Institute estimates that the country loses about $75 billion in fifty-five metropolitan centers due to costs attributable to this congestion. In Japan, 147 advanced traffic management systems are operated in urban areas with about a million privately owned vehicles carrying intelligent systems that communicate with the larger transportation systems to optimize the traffic flow. The lesson here is that public infrastructure investment must be dealt with first before private investment becomes worth doing.

Cases where U.S. infrastructure has been disrupted:

1. In 1916, all of U.S. coastal shipping was handled by foreign-flagged ships. In World War I, that shipping was completely withdrawn. The problem was solved by the Jones Act, which required that all coastal shipping be handled by American ships.

2. Bank failures in the 1930s were solved by requiring deposit insurance for the small depositors and by setting minimum reserve requirements for all banks.

3. The U.S. experienced a major railroad strike, and learned that if the infrastructure goes down for a week or two, the economy will grind to a screeching halt. So a cooling-off period was legislated (Railway Labor Act). If management and labor were unable to find a settlement during the cooling-off period, the government would legislate a settlement and both parties would be forced to live with it.

Stephen Lukasik

Two different views of the stability of infrastructures have emerged during this conference:

1. The fragile systems view: Many holes in security exist; systems are easy to penetrate; rapid propagation of failures is possible because of extensive connectivity; and software is difficult to monitor and to understand. This perspective tends to be prevalent among those people who speak about the technology side of the issue.

2. The robust systems view: The national infrastructures comprise what is effectively a system of systems that are multiply connected, have excess capacity, and have distributed control.

In coming to some sort of equilibrium between these two points of view, use of the generic term “infrastructure” is problematic because it raises the problem to too high a level of abstraction to answer stability questions. The situations are very different for different infrastructures, so they should be dealt with on an individual basis.

The telecommunications system must be seen as the central infrastructure of concern because it carries the signals to all the other infrastructures. Electric power is next in importance. If the phones go out and the power goes out, you're in trouble. If one wants to do bad things, doing them in the dark when no one can call for help is an ideal time to do them. The banking and financial system is sufficiently important to add to Willis Ware's list of critical systems. Unlike lots of things, the movement of capital has some of the least inertia connected to it than any other system, and it is thus much easier to create global scares. Other systems such as the water distribution system and the gas distribution system are more stable, and thus deserve careful examination to understand the nature and quality of their stability.

Would a regulatory council wrapped around these three systems, but excluding the other infrastructures to keep things simple, be a viable solution? It might have an NSC committee focus, to keep the President informed, but it must involve the DoD and intelligence community, with the DoD worrying about any strategic warfare issues and intelligence working on possible threats. As the other speakers mentioned, law enforcement is a better framework for dealing with the international situation than the defense establishment.

However, many arguments against regulatory mechanisms remain: the regulatory approach involves more recordkeeping, is heavy-handed, produces uninformed decisions, and inhibits innovation. In spite of these arguments, the regulatory approach is still a viable one worthy of study because many regulatory mechanisms can be bent to the issue. Bad guys must be caught, regardless of how information warfare evolves.

While much of the discussion of regulatory and statutory measures has focused on adding regulations, of equal importance is the question of what, if any, regulatory and statutory constraints can be removed. One example might be removing antitrust regulations to enable companies and industries to work together on these problems of security.

One of the most important things the Commission can do is to leave behind an organizational entity to represent the public after it disbands. No existing organization satisfactorily addresses this problem: the DoD would rather avoid the issue; FEMA exists but has not been discussed much in this capacity; regulators are seen as part of the problem rather than part of the solution; and no one wants to create a new agency. A permanent organizational structure is not necessarily the answer, but one that lasts on the order of ten years would certainly be useful. In ten years much progress could be made in information security. Ten years, being approximately the term of office for a two-term president, happens to be about the length of time that the country can sustain a political focus.

For most aspects of the problem, cobbling together existing organizations and agencies is probably a better approach than attempting to invent new organizations. These groups would include experts from EPRI, CIOs and chief engineers of corporations, and researchers from the national laboratories.

William Perry

The infrastructures that have been discussed have suffered from, and will continue to suffer from, faulty design, work overloads, amateur users, and hackers. But the focus of this symposium is on organized attacks by organized crime, terrorists, and nation-states.

Observations:

1. A fairly broad consensus exists that the threat is serious and will get worse because of increasing use and increasingly diverse technologies. The threat will also get more serious as organized groups become increasingly aware of the potential for creating mischief. Ironically, conferences such as this one serve to increase such awareness.

2. The stakes are high. Society is dependent on these networks, and the vulnerabilities are also high. Great potential exists for a real catastrophe.

3. Technologies exist to decrease our vulnerability, but such solutions are costly and difficult to implement. Implementation will involve many people and groups and must therefore overcome much inertia.

4. The will to act is lacking. This lack exists not only because of the difficulty in finding and implementing solutions, but because the fundamental question of who is responsible for acting has not yet been resolved. Who profits from attacking the information infrastructure? Must a catastrophe take place to galvanize us to act? I fear that it will and hope that it will be a low-level catastrophe rather than a high-level one.

Questions:

1. What can be done to increase the public awareness of this problem in the absence of a catastrophe?

2. What can be done to provide incentives to business to do more to help solve this problem? How can incentives be structured so that business is simply responding to natural market forces rather than acting solely in the public interest? How can the development of protection systems be made more profitable? How can incentives be developed to encourage industry to work more closely with the government?

3. What is the proper role for government? What programs should it pursue? Some suggestions:

A) Support of R&D.

B) Get the government "feet-first" into the role of developing models and simulation (something the government does well because effective simulation is large-scale, expensive, and requires access to information that most private entities lack).

C) Develop real testing of infrastructures and systems. The military is especially good at this.

D) Work with industry to develop security standards. Past agreements on standards led to the growth of the Internet, and now that it has come into being, security standards are needed to protect the networks.

4. What is the role of the university? This symposium has produced a rich menu of research areas that can be pursued by universities. This symposium is also a living example of the unique ability of universities to act as a catalyst to bring government and industry together.

4.0 Observations and Further Research

The sections that follow represent the organizers' efforts to distill some important observations and research directions from the workshop presentations and discussion.

Vulnerabilities and threats

Two trends are dramatically increasing U.S. infrastructure vulnerability, one extensive and one intensive. The extensive trend is that IT is increasingly permeating all systems, from telecommunications to the Internet to the logistic control of physical infrastructures. The intensive trend complements this: the *kind* of IT being adopted is shifting from stand-alone customized systems to integrated applications using more off-the-shelf hardware and software, dramatically increasing the prospect of cascading system failures within and across infrastructures.

The potentially covert nature of IW and the ease of limiting direct casualties without sacrificing the ability to do great economic harm lower the political threshold for engaging in IW. The obvious way to adapt to this lowered threshold for IW is to adopt defensive measures. However, there are many barriers to doing this, as various conference participants pointed out. The public is almost completely unaware of the problem and scant effort is being made to educate or inform them other than the occasional sensational popularization in the press. Political support for rapid changes or large expenditures is unlikely until an overall public education campaign has "raised consciousness" about the scope of the problem.

Corporate players are more informed, but are constrained by market realities. Companies seeking to serve their customers must balance their risk against the attention, organizational education, and investment costs needed to respond to the problem. Much of the response is of common value, such as hot pursuit of intruders into IT systems, rather than merely expelling them, so corporations reason that it is the job of law enforcement or national security rather than an issue to be addressed by private-sector attention or private/public partnerships. Also, "keeping it quiet" is the all-too-common corporate response to a problem, especially in financial services where copycat attempts are feared and public trust is the *sine qua non* of business.

The realities of private-sector cost incentives are exacerbated by the fact that many of the costs of system failure are borne by others. For example, the costs of power and telephone service outages are borne by customers, not the utility companies. Insurance is not yet able to include coverage (or deny responsibility) in policies. It is therefore tempting to treat infrastructure threats as nonexistent due to the lack of experience on the part of those not directly bearing the costs and inconveniences posed by such threats.

Actors

Infrastructures face a wide spectrum of threats from various actors, including natural hazards, states, terrorist organizations, organized crime, corporate actors, and individuals. The conference examined the capabilities and modes of action of these different players, which are briefly characterized here.

Natural hazards (and this would include things such as system overload or human carelessness), while occasionally creating crises with high economic and even political costs, have proved to be a useful arena for testing vulnerabilities in infrastructure systems, though not in a controlled and scheduled fashion. The participants pointed to the need for personnel training and increased organizational readiness to deal with the natural threats that already exist. It was also pointed out that future natural disasters may reveal weaknesses in infrastructures that could be attacked by those so inclined before they are remedied.

State-level actors, both overt and covert, include military actors (both offensive and defensive), law enforcement, intelligence agencies, and even political factions within states using state apparatus for political ends. So far, state action of an offensive nature seems to have been mostly limited to the gathering of intelligence; the U.S. claims to have developed an extensive IW capacity, but information on this is classified and hence not discussed in detail in conference proceedings.

Few incidents of terrorist threats to infrastructure seem to have surfaced (the plan to attack New York City infrastructure by the group that committed the World Trade Center bombing is a notable exception). However, no conference member disputed the possibility of this becoming a problem in the future. Organized crime has concentrated on financial theft and fraud.

Because of the implied leverage in many infrastructure systems, individual actors play a large and increasing role. These can be insiders from the above categories, freelance hackers, or unwitting or accidental accomplices to attacks on infrastructure through carelessness or ignorance.

Techniques for Infrastructure Attacks

Considerable attention was devoted to the physical and cyber techniques that can be used to facilitate these threats. Physical techniques include conventional physical attacks on transportation infrastructure, but also include such technologically advanced methods as ultra-wide band electromagnetic radiation, which can disrupt most electronic components of information systems with an electromagnetic pulse of high peak power when produced at close range. Other kinds of attacks are less aimed at creating damage than they are at achieving control, and thus often use IW techniques against information infrastructures: dissemination of replicating viruses, the production of cascading system failures, intentional system saturation, information blockade, deception (via dissemination of misinformation or spoofing), and delay and/or denial of service.

Roles and responsibilities

The conferees were unanimous in seeing a greater need to communicate between industry and the various civilian and government agencies on how to prepare for IT threats. However, several roadblocks to open communication surfaced. Banks, for public relations reasons, would rather eat their losses quietly than risk leaking to the public that they suffered thefts via electronic security breaches. Military branches of government may not want to reveal to industry what they know about electronic security vulnerabilities and how they can be fixed, as these problems pervade the information infrastructure of other countries as well, countries which might be targets of IW in the future. For obvious reasons, government agencies do not want wide distribution of their own vulnerabilities either. The suggestion was made that perhaps software companies should be required to publish information to customers and prospective customers as to the known security flaws in their products; however, this policy also seems a good way to increase the efficiency of hackers. Beyond these observations, few concrete suggestions were made as to what to do to get past these problems.

Research is clearly needed on what changes to the status quo are possible. It may be necessary to give financial institutions anonymity when gathering statistics of computer crime-related attacks and losses, perhaps by going through trusted third parties, who could conduct such surveys.

After it became evident that considerable divergence of opinion existed regarding current threat levels, participants agreed that the gathering of such comprehensive, reliable data is needed for the quantification of current threats and assessment of future threat potential. This divergence was fueled primarily by the sparseness of present statistics and uncertainty as to the reliability of those statistics.

Without such data, no consensus was possible on the question of what degree of protection from such threats is needed and what the value of such protection is. Such determinations are needed before progress can be made on suggestions made by participants of the need for a government-affiliated and/or private standard-setting body to decree security standards for software, the need for national campaigns to educate personnel in good safety practices, legal changes such as reform of antitrust law to allow for corporate collective action on security measures, the inauguration of tax incentives for private firms that increase security, and the revision of export regulations on cryptography.

A closely related problem is that of the complementary roles of the market and of government. Are the threats so severe that they are primarily a national security issue, or merely a large but undeveloped market opportunity for private software security firms? Will we, while debating the issues, roles, and responsibilities, add more insecure software, hardware, and interconnections between information systems, thus increasing the probability of cascading system failure, or will we contribute to building security measures while removing fundamental vulnerabilities?

One problem is hierarchical-jurisdictional: Who gets involved when an incident occurs? Local, state, federal, or international government bodies, or a combination? Conference participants suggested that allocating jurisdictions and responsibilities among these groups is such a big problem that two separate conferences may be needed to tackle the federal/state and local and nation-state/international aspects of information vulnerability.

Research needs

The problem before the Commission is new and one of great complexity. Based on the views, questions, and ideas put forward at the current workshop, it is evident that even framing the problem acceptably will require much work, and devising practical plans for action outside the sphere of direct government control will not be a short-term undertaking.

One of the purposes of the series of workshops that Stanford and Lawrence Livermore Laboratories are conducting on the protection of critical civil infrastructure is to obtain help in defining a research agenda for improving the understanding of the subject. We have attempted to distill from the participants' inputs a preliminary (and incomplete) list of topics that need further analytical work if some consensus for action is to emerge. Each suggested topic below is preceded by samples of the diversity of views it entailed.

Problem Definition

The nature of war has changed, and the civilian population and its supporting infrastructure are vulnerable. Organized cyber threat potentially has several sources: traditional adversaries, rogue states, organized crime, espionage (military and economic), disinformation, organized crime, and terrorism. The Commission was created to "do something," and needs to formulate a timely response.

Risks beyond hackers and disgruntled employees are highly speculative. Certain low probability events may occur, such as truck bombs or cascading system crashes, but the prevention of loss should not exceed the logical likelihood of attacks. Also, response should be encouraged, not mandated. Standards should be set and responses incentivized, but government-specified "solutions" should be avoided.

Many problems are being studied simultaneously. They need to be disaggregated. Careful evaluation of potential events is necessary to clarify the nature of the problems, evaluate their likelihood, and estimate their cost and impact. Potential solutions should be compared and implemented according to a road map developed by further research. A key tool in this effort is modeling and simulation.

Statistics

The current loss experience is small compared to potential damage from one or more serious attacks. The published reports are incomplete and not reliable, however. Some form of information sharing and attack reporting is necessary. How to generalize from the data on individual attacks or natural disasters the impact of organized attacks is a difficult issue.

Current losses are being sustained, but not in high enough doses to warrant a radical change of approach. Most of the losses occur from crime and vandalism, including current or former "insiders," not from state-sponsored terrorism or similar organized attacks. Statistical analysis must carefully define the nature of the problem and the extent of losses.

Most reports, not surprisingly, are anecdotal and unreliable, given the lack of consensus about definitions and reporting requirements, the bias for shyness instead of publicity, and the lack of agreement about potential attack potential. A great deal more study is required, perhaps along the lines of the RAND study of high-technology crime commissioned by the International Electronic Security Association.

Early Warning, Information Sharing, and Response Planning

Better mechanisms are needed to alert officials when intrusions occur. Early warning includes both automated measures (David Cooper described an ideal system) and organizational responses. International, intergovernmental, and public/private institutions are needed to provide coordinated evaluation and response.

Mandates would possibly concentrate the likelihood of specific attacks, and be inappropriate for specific business situations. However, the proper role of government is to provide the information and possibly the incentives and technology so that businesses can take action in response.

A considerable amount of work is needed to describe the current vulnerabilities, establish technical and organizational warning systems, overcome conflicting incentives (ejecting intruders versus trapping and pursuing them), and raise consciousness about the entire field. Information sharing programs need wise planning with buy-in from key institutions. Early warning systems need to be coupled with one or more crisis response organizations so that events can be understood, categorized, and responded to. Response planning deserves a lot more attention, including risk assessment from multiple points of view (power outage, GDP losses, etc.). Simulation, response, and scenario analysis may expedite consensus on the best course of action.

Deregulation

Multiple telephone companies, interlinked electric companies, and the patchwork quilt of decision-makers complicates national security preparedness. Older understandings need to be reviewed in light of the current trends, both here and abroad. Careful use of incentives and regulations will be needed to obtain compliance.

The new market-driven regulatory environment is here to stay. Companies that might have amortized expensive security equipment and training over all rate payers may now be unwilling or unable to pass on costs, and may be reluctant to incur capital expenses for some nebulous "public good." Any response should be coordinated so that no one suffers competitive disadvantage. Also, incentives are the only reliable way to achieve action.

A special group or conference should be held to address the issues of utility deregulation. The workshop is correct in identifying telecommunications as the top priority for information warfare research, and then the electric utilities, in that almost all infrastructure is dependent on electricity from the grid. A separate group or conference should consider the problems of banking and finance, which, although undergoing regulatory changes, are subject to very different constraints. The diversity of systems may make a nationwide attack more difficult. Small-scale attacks are facilitated (many points of attack), but system failure is less likely because of the lack of interoperability of many systems.

System Design, Software Bugs, and Conflicting Priorities

The interconnection of vulnerable systems opens the door for attackers (domestic and foreign) to "cruise the net" without limitation. Standards need to be implemented to limit security loopholes and to validate protective measures.

William Miller described the real world with windows of product introduction, marketing preeminence, legacy systems, and the need for incentives over mandates. A subset of industry participants thinks the whole problem may be one of product design, not institutional response. International standardization opens the door for attackers anywhere to plague infrastructure anywhere. It also suggests that the responses should be coordinated internationally.

Technology was not the centerpiece of this conference. To the extent that technology is a major element of protection, a special group should be established on an ongoing basis.

State and Local Participation

Frontline responses may come from those who regulate utilities and provide vital services (emergency medical, police, fire, schools, transportation, etc.). Future conferences should include decision-makers from state and local government, trade associations, and experts sensitive to the dilemmas faced by local personnel. Regulatory leaders could meet with infrastructure-specific specialists (the Electric Power Research Institute, plus state public utility commissions, utilities, IT experts). An ultimate solution will require a clear chain of command and preplanned marching orders.

More governmental discussion is fine, but this is primarily a private industry problem.

Even with post-deregulation industry dynamics, this is a concentrated business. A lot of benefit could come from including key industries in developing appropriate responses to high probability threats. A lot of work on organizations, people, and incentives is needed. Future conferences should actively recruit participants from state and local governments, law enforcement, medicine, education, and regulatory bodies.

International Participation

Our allies are as vulnerable as we are to this kind of attack. We should actively include government and private leaders in future meetings, and seek specific information about response mechanisms, military preparedness, dangerous groups, and multilateral response opportunities.

Everything is global, including markets for security services, threats, etc. Export controls on cryptography should be lifted (recognizing the fact of global utilization of programs such as PGP and the potential profitable business in trusted products). Perhaps rights and responsibilities should be negotiated worldwide (First Amendment, privacy, etc.).

International cooperation requires bridge-building on several matters, including awareness by government officials, industry leaders, researchers, and the public; information-sharing organizations; early warning and response teams; joint funding of certain technologies; and law enforcement cooperation. Similarly, rights and responsibilities must be discussed in light of new technologies and new threats.

Legal Institutions

Comprehensive use of regulations, new laws, and treaties is needed to respond to this problem. Blame should be apportioned in ways that lead to stronger asset protection, in the public interest. An active public/private relationship is needed, given the nature of the control of assets and the overlapping responsibility for national security and infrastructure protection.

Mandates, compliance rules, taxes, and procurement delays are business inhibitors. Institutions should be adapted to the needs of business, with the marketplace as the best regulator.

Legal institutions play a vital role in communicating the rules of the game to all participants. Further research is needed, especially on the topics of liability, insurance, intellectual property protection, espionage prevention, and regulatory reform. For example, Who pays the full costs of power outages? How should criminal and business law interact to protect corporate assets? What jurisdictional issues arise in connection with information warfare?

Past Successes and Failures

An assessment of several national security problems addressed jointly by government and the private sector showed mixed results. This was instructive as to both the diversity of means of cooperation and the difficulty of determining the best response to a problem.

Public/private partnerships have a long and successful history of protecting the country, in times of both war and peace. Airline security was cited as a successful example, while major system procurement was a risky enterprise.

Mandates are a bad idea. The Clipper Chip wars are a classic example of why the government should stay out of the way. In general, private industry believes that private industry is doing just fine.

A great deal more research and analysis is needed here. No good model exists of what this problem is like (it isn't a military situation, it isn't a diplomatic situation, it isn't limited to crime control measures, it doesn't cost much to play, and it crosses all boundaries). Different economic, liability, and policy models should be considered.

Technology

David Cooper of LLNL spoke on the technical potential for enhancing security, through technological and organizational responses. He proposed a program of deterrence, detection, response, and pursuit, but noted that current technological safeguards are "embryonic." He then outlined a futuristic vision of how parallel system technology (a replica system just for hackers to loiter in) and expert systems could be used to trap intruders. As to the cost of the new safeguards, he challenged the audience with a thought-provoking counterpoint: "Can we afford *not* to do this?"

Anything could come at us: cascading system failure; logic bombs; natural disasters; bank robbing on-line; hacker bulletin boards; state-sponsored attacks on population centers; extortion; espionage; weapons system hijacking; EMP devices; or "other." Be prepared.

Very little bad has happened. Better firewalls, bug fixes, and encryption are needed. Commerce needs to be safe. Truck bombs near data centers are not likely to be a problem.

Good models of the Internet and of key infrastructures are needed to develop priorities. Legacy systems will be with us always. People are more important than technology, although the two must be studied together. Only preparedness and study can keep us ahead of the threats.

5.0 Program

Monday, March 10, 1997

8:15–8:30	Continental Breakfast
8:30–9:00	Welcome – *Michael May*
	Purpose of the workshop – *Seymour Goodman, Ronald Lehman*
9:00–9:20	Assuring the critical infrastructure: A public/private sector challenge – *Tom Marsh* (introduction by *Bruce Tarter*)
9:20–9:40	Discussion
9:40–10:20	The capability to do damage: Perspectives on vulnerabilities and threats – *Brenton Greene, Ray L. Leadabrand, Peter Neumann*
10:20–10:45	Discussion
10:45–11:00	Break
11:00–11:30	Enhancing security: Technological and organizational responses – *David Cooper*
11:30–12:00	Enhancing security: Public and private roles in the protection of information-dependent infrastructure – *Stephen Lukasik*
12:00–12:30	Discussion and break
12:30–1:45	Luncheon Speaker: Early thoughts on responses from the information technology industries to government actions or mandates – *William Miller*
1:45–2:15	Lessons from other government efforts to shape civil actions for national security purposes – *David Elliott*
2:15–3:45	Industry Panel: Perspectives from the community of system users, network providers, and hardware and software producers on what government can do to persuade industry to invest in infrastructure protection in the future. What might work? What would not? – *Chair: Guy Copeland*
3:45–4:00	Discussion
4:00–4:10	Break
4:10–4:45	Legal approaches and issues – *Lawrence Greenberg, David Keyes*
4:45–5:00	Discussion
6:00–8:00	Dinner Speaker: *William Owens* (introduction by *William Perry*)

Tuesday, March 11, 1997

8:15–8:30 Continental Breakfast

8:30–9:15 Infrastructure protection: Technology required – *Willis Ware, William Joyce*

9:15–11:00 Workshop roundtable: What do we think we know and don’t know? Where do we need to concentrate our attention? – *Chair: William Perry. Panelists: Edward Feigenbaum, Charles Giancarlo, William Harris, Stephen Lukasik, William Owens*

11:00–11:15 Break

11:15–12:00 Discussion of the next workshop and interim effort. Possibilities to be pursued: interim working groups on prioritized unsettled issues from this workshop; economic approaches to key problems; legal issues; and the international dimensions of the problems.
Co-Chairs: Seymour Goodman and Ronald Lehman

6.0 Participants and Attendees

Principal participants and organizers

David Cooper is Associate Director for Computation at LLNL. Prior to joining Livermore he was with NASA in several capacities concerned with high performance computing. He has been appointed by President Clinton to the newly formed Advisory Committee on High-Performance Computing and Communications, Information Technology, and the Next Generation Internet.

Guy Copeland is with the Computer Sciences Corporation and represents it on the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee (NSTAC). He chairs the NSTAC Information Assurance Task Force and co-chairs its NII Task Force. He also serves with the Information Technologies Association of America.

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.

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, especially expert systems.

Charles Giancarlo is Vice President for Business Development at Cisco, the major manufacturer of network hardware used for the Internet and other major networks.

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 IT-related law.

Brenton Greene is the Commissioner from the Department of Defense. Before joining the Commission he was Director for Infrastructure Policy, Office of the Under Secretary of

Defense for Policy, where he led the DoD staff responsible for plans, programs, and procedures for infrastructure assurance policy and infrastructure warfare.

William Harris, an expert in the field of transportation, is a Commissioner from the private sector. In addition to his consulting practice, he was the Associate Director of the Texas Transportation Institute from 1985 to 1995. His most extensive expertise is in railroad systems.

William Joyce is the Commissioner from the Central Intelligence Agency. Before joining the Commission he held several positions overseas and in Washington where he specialized in the collection and processing of foreign public information and the development of electronic distribution systems.

David Keyes is the Commissioner from the Federal Bureau of Investigation. He has held a wide variety of positions with the FBI during twenty-six years of service, most recently as the Bureau's representative on the Deputy Attorney General's Critical Infrastructure Working Group.

Ray L. Leadabrand is President of Leadabrand and Associates. He was a Senior Vice President of SAIC and SRI International and has extensive experience in the offensive and defensive information warfare arenas, particularly with rf disruption technologies.

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."

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 Converse Government Systems Corp., and serves in various senior capacities for other companies. He is a retired four-star general whose last assignment was as commander of the Air Force Systems Command.

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.

William Miller is Professor of Business and director of the Stanford Computer Industry Project. He is a former Provost of Stanford and a founder of its Computer Science Department, a former President of SRI, and a founder of Smart Valley. He serves on the boards of many high technology companies.

Peter Neumann is a senior staff researcher at SRI who studies computer-related security problems and the full spectrum of risks that may be associated with the use of the information technologies.

William Owens is President of SAIC. Before joining SAIC he was a four-star Admiral and Vice Chairman of the Joint Chiefs of Staff. During his tenure with the JCS, he was one of the principal proponents of the pervasive use of IT in the U.S. military.

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.

Bruce Tarter is the director of Lawrence Livermore National Laboratory.

Willis Ware is a senior staff member at the RAND Corporation who has studied computer-related security problems longer than almost anyone.

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.

Attendees

Janet Abrams, PCCIP Staff
Mitchell Anderson, CSATI
Axel Angely, Ministry of Defense, France
Elizabeth Banker, PCCIP Staff
Dave Bernstein, Stanford
C. K. Chou, LLNL
Ronald Cochran, LLNL
Al Despain, USC and Jasons
Whitfield Diffie, Sun Microsystems
Spiros Dimolitsas, LLNL
Paul Edwards, Stanford
Colin Elrod, Amdahl
Bill Eyres, The Eyres Group
William Firesheets, Bank of America
Lew Franklin, TRW (Retired)
Wendy Freeman, SAIC
Mike Gamble, Argo Systems
Anatole Gershman, Andersen Consulting
Diane Goodman, CISAC Staff
Kevin Harrington, CISAC Staff
Brian Hoey, PCCIP Staff
Dave Johnson, SAIC
Barry Leiner, MCC
Herb Lin, NRC
Ken Malpass, CISAC Staff
Robert Mathews, ICICX
Bill Murray, Deloitte & Touche
Dick O'Neill, OSD(C3I)
Donn Parker, SRI
Donald Prosnitz, LLNL
Michael Rostoker, Kawasaki Microelectronics
Harry Rowen, Stanford
Jeff Rulifson, Sun Microsystems

Paul Saffo, Institute for the Future
Scott Sagan, Stanford
Banani Santra, CISAC Staff
Paul Sedkewicz, Hewlett-Packard
Wayne Shotts, LLNL
Stan Trost, LLNL
Jeffrey Wadsworth, LLNL
Larry Wilcher, U.S. Department of Energy
Dean Wilkening, Stanford

Center for International Security and Arms Control

Stanford University

Please send orders to: Publications, 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).

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).

David Bernstein and Jeffrey Lehrer. *Restructuring of Research Institutes in Russia: The Case of the Central Aerohydrodynamic Research Institute*. 1994 ($14 pages, $4.00).

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).

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

Richard D. DeLauer. *Defense Resource Allocation in the 1990s: A Rational Approach*. 1990 (25 pages, $8.00).

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

Sidney D. Drell and Thomas H. Johnson. *Technical Trends and Strategic Policy*. 1988 (41 pages, $9.00).

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).

John S. Earle and Richard Rose. *Ownership Transformation, Economic Behavior, and Political Attitudes in Russia*. 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).

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).

NEW 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).

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

Liu, Huaqiu. *China and the Neutron Bomb*. 1988 (49 pages, $9.00).

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).

A Program for Strengthening Security and Reducing the Risk of War in the Asian-Pacific Region (text in English and Russian). 1988 (20 pages, $5.00).

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).

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

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).