Critical Information Infrastructure Protection and the Law

AN OVERVIEW OF KEY ISSUES

NATIONAL ACADEMY OF ENGINEERING
NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

Critical Information Infrastructure Protection and the Law

AN OVERVIEW OF KEY ISSUES

Committee on Critical Information Infrastructure Protection and the Law

Computer Science and Telecommunications Board

NATIONAL ACADEMY OF ENGINEERING
NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

Stewart D. Personick and Cynthia A. Patterson, Editors

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided by the National Academy of Engineering. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsor.

International Standard Book Number 0-309-08878-X (book)
International Standard Book Number 0-309-50637-9 (PDF)

Copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, D.C. 20055, (800) 624-6242 or (202) 334-3313 in the Washington metropolitan area. Internet, http://www.nap.edu

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW

STEWART D. PERSONICK, Drexel University, *Chair*
MICHAEL COLLINS, Lockheed Martin
WILLIAM J. COOK, Freeborn & Peters
DEBORAH HURLEY, Harvard University
DANIEL SCHUTZER, Emerging Technologies, Citigroup
W. DAVID SINCOSKIE, Telcordia Technologies
RICHARD R. VERMA, Council on Foreign Relations
MARC J. ZWILLINGER, Sonnenschein Nath & Rosenthal

Staff

CYNTHIA A. PATTERSON, Study Director and Program Officer
MARJORY S. BLUMENTHAL, Director
D.C. DRAKE, Senior Project Assistant

NATIONAL ACADEMY OF ENGINEERING
PROGRAM COMMITTEE

PETER STAUDHAMMER, TRW Inc., *Chair*
RODICA A. BARANESCU, International Truck & Engine Corporation
CORALE L. BRIERLEY, Brierley Consultancy LLC
PALLAB K. CHATTERJEE, i2 Technologies
WOODIE C. FLOWERS, Massachusetts Institute of Technology
GORDON E. FORWARD, TXI
RENATO FUCHS, Transkaryotic Therapies, Inc.
MARTIN E. GLICKSMAN, Rensselaer Polytechnic Institute
THOMAS E. GRAEDEL, Yale University
BRUCE HAJEK, University of Illinois
GEORGE M. HORNBERGER, University of Virginia
KENNETH H. KELLER, University of Minnesota
MARGARET A. LEMONE, National Center for Atmospheric Research
RICHARD J. LIPTON, Georgia Institute of Technology
EUGENE MEIERAN, Intel Corporation
FREDERICK G. POHLAND, University of Pittsburgh
C. PAUL ROBINSON, Sandia National Laboratories
FRIEDER SEIBLE, University of California, San Diego
LAURENCE C. SEIFERT, AT&T Corporation
CHRIS G. WHIPPLE, Environ, Inc.

Ex Officio Members

GEORGE M.C. FISHER, Eastman Kodak Company, NAE Chair
SHEILA WIDNALL, Massachusetts Institute of Technology, NAE Vice President
WM. A. WULF, National Academy of Engineering, President

Staff

PROCTOR REID, National Academy of Engineering, Associate Director, Program Office
JACK FRITZ, National Academy of Engineering, Senior Program Officer, Program Office

Preface

Critical infrastructure protection emerged as a national concern in the late 1990s. The establishment in 1996 of the President's Commission on Critical Infrastructure Protection (PCCIP), its 1997 report *Critical Foundations: Protecting America's Infrastructures*, and the issuance in 1998 of Presidential Decision Directive 63 and the establishment of the Critical Infrastructure Assurance Office (CIAO) promoted awareness of critical infrastructure issues. Among the many forms of critical infrastructure—such as transportation, energy, and water—the information infrastructure, which combines computing and communications systems, stands out as important in its own right and as a crosscutting factor in all other infrastructures. Like power, information infrastructure is a critical infrastructure that all other critical infrastructures depend upon. The Bush administration's review of critical infrastructure protection activities, the tragic events of September 11, and the new national focus on homeland security in general (and cyberterrorism in particular) signal a need for broader reflection, as well as action, on these issues. Progress, however, will require the development of a clear legal framework, in addition to focusing on the technology and current business practices in the public and private sectors.

The National Academy of Engineering asked the Computer Science and Telecommunications Board to organize a symposium to illuminate the range of legal issues and the range of perspectives on issues associated with protection of the critical information infrastructure. CSTB convened the Committee on Critical Information Infrastructure Protection

and the Law (see Appendix A for committee biographies) to undertake the project, asking it to focus on information sharing and liability. While previous CSTB efforts addressed technical, procedural, and policy aspects of [information] security and crisis management, this project emphasizes the role of the law as a barrier to or a facilitator of progress.

The committee met in June 2001 to plan a 2-day symposium, which was held October 22-23, 2001 (the agenda is listed in Appendix B). The committee met again in December 2001 to plan the structure and format of this summary report, which evolved through the end of 2002.

The attacks of September 11, 2001, had a major impact on this project. The tragic events forced some expected participants to cancel their travel, while other initially reluctant parties became willing to participate. The subject matter of the symposium became even more relevant to participants who were not speakers, and the tone and subject matter of presentations and discussions were tailored to and colored by the attacks. As a result, the symposium was larger than anticipated. The discussions were less abstract or hypothetical and more rooted in various realities. Concerns that were expressed at the symposium about issues such as privacy rights and the legal and business risks of sharing information appeared to some committee members to be surprisingly muted. Law enforcement representatives at the symposium expressed a surprising willingness to share information in ways that might impair their ability to prosecute suspected criminals and terrorists, in exchange for improving the ability of the broader community to prevent attacks. The committee does not know if this is a short-lived, politically correct retrenchment or a permanent shift to a new balance of the trade-offs associated with these complex issues.

Meanwhile, responses to September 11 continued to unfold throughout the period in which this report was drafted, greatly complicating the task of describing contemporary conditions and prospects. The dynamism of the situation would make any report with concrete recommendations obsolete before it was published. Against this backdrop, the committee chose to highlight enduring observations, focusing on two issues that could potentially facilitate critical information infrastructure protection efforts—information sharing and the liability of unsecured systems and networks. The committee sought to summarize the debate surrounding use of the Freedom of Information Act (FOIA), antitrust, and liability laws that lie at the heart of critical information infrastructure protection, attempting to maintain that focus in the face of substantial blurring between those issues and the larger set of homeland security issues facing the country. The content of this report reflects the issues identified at the symposium and during subsequent deliberations by the committee. The value of the

report lies in its integration of a very diverse set of perspectives to provide a roadmap and stimulus for future more focused and in-depth inquiries.

The committee is particularly grateful to Wm. A. Wulf, whose commitment to addressing the problems posed by critical infrastructure protection (CIP) and whose recognition that the law presents challenges and opportunities in that arena helped to shape this project. His engagement with members of the National Academy of Engineering (NAE), among them John Harris, and with its program committee provided most of the project's funding.

The committee thanks the symposium participants (see Appendix B for a list of speakers) as well as the many people who responded to its requests for briefings and discussions. Lee Zeichner and Timothy Nagle provided informed discussion on how to frame the project. The committee appreciates the thoughtful comments received from the reviewers of this report. These comments were instrumental in helping the committee to sharpen and improve the report.

The chairman and the entire committee wish to express their deep appreciation for the herculean efforts of the study director, Cynthia Patterson, and the project assistant, David Drake, who performed the lion's share of the work required to organize and run the symposium, to create this report, and to shepherd it through the necessary review and revision processes. We would also like to express our deep appreciation for the guidance, leadership, encouragement, and advice provided to us by Marjory Blumenthal, the director of the Computer Science and Telecommunications Board of the NRC.

Stewart D. Personick, *Chair*
Committee on Critical Information
Infrastructure Protection and the Law

Acknowledgment of Reviewers

This report was reviewed by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's (NRC's) Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the authors and the NRC in making the published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The contents of the review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their participation in the review of this report:

Kent Alexander, Emory University;
David A. Balto, White & Case LLP;
Stanley M. Besen, Charles River Associates;
Nicholas M. Donofrio, IBM Corporation;
Marc D. Goodman, Decision Strategies;
John C. Klensin, AT&T Labs;
David J. Loundy, DePaul University College of Commerce;
Alan B. Morrison, Stanford Law School;
Robert Murphy, Congressional Budget Office;
Debra Pearlstein, Weil, Gotshal & Manges LLP;

Abraham D. Sofaer, Stanford University; and
Suzanne Spaulding, American Bar Association's Standing Committee on Law and National Security.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Chris Sprigman of King & Spalding LLP. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

EXECUTIVE SUMMARY 1

1 INTRODUCTION AND CONTEXT 8
Rise of CIP as a Policy Issue, 9
Events of September 11, 2001, 14
This Report, 15

2 INCREASING THE FLOW OF INFORMATION 17
Information Sharing Framework, 20
(Perceived) Barriers to Information Sharing, 24
Freedom of Information Act, 25
Antitrust, 30
Concluding Observations, 33

3 LIABILITY FOR UNSECURED SYSTEMS AND NETWORKS 35
Criminal Law, 35
Domestic Jurisdiction, 36
International Jurisdiction, 39
Civil Liability, 40
Contract Law, 44
Tort Law, 45
Standards and Best Practices, 50
Regulation, 56

4 MOVING FORWARD 61
Motivating the Private Sector, 62
Market Failure?, 62
Insurance: Motivator for Good Behavior, 65
R&D to Alter the Costs of Security, 66
Awareness, 67
Security and Privacy Tensions, 69
A Trust Network, 72

APPENDIXES

A COMMITTEE MEMBER AND STAFF BIOGRAPHIES 77
B SYMPOSIUM AGENDA 83

Executive Summary

All critical infrastructures (transportation, finance, electric power, water, etc.) are increasingly dependent on the evolving information infrastructure—the public telephone network, the Internet, and terrestrial and satellite wireless networks—for a variety of information management, communications, and control functions. September 11 significantly increased the nation's awareness of the interdependencies of critical infrastructures, and it heightened the government's sense of urgency regarding the need for increased private sector and public sector information sharing with respect to cyber and physical threats. The Committee on Critical Information Infrastructure Protection and the Law held a symposium October 22-23, 2001, to outline issues related to the protection of the critical information infrastructure. This symposium, which had been scheduled well in advance of September 11, was profoundly influenced by those tragic events. Twenty-four presentations, over 2 days, illustrated the wide range of perspectives and concerns that complicate policy making and the development of an adequate legal regime when it comes to critical information infrastructure protection (CIIP). Subsequent crafting of new law and administrative activity under the rubric of homeland security have kept the legal framework for CIIP a moving target. This report examines the range of legal issues associated with information infrastructure protection, particularly those that affect the willingness of private sector companies and organizations to cooperate with the government to prevent, detect, and mitigate cyberattacks. It considers separately different aspects of information sharing and liability—recognizing that

there is a tension between these approaches that strategies for critical information infrastructure protection must ultimately resolve.

INFORMATION SHARING

Although the sharing of information has been the centerpiece of both the government's and the private sector's efforts over the past several years to protect critical information systems, most information sharing still occurs through informal channels. Fundamental questions persist about who should share what information, when, how, why, and with whom. One reason for the lack of progress, according to private industry representatives, has been the lack of clarity regarding the benefits and associated liabilities in sharing information within and between industry sectors and with the government. For example, information sharing could lead to allegations of price fixing, restraint of trade, or systematic discrimination against certain customers; it could raise privacy concerns, expose proprietary corporate secrets, or reveal weaknesses and vulnerabilities that erode consumer confidence and invite hackers. Overcoming these concerns requires an informed position on the existing legal framework—an imperfect understanding of the law is both excuse and explanation for some observed limits to sharing.

Freedom of Information Act

Many private sector companies believe that proprietary CIIP-related information shared with federal government entities may be disclosed to third parties under the Freedom of Information Act (FOIA). Therefore, private sector companies have proposed amending FOIA to create a new exemption that would protect critical infrastructure information from disclosure. Opponents of such an exemption argue that the case law and agency interpretations demonstrate that the information—that is, information that is a trade secret or information that is commercial or financial, obtained from a person, and privileged or confidential—already is protected under the existing FOIA Exemption 4. Changing the FOIA, opponents argue, could upset the existing FOIA framework and open up the possibility for new litigation. Although the Homeland Security Act of 2002 did feature such an exemption, the fundamental issues remain.

A key problem is whether the federal government has the processes in place to protect information that should be protected under existing FOIA rules from inappropriate or accidental disclosure. The government may need to strengthen its formal controls on disclosure of information under FOIA, disclose to the private sector what those controls entail, and

strengthen its programs to better educate federal agency employees (who respond to the FOIA requests) about the types of information that cannot be released under existing law.

Antitrust Law

An additional concern of many in the private sector is that sharing CIIP-related data with competitors could be viewed as a violation of the provisions of the Sherman Antitrust Act. As a result, many in the private sector have called for a new antitrust exemption. Opponents argue that a new exemption is not needed to protect firms from allegations of anti-competitive behavior. They suggest that firms can obtain informal legal advice from antitrust experts or formal advice from the Department of Justice—in the form of a business review letter—on whether its proposed future conduct would be viewed as a violation of the antitrust laws. In addition, an exemption would create a new body of law that would upset 30 years of case history and lead to years of new litigation. Hence, the American Bar Association opposes new antitrust exemptions. Like FOIA, the existing antitrust law does not prevent the private sector from sharing critical infrastructure information. However, because official reviews of proposed information sharing activities require time and money to obtain, the use of such reviews may be a barrier to the types of ad hoc information sharing that are most likely to uncover well-planned attacks on the infrastructure. Also, as with FOIA, there are persistent perception problems related to what may be deemed permissible and what may be deemed illegal.

LIABILITY

Experts observe that criminal law alone is not sufficient to deter hackers and prevent cybercrime; civil liability is necessary to ensure proper disincentives are in place to deter would-be cybercriminals. Ideally, civil liability allows a victim to recover losses from third parties if such parties were negligent or engaged in intentional misconduct and if such negligence or misconduct was the proximate cause of the loss. Because contract law does not provide an adequate remedy for third parties that have no privity of contract, many experts have suggested the use of tort law as a model for computer-related cases. Proponents of tort liability argue that companies that control the computer networks are in the best position to implement appropriate security measures. If a company knows or has reason to know that its computer network is being used to cause harm, and it has the capacity to stop such harm from occurring, the company could be subject to liability if it does not take some corrective action. The

applicability of tort law and the potential for civil lawsuits and monetary damages could encourage companies to invest in computer security measures. Debate continues in the private sector on whether there is a legal duty on the part of the company to secure its critical information infrastructure.

Standards, Best Practices, and Audits

Establishment of operational best practices for network administrators and users, combined with ongoing training and enforcement of the practices through random tests, is one possible way of increasing computer security. An obvious option is for firms to begin immediately to share best practices, including attack scenarios and practices to protect against these attacks. Best practices should focus on policies that improve computer network security rather than on procedures and rituals, which only create a perception of protection. In addition to playing a role in tort liability determinations, best practices can also serve as a benchmark against which firms can be audited. Routine audits based on well-accepted principles of testing and analysis, principles that need to be developed for computer security, can help firms avoid litigation or reduce liability.

As a force motivating industry to adopt best practices, tort law can be a significant complement to standard-setting practices, since compliance with industry-wide standards is often an acceptable demonstration of due care. If tort liability were more directly applicable in computer security cases, implementing security standards would be a way for a company to minimize its liability. Adopting a nationally recognized computer security standard of care is not, however, a simple process, owing to the evolving nature of security vulnerabilities and the diverse players that have an Internet presence. In addition, the meaning of "reasonable care" is never static, and firms must adapt the standard as technology changes.

The Participants

Because legal liability often depends on which actors are best positioned to prevent the harmful activities (in this case, computer attacks), some experts suggest that the diverse entities in the Internet community should not all be held to the same standard of care with respect to computer network security. Given that certain Internet Service Providers (ISPs) may know (or should know) about risks and have the capability to mitigate attacks, many experts suggest that ISPs should face significant liability if their systems are insecure. It is possible to reduce (although not

eliminate) the frequency and severity of errors through the use of tools and testing methods prior to the release of a product. If the use of such tools and testing methods were part of industry-accepted best practices, it would be possible for vendors who do not perform such tests to face greater exposure under theories of negligence. Allowing vendors to be held liable for negligence may change the cost-benefit calculation, encouraging the development and delivery of more secure computer products.

Home users represent an important source of potential security hazards (as well as potential victims) since they often do not have the knowledge or expertise needed to secure their computers to prevent hackers from using them in a denial-of-service attack. Efforts to educate home users about the use of firewalls or antivirus software undoubtedly will help, but thought should be given to assigning liability to those other entities who are best positioned to mitigate the risks related to the systems and services used in the home.

Regulation

The patchwork of regulations relevant to CIIP complicates efforts to develop a regulatory framework for critical infrastructure protection. The Gramm-Leach-Bliley Act (GLB), which resulted in regulations promulgated by several government agencies (including the banking agencies, the Securities and Exchange Commission, and the Federal Trade Commission), outlines the responsibilities of financial institutions with regard to protecting consumer privacy. The GLB-implementing regulations help set the stage for best practices and may become a de facto standard in assessing negligence liability. Regulatory compliance and the desire to avoid new regulations serve both to require and to motivate all parties to pay more serious attention to securing our critical infrastructure against cybercrime. The mere threat of such regulation could motivate vendors and corporations to self-regulate, providing their own standards and audit policies. The heightened interest in private sector Information Sharing and Analysis Centers (ISACs) in the last few years is a sign of movement toward self-regulation. The government could periodically review such self-regulation efforts and provide reports showing deficiencies that would need to be corrected by a given deadline if regulation is to be avoided. The Federal Trade Commission, for example, has done this for Web site privacy policies. Another approach to encouraging companies to protect the critical infrastructures that they own and operate is to adopt requirements for disclosing the steps that have been taken to evaluate risks and mitigate them, similar to the requirements of the Securities and Exchange Commission for Y2K.

THE BIG PICTURE

The legal framework for critical information infrastructure protection must be considered in the larger context of the business, social, and technical environment. The increasing dependence on common technology and interconnected systems suggests that many of the technical vulnerabilities can be overcome only through collective, concerted action. Externalities are common in computer network security; the incentive that one network owner has to invest in security measures is reduced if the owner believes that other connected networks are insecure. Insurance can play a role in motivating the private sector by transferring the risk of computer security losses from a company to the insurance carrier. The few cyber insurance policies in effect today require companies to employ appropriate security measures. Most policies also require firms to undergo an initial independent security evaluation of network defenses and ongoing intrusion-detection tests during the life of the policy.

Prior to September 11 the security of information systems and the protection of personal data and privacy were considered to be mutually reinforcing and compatible goals. Many experts suggest that the crisis-management mentality in the aftermath of September 11 has pushed aside issues of privacy and civil liberties. Technical mechanisms proposed to aid government efforts in the war on terrorism appear, to some, to sacrifice privacy and civil liberties for only the illusion of an increased ability to protect the nation's infrastructures. Mechanisms should be implemented to ensure that surveillance conducted to combat terrorists and hackers does not result in a loss of privacy for innocent citizens. Symposium participants noted that the seriousness and urgency of protecting the nation's infrastructures make it even more important to protect well-established constitutional and statutory principles of privacy and civil liberties in crafting a solution.

Trust among those sharing information is one of the most important prerequisites for successfully protecting the nation's critical information infrastructures. Trust is necessary to achieve an atmosphere of openness and cooperation. Although trust has been a central component of the government's CIIP efforts over the past several years, the government has failed to build sufficient trust between the public sector and the private sector for four reasons. First, the government's message to the private sector has vacillated—at times it stresses national security, at other times, economic vitality—raising concerns about whether the priority of the day will trump prior promises. Second, the government has so many focal points for CIIP that firms often do not know which agency to contact or what authority and established processes underpin the promises of that agency to protect information from disclosure. Third, the government has been slow to reciprocate in sharing information with the private sector.

Finally, in the aftermath of September 11, the government took actions that produce a perception (right or wrong) that it may unilaterally suspend prior agreements with respect to the nondisclosure of information if it deems that circumstances warrant. The government should clearly and consistently explain to the private sector what its objectives are for CIIP, how it has organized itself to accomplish those objectives, what the information flows are, what kind of information should be shared and in what form, what the government is willing to share with the private sector, and why all of this is important (i.e., what the threat is, and how the proposed actions will address that threat). This message should clearly and consistently articulate what protections already exist for information sharing and what safe harbors exist (or will be established) to encourage information sharing in light of FOIA and antitrust concerns in the private sector. Consolidation of critical infrastructure protection functions in the new Department of Homeland Security will create a focal point; the tasks of clarifying the policies and communicating with the public remain. A clear and consistent message from the government to the private sector will go a long way toward building the trust that is necessary to protect the nation's critical information infrastructures.

1

Introduction and Context

The information infrastructure is the combination of computer and communications systems that serve as the underlying infrastructure for organizations, industries, and the economy.[1] All critical infrastructures (e.g., transportation and electric power) are increasingly dependent on telecommunications—the public telephone network, the Internet, and terrestrial and satellite wireless networks—and associated computing assets for a variety of information management, communications, and control functions.[2] Private industry and other organizations, in turn, depend directly on their own information infrastructures and on various critical infrastructures. This dependence has a national security component, since information infrastructure undergirds and enables both economic vitality and military and civilian government operations. In particular, the government and military information infrastructures depend on commercial telecommunications providers for everything from logistics and transport to personnel and travel functions.[3] The importance of the telephone system during crises was recognized 40 years ago, when President Kennedy established the National Communications System (NCS) to pro-

[1]Computer Science and Telecommunications Board, National Research Council. 1999. *Trust in Cyberspace*. National Academy Press, Washington, D.C.

[2]An information infrastructure includes not only the networks but also the network management systems, such as the Domain Name System.

[3]Based on a presentation by Colonel Timothy Gibson, U.S. Army, at the symposium on October 22, 2001.

vide better communications support to critical government functions during emergencies.[4] That provided an important basis for an expanding set of activities associated with national security and emergency preparedness (NS/EP) communications. The rise of the Internet has introduced new elements—systems, applications, and players—into the conceptualization of critical information infrastructure and policy options for its protection.

Issues in the protection of critical information infrastructure were the focus of an October 2001 symposium and subsequent discussions by the Committee on Critical Information Infrastructure Protection and the Law, which form the basis of this report. Twenty-four speakers presented topics ranging from information sharing to legal issues (see Appendix B for the agenda and speakers). The quotations (and attributed ideas) from participants in the symposium that are included in this report illustrate the wide range of perspectives and concerns that complicate policy making when it comes to critical information infrastructure protection (CIIP).

RISE OF CIP AS A POLICY ISSUE

The President's Commission on Critical Infrastructure Protection (PCCIP) was created in 1996 to assess the physical and cyberthreats to the nation's critical infrastructures and to develop a strategy to protect them.[5] Certain infrastructures—telecommunications, electric power, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services, and government services—were deemed so critical that their "incapacity or destruction would have a debilitating impact on the defense and economic security"[6] of the United States. Box 1.1 provides an overview of the key critical infrastructure protection (CIP) activities over the past several years. Early efforts were dominated by a focus on national security, emergency preparedness, and law enforcement, although from the beginning outreach to industry was attempted. Because of the private ownership of critical infrastructures and the prominence of private parties in the use of these infrastructures, forming public-private partnerships was thought to be one of the keys to CIP progress. The leadership role was assigned to the Critical Infrastructure Assurance Office (CIAO), although its placement within the Department of Commerce (with limited resources and authority) resulted in programs that

[4]Information about the presidential memorandum signed on August 21, 1963, to establish the NCS is available online at <http://www.ncs.gov/ncs/html/NCSHistoryBkgrd.html>.

[5]President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations*. Washington, D.C.

[6]Ibid., p. 19.

BOX 1.1
Brief History of the Nation's
Critical Infrastructure Protection Activities

Pre-PCCIP

After communications problems between critical entities threatened to heighten the Cuban missile crisis, President Kennedy appointed a commission to investigate underlying problems and recommend a solution. The commission recommended a unified emergency communications capability, and President Kennedy formally established the National Communications System (NCS) by a presidential memorandum on August 21, 1963. NCS is an interagency organization whose mission is to ensure reliability and availability of national security and emergency preparedness communications. President Reagan and President Bush broadened the NCS's national security and emergency preparedness (NS/EP) capabilities with Executive Order 12472 in 1984 and Executive Order 13231 in 2001.[1]

After recognizing that the private sector needed to be included in infrastructure protection efforts, President Reagan created the National Security Telecommunications Advisory Committee (NSTAC)[2] by Executive Order 12382 in September 1982. Composed of up to 30 industry chief executives, NSTAC provides industry-based expertise to the President on issues related to implementing NS/EP communications policy.

The National Coordinating Center (NCC) was established in 1984 as a result of a NSTAC recommendation to develop a joint government-industry national information-sharing mechanism for NS/EP communications. In January 2000, NSTAC expanded NCC's responsibilities to include functioning as the Information Sharing and Analysis Center (ISAC) for the telecommunications sector.

Following the Morris Internet worm incident in November 1988, the federally funded CERT Coordination Center (CERT/CC)[3] was established at the Software Engineering Institute (SEI) at Carnegie Mellon University to coordinate communication among experts during security emergencies and to help prevent future incidents. CERT/CC's role has expanded to include handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing and publishing security practices to ensure the survivability of networked systems. Other focused CERTs have been established too.

President's Commission on Critical Infrastructure Protection

In the wake of the Oklahoma City bombing in 1995, President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP)[4] in July 1996 by Presidential Executive Order 13010. PCCIP was the first comprehensive effort to address the vulnerabilities of national critical infrastructures. Divided into five sectors (Information and Communications; Physical Distribution; Energy, Banking and Finance; and Vital Human Services) to evaluate risks, threats, and vulnerabilities, the PCCIP formulated a national strategy for protecting critical infrastructures from physical and cyber threats. In its 1997 report *Critical Foundations: Protecting America's Infrastructures*, PCCIP recommended several components to protect critical infrastructures: a top-level policy-making office in the White House, councils composed of industry executives and government leaders at all levels, education and awareness programs and federal research and

development programs, industry information clearinghouses, public-private partnerships, a real-time attack warning capability, and a streamlining of the legal tenets that address infrastructure issues, updated to keep pace with technology advances. After submitting its report, the PCCIP was dissolved.

Presidential Decision Directive 63

Presidential Decision Directive 63 (PDD-63),[5] issued by President Clinton on May 22, 1998, created a national structure to accomplish the goals laid out in the PCCIP's report. PDD-63 created the office of national coordinator at the National Security Council to serve as the top-level office in the White House to guide policy for federal agencies and advise nongovernmental entities on protective measures for the nation's information infrastructure. The Critical Infrastructure Assurance Office (CIAO)[6] was formed at the Department of Commerce to provide support to the national coordinator's work with government agencies and the private sector in developing a national plan. CIAO serves a number of functions, including coordinating a national education and awareness program, administering legislative and public affairs, and assisting in developing long-term research. Project Matrix, a CIAO program, was designed to identify and characterize the assets and associated infrastructure dependencies and interdependencies among and between federal agencies and the private sector.

To facilitate real-time warnings, PDD-63 established the National Infrastructure Protection Center (NIPC), an interagency unit at the FBI, to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against critical infrastructures. NIPC created the InfraGard initiative to facilitate the sharing of information on cyber intrusions, exploited vulnerabilities, and infrastructure threats with private sector infrastructure owners and operators.[7] Members have access to an Alert Network and a secure Web site to voluntarily report intrusions, disruptions, and vulnerabilities of information systems.

The Federal Computer Incident Response Center (FedCIRC),[8] the federal civilian agencies' focal point for computer security incident reporting, provides assistance with incident prevention and response.

The National Plan for Information Systems Protection Version 1.0,[9] released in January 2000 by President Bill Clinton and Richard Clarke (then the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism), focused on tightening cybersecurity in the federal government and promoting public-private partnerships. Version 1.0 of the National Plan addresses the complex interagency process for approaching critical infrastructure and cyberrelated issues in the federal government. Progress on Version 2.0 carried into the Bush administration but was superseded by new activities carried out in response to September 11 (see below).

In response to encouragement from the government, private industry began forming sector-specific ISACs to facilitate sharing critical infrastructure information between companies in a given industry and between private industry and the government (for more on ISACs, see Chapter 2). Another private sector initiative, the Partnership for Critical Infrastructure Security (PCIS),[10] was established in December 1999 as a public-private forum to address issues relating to infrastructure security. PCIS, incorporated as a nonprofit organization in February 2001, is operated by companies and private sector associations representing each of the critical infrastructure industries.

continued

BOX 1.1 Continued

Since September 11

In response to the September 11 attacks, President Bush extended and amplified PDD-63 in Executive Order 13231, replacing the earlier Executive Order 13010. E.O. 13231 established the Critical Infrastructure Protection Board. The board recommends policies and coordinates programs for protecting information systems for critical infrastructure through outreach on critical infrastructure protection issues with private sector organizations; information sharing; the recruitment, retention, and training of executive branch security professionals; law enforcement coordination; research and development; international information infrastructure protection; and legislation. The board consults with affected executive branch departments and agencies and communicates with state and local governments and the private sector, as well as communities and representatives from academia and other relevant elements of society. The board coordinated with the Office of Homeland Security (OHS) on information infrastructure protection functions that had been assigned to the OHS by Executive Order 13228 of October 8, 2001.

The board is chaired by the special advisor to the president for cyberspace security (often referred to as the cybersecurity czar). This office replaced the national coordinator. As cybersecurity czar, Richard Clarke now reports to both the assistant to the President for national security affairs and to the assistant to the President for homeland security.[11] The director of CIAO was also appointed as a member of the board.

In February 2003 the Directorate of Information Analysis and Infrastructure Protection in the Department of Homeland Security absorbed CIAO, NIPC, FedCIRC, and the National Communications System,[12] but the InfraGard program remained in the FBI. An Executive Order issued on February 28, 2003, abolished the President's Critical Infrastructure Protection Board, but a special coordinating committee may be created to replace it.[13]

---

[1]More information on the NCS is available online at <http://www.ncs.gov/>.

[2]More information on the NSTAC is available online at <http://www.ncs.gov/nstac/nstac.htm>.

[3]More information on CERT is available online at <http://www.cert.org>.

[4]See <http://www.ciao.gov/resource/pccip/intro.pdf> and <http://www.info-sec.com/pccip/web/backgrd.html>.

[5]For more information on PDD-63: <http://www.fas.org/irp/offdocs/pdd-63.htm>.

[6]More information on CIAO is available online at <http://www.ciao.gov>.

[7]More information on NIPC and InfraGard is available online at <http://www.nipc.gov> and <http://www.infragard.net/>.

[8]More information on FedCIRC is available online at <http://www.fedcirc.gov>.

[9]The National Plan is available at <http://www.ciao.gov/publicaffairs/np1final.pdf>.

[10]More information on PCIS is available online at <http://www.pcis-forum.org>.

[11]For more information, <http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html>.

[12]Michael Fitzgerald. 2003. "Homeland Cybersecurity Efforts Doubled." *Security Focus*. March 11.

[13]Diane Frank. 2003. "Filling the Cybersecurity Void." *Federal Computer Week*. March 6.

focused on generating awareness in the private sector of critical infrastructure vulnerabilities and exhorting communication between industry and the government—and within industry—about infrastructure weaknesses and incidences of attacks and other failures. Until September 11, 2001, the backdrop for these efforts was a steady rise in hacking incidents and computer crime.[7] Estimates from market researchers, publicized large-scale incidents (such as the distributed denial-of-service attacks of early 2001), growth in the sales of antivirus software and firewalls, and growth in prosecutions of computer crimes are among the indicators that the need to protect information infrastructure had begun to attract more attention by the beginning of this century—albeit less than security experts would have liked to see.

In 2002, development of the National Strategy to Secure Cyberspace provided a focal point for Bush administration efforts in critical information infrastructure protection. Originally, the administration had planned to release the report in its final version in September 2002; however, ongoing negotiations between the administration and the other parties involved in the strategy's formulation led to the draft version and a 60-day comment period in which input at all levels was solicited. The administration also convened a number of town-hall meetings across the country to gather additional input. Early drafts included proposals to suspend wireless Internet service until security holes were addressed, require Internet service providers to include firewall software, recommend that government agencies use their power as a major purchaser of computer software to push software vendors to improve the security of their products, provide financial incentives for vendors to improve the security of their products, and impose legal liability for failing to meet basic security standards.[9] However, the final version, released February 14, 2003, scaled back on the government's role and emphasized voluntary industry initia-

[7]Computer crime, or cybercrime, can encompass a wide range of situations involving IT in the context of crime. The absence of a definition is problematic and often hampers cooperation and funding, not to mention legal cooperation and policy coordination. There are important differences (both in the challenges and the solutions) between protecting networks from attacks by hackers and protecting them from a resourceful, determined adversary. For an in-depth look at the use of information technology to protect against the threat of catastrophic terrorism, see Computer Science and Telecommunications Board, National Research Council. 2003. *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. The National Academies Press, Washington, D.C.

[8]Available online at <http://www.whitehouse.gov/pcipb>.

[9]Jonathan Krim. 2003. "Cyber-Security Strategy Depends on Power of Suggestion." *Washington Post*, February 15, p. E01.

tives.[10] Consumer education, partnership between the private and public sector, and investment in research are among the proposals in the final cyberspace plan.

Events of September 11, 2001

The terrorist attacks of September 11, 2001, resulted in a massive destruction of property and loss of human life, but the attacks also demonstrated the vulnerability of America's information infrastructure and its importance to crisis management.[11] In the wake of those events, experts noted that attacks on information infrastructure can amplify the effects of attacks on physical infrastructure and interfere with response activities, such as by overloading surviving communications networks.[12] Ronald Dick, then director of the National Infrastructure Protection Center (NIPC), noted at the symposium that September 11 had increased awareness of the interdependencies of critical infrastructures and heightened the sense of urgency surrounding information sharing on cyber and physical threats. For example, Mr. Dick commented that NIPC was holding multiple daily briefings with the electric power and financial services ISACs to provide threat and vulnerability assessments.

Legislative initiatives have been prominent among the responses to September 11. Although those responses have been framed as supporting "homeland security," several policy measures were introduced that recognized the importance of critical infrastructures to national security. The USA PATRIOT Act,[13] enacted in October 2001, calls for actions necessary to protect critical infrastructures to be carried out by a public-private partnership. The Office of Homeland Security (OHS) was established by executive Order 13228 and was tasked with coordinating efforts to protect critical infrastructures. Executive Order 13231 established the President's Critical Infrastructure Protection Board on October 16, 2001 (it was abolished on February 28, 2003). A new position, the special advisor to the President on cyberspace security, was established to provide leadership in the protection of information infrastructure, and that function was

[10]Jennifer Lee. 2003. "White House Scales Back Cyberspace Plan." *New York Times*, February 15, p. A12.

[11]Computer Science and Telecommunications Board, National Research Council. 2002. *Internet Under Crisis Conditions: Learning from September 11.* National Academy Press, Washington, D.C.

[12]National Research Council. 2002. *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* National Academy Press, Washington, D.C.

[13]PL 107-56.

integrated with the evolving activities of both the OHS and the National Security Council and coordinated with relevant activities associated with the Office of Science and Technology Policy. Executive Order 13231 also places more emphasis on cooperation with the private sector. This raises questions about the role of government, as well as that of industry, in achieving cooperation. The new team of cybersecurity leaders began to develop a cybersecurity strategic plan, echoing earlier efforts to develop CIP strategic plans. Both early 2002 proposals for consolidating the functions associated with CIP into OHS and mid-2002 proposals for organizing a new Department of Homeland Security have created some confusion about who is in charge of CIP activities. A recent General Accounting Office (GAO) report[14] found that over 50 organizations (including five advisory committees; six organizations in the Executive Office of the President; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and three other organizations) are involved in CIP. Adding in state and local entities would greatly enlarge the total number. As the establishment of the Department of Homeland Security in early 2003 underscores, the organizational structure of CIP—and within it, CIIP—may continue to evolve for quite some time, and the form it eventually takes will determine the extent to which infrastructure protection is singled out from or integrated within other elements of homeland, national, and economic security. The organizational approach may interact, in turn, with policy decisions about the role of law, technology, and procedure in addressing CIP/CIIP needs. Current trends suggest that law will play a growing role, inasmuch as the increasing focus on homeland security seems to have accelerated the formation and implementation of relevant laws.

THIS REPORT

This report examines legal issues[15] associated with information infrastructure protection, with an emphasis on information sharing and liability. It is not a general description of computer crime or cybercrime. Since the private sector owns the majority of the critical infrastructures, the

[14]U.S. General Accounting Office. *Critical Infrastructure Protection: Significant Challenges Need to Be Addressed*. GAO-02-961T. July 24, 2002.

[15]The PCCIP issued a series of reports, known as the Legal Foundations reports, that identified many legal issues associated with information assurance, including the Freedom of Information Act (FOIA), antitrust, tort liability, the Defense Production Act, and the Stafford Act. These reports are available online at the CIAO Web site <http://www.ciao.gov/resource/pccip/pccip_documents.htm>.

laws examined are those that affect the willingness of industry to cooperate with the government to prevent, detect, and mitigate attacks. A central issue is the framework for sharing information associated with information system vulnerabilities and their exploitation. Security experts would like to see more such sharing, and private parties and some government agencies have been reluctant to comply. Chapter 2 outlines the situation and comments on the two laws most frequently cited as discouraging information sharing: the Freedom of Information Act and the antitrust laws. Although the intent of criminal law is to deter future crime and punish perpetrators, some experts suggest that it is not sufficient to prevent attacks on the nation's critical information infrastructures. The ability to impose civil damages on infrastructure owners who are proven negligent could motivate them to invest the necessary resources to improve the security of the nation's information infrastructures. Chapter 3 discusses where liability currently lies for producing, maintaining, or operating unsecured systems and networks, and how changing the assignment of liability could contribute to infrastructure protection. The final chapter examines the larger business, social, and technical context. The report identifies issues and differences of opinion, providing an overview rather than an exhaustive analysis.

The symposium noted that privacy and civil liberties could become casualties to more aggressive CIP/CIIP, depending on how legal mechanisms are designed and enforced. These concerns have grown since that time owing to new legislative and administrative developments, noted in Chapter 4. This report notes the tension between security and civil liberties but given the limited resources of the project does not address them in detail.

2

Increasing the Flow of Information

The sharing of information has been the centerpiece of both the government's and the private sector's efforts over the past several years to protect the information systems underlying our critical infrastructures. The assumption is that information sharing can help crystallize the threat, identify vulnerabilities, devise better defenses, establish best practices, and detect and mitigate attacks. Eric Benhamou, chairman of 3Com, suggests that the one thing that would have the greatest return is for firms to begin immediately sharing information about attack scenarios, best practices to protect against attacks, and perpetrators. The most useful thing the government can do, according to Craig Silliman, director of the Network and Facilities Legal Team at WorldCom, is to facilitate the establishment of a single technical point of contact that would enable the administrators at the backbone ISPs to share, in real time, information to combat a cross-industry attack (such as Code Red[1] or Nimda[2]). Coordi-

[1]Code Red was a worm that exploited buffer overflow vulnerabilities in unpatched versions of Internet Information Server (IIS) Web software. Several variants of the worm spread throughout the world in the summer of 2001. Infected hosts were used to launch distributed denial-of-service attacks and deface Web pages. Information about the vulnerability was released in mid-June of 2001 and the worm began spreading in mid-July. The Cooperative Association for Internet Data Analysis (CAIDA) provides an analysis of the Code Red worm at <http://www.caida.org/analysis/security/code-red/>.

[2]The Nimda worm exploited the same vulnerability in IIS Web servers that Code Red used. Nimda, which spread via e-mail, network scanning, and Web surfing, modified files on the infected systems and caused denial of service. See the CERT Advisory for more information, <http://www.cert.org/advisories/CA-2001-26.html>.

nation among the technical experts during a distributed denial-of-service (DDOS) attack, for example, would help them to identify the source of an attack, identify potential solutions to block the attack, and restore the network to operational capacity more quickly.[3] Informal communication and coordination do take place, but there is interest in increasing the scope and scale of such activity, in tandem with the evolution of the Internet itself.

The federal government has made a number of attempts to promote information sharing relevant to critical information infrastructure protection. NIPC created the InfraGard initiative to facilitate the sharing of critical infrastructure information with the private sector. Ronald Dick suggests that confidentiality in the reporting of incidents is one of the key elements in the InfraGard program that help to build trust between the government and private sector entities. However, the General Accounting Office (GAO) reported[4] that NIPC has had mixed success in forming partnerships with private industry and other government agencies. The President's Commission on Critical Infrastructure Protection recommended industry-based vehicles known as information sharing and analysis centers (ISACs, see Box 2.1). While several ISACs have been created, many are still in their infancy and many others are in the planning stages. GAO notes that only three ISACs had been created before December 2000.[5] Although formal information-sharing arrangements are slowly being established, most information sharing occurs through informal channels. One deterrent, according to private industry representatives, has been the lack of clarity regarding the benefits and associated liabilities in sharing information with one another and with the government.

Whitfield Diffie, Distinguished Engineer at Sun Microsystems, notes that regulated industries have a tradition of sharing some information with the government and the public, even when disclosure puts them at a disadvantage from a business viewpoint. For example, airlines are required (upon request) to disclose arrival and departure times of all flights, even though it is clearly a disadvantage to have the customers know that they are frequently late. Retailers and credit card issuers worry that disclosing any loss of online transactional security (e.g., hackers gaining access to

[3]Because an attacker has the advantage of being able to deliberately exploit any weakness that he can identify, network administrators need to be able to rapidly disseminate any information while the attack is under way to recapture the advantage and prevent the attack from succeeding.

[4]U.S. General Accounting Office, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities," GAO-01-323, April 25, 2001.

[5]U.S. General Accounting Office, "Information Sharing Practices That Can Benefit Critical Infrastructure Protection," GAO-02-24, October 15, 2001.

BOX 2.1
Information Sharing and Analysis Centers

PDD-63 called for the creation of sector-specific information sharing and analysis centers (ISACs) to encourage industry to gather, analyze, sanitize, and disseminate information to both industry and, as deemed appropriate, the government. ISACs have now been created in several industry sectors, including financial services, information technology, electric power, telecommunications, chemical, and surface transportation (rail industry). Each ISAC operates independently and determines what corporate structure to adopt, how it should operate, and how it should share information with its own members, with other ISACs, and with the government. For example, the financial services ISAC (FS-ISAC) is a nonprofit corporation open to eligible members of the banking, securities, and insurance industries.[1] FS-ISAC members can submit either anonymous or attributed reports about information security threats, vulnerabilities, incidents, and solutions. Members have access to information provided by other members and analysis of information obtained from other sources (including the U.S. government and law enforcement agencies and the CERT Coordination Center). Although the FS-ISAC does not allow any U.S. government agency, regulator, or law enforcement agency to access their members' information, it does share information with the government and other ISACs through meetings and other arrangements.[2] By contrast, the National Coordinating Center for Telecommunications ISAC (NCC-ISAC) brings together industry and government participants in a government facility.

[1]According to the FS-ISAC Web site, "[m]embership is open to the following categories of U.S. entities registered, and in good standing, with their appropriate regulators: FDIC Insured Bank, NASD Licensed investment firm, Designated Financial Services exchanges and finance sector utilities, Specialized U.S. or state-licensed banking companies, U.S. or state-licensed Insurance companies." See <http://www.fsisac.com/faq.cfm>.

[2]See <http://www.fsisac.com/aboutus.cfm>.

credit card numbers or purchase history) may undermine public confidence in Internet commerce, to the detriment of their businesses. However, the companies that own and operate the information infrastructures include both regulated telecommunications providers and others, such as cable and other ISPs, who are regulated differently, if at all. Although the traditional telecommunications players have a history of successful information sharing with each other and the government through the NSTAC/NCC, the telecommunications industry is changing. The convergence of voice and data networks is enlarging the number of players involved in the telecommunications sector. W. David Sincoskie, committee member and vice president of the Internet Architecture Research Laboratory at Telcordia Technologies, noted that the Internet now carries more traffic than the public switched telephone network (PSTN). Captain J. Katharine

Burton (U.S. Navy), assistant deputy manager at the National Communications System, noted that wireless networks, a new and important component of national security and emergency preparedness activities, did not have the ability to give priority to national security applications during the September 11, 2001, crisis.[6] A lesson from the wireless experience on 9/11 may be to think early about how to incorporate new and emerging media into emergency response. Unlike the traditional telecommunications players, these new players (including the owners and operators of the Internet, wireless networks, and the underlying transmission networks)[7] do not have 40 years of established history, nor do they have a culture of sharing information for national security purposes.

INFORMATION SHARING FRAMEWORK

Information sharing remains an ambiguous, even an opportunistic concept. One reason progress may be slow is that what it means depends on what is asked of whom. Fundamental questions persist about who should share what information, when, how, and why—as well as with whom. Note that in the middle of the last century, these questions were obviated by the domination of the telecommunications and computer industries by single large players with whom the government could—and did—communicate in the event of a crisis. They first surfaced in the early 1980s, when the telecommunications industry was transformed by the AT&T modified final judgment, which led to a relatively effective vehicle for government communications with the regulated telecommunications providers (NSTAC); government efforts to communicate with

[6]In 1995, the President directed the National Communications System, in cooperation with industry, to implement a priority access service for wireless NS/EP users. The FCC responded in July 2000 with a "Report and Order" that made wireless access priority service voluntary (see <ftp://www.fcc.gov/pub/Bureaus/Wireless/Orders/2000/fcc00242.txt>). In response to the events of September 11, the National Security Council issued guidance to the National Communication System to provide immediate wireless priority access service to limited geographic areas. Initial operating capability for the NCS Wireless Priority Service (WPS) was achieved in December 2002. Nationwide end-to-end wireless priority communications capability for all NS/EP personnel is scheduled for December 2003. WPS complements the Government Emergency Telecommunications Service (GETS), which provides landline priority service to NS/EP personnel. More information is available online at <http://63.121.95.245/wps/> and <http://gets.ncs.gov/>.

[7]There are also many more of these actors than there were before, and there are practically no barriers to entry. Because a potential attacker could easily establish an ISP (either within U.S. territory or outside it), information sharing among ISPs (or between ISPs and the government) might result in unfortunate or even damaging disclosures. The increasing number of players in the telecommunications sector needs to be considered when developing information-sharing strategies.

the computer industries about computer security risks in the 1980s did not fare as well, for a variety of reasons, including difficulties in formulating a compelling message and in reaching and persuading an increasingly diffuse set of industries. Many of these problems persist in today's CIIP efforts.

In thinking about *what* information should be shared,[8] Lieutenant General (retired) David J. Kelley, vice president of Information Operations at Lockheed Martin, suggested that threats, vulnerabilities, network status, intrusion reports, best practices, and tools should all be shared. Companies need to be able to share information in ways that (and whose nature) may not be predictable in advance. Like Sherlock Holmes solving a difficult case, seemingly unconnected bits of information, when ingeniously combined, produce clues and evidence that can help to detect, prevent, and mitigate network attacks. If companies are not sure what information can and should be shared, they risk losing the potential for identifying large-scale, cross-cutting attacks—essentially putting an adversary at a great advantage. On the other hand, sharing critical infrastructure information raises interest-balancing challenges because the information can carry with it additional risks[9] to public and private interests. Information sharing could be construed as price fixing, unreasonable restraint of trade, or systematic exclusion of or discrimination against certain customers. It also could raise privacy concerns, expose proprietary corporate secrets, and reveal weaknesses and vulnerabilities that erode public confidence and invite hackers. Erosion of public confidence could be particularly damaging to a publicly traded corporation, so information sharing could constitute a breach of fiduciary duty in some cases. For example, Craig Silliman noted that releasing a top ten vulnerabilities list to the public could provide hackers with the information they need to successfully attack at-risk networks.[10] However, vendors need to be

[8]For example, a Partnership for Critical Infrastructure Security (PCIS) working group proposed (in a white paper dated September 5, 2001) that information that fits into the following categories should be shared: publicized system failures or successful attacks; threats to critical infrastructures; system degradations; vulnerability information; obvious interdependencies [and] incidents of perceived limited impact; other useful information, including remediation methodology, risk management methodology, and research and development goals and needs.

[9]For a discussion of the inherent tension between the benefits and risks of disclosing information on critical infrastructure vulnerabilities, see Computer Science and Telecommunications Board, National Research Council. 1990. *Computers at Risk: Safe Computing in the Information Age*. National Academy Press, Washington, D.C., pp.20-21.

[10]The SANS Institute and the FBI maintain a prioritized list of the top 20 security vulnerabilities. The list is intended to help systems administrators focus on correcting the flaws that are most often targeted in computer network attacks. See <http://www.sans.org/top20/> for more information.

informed of vulnerabilities to create patches. Private companies also rely on the alerts to implement timely preventative measures. Some people argue that companies are slow to fix vulnerabilities without the threat of publicity. A lag time between private notifications sent to vendors and the public announcements is one approach that would give vendors and private sector entities sufficient time to implement preventative measures without facilitating hacker attacks. This example also highlights the importance of analyzing both benefits and risks in determining *when* to release sensitive information.

Since many of the ISACs were established only in the last couple of years, they are still troubled by the difficult question, *With whom* should information be shared? Each ISAC needs to create a process that outlines how decisions are made regarding the sharing of information collected by the ISAC. Most ISACs are funded through membership fees. Should the information collected by an ISAC be shared only with paid members? When should information be shared with other companies in the same industry sector (e.g., smaller businesses who may not have the resources to become a full ISAC member)? Most of the current members of ISACs are large, multinational corporations. What should the ISACs do to encourage small and medium-size businesses to participate in information-sharing activities? Who should fund these efforts? If ISACs choose to share information with the government, they must decide which agencies should receive the information (e.g., DHS and agencies that have regulatory authority over that industry). Should all information be shared with the government, and if so, should it be anonymized first? What measures do the ISACs need to put in place to encourage the government to provide (possibly classified) information on suspected pending attacks? Information-sharing models must also consider the public interest. Does the general public have a right to information about the infrastructure(s) on which it depends? Is it sufficient for the government to hold that information as the public's representative? One reason why debates over the scope and barriers to information sharing seem to elude resolution is that the fundamental issues outlined above remain to be worked through.

Selecting the appropriate information-sharing model requires ascertaining the costs and benefits. ISACs can add value by providing an analysis of the information gathered from their members. For example, ISACs can use aggregated time series data to identify attack patterns. ISACs also can use the data to develop guidelines for security best practices. In spite of the benefits of doing so, companies are reluctant to share information. They are concerned that shared information may be disclosed, causing irreparable harm—financial harm, public relations damage, competitive damage, litigation liability, or possible government intervention/investigation. Underlying the reluctance is a lack of trust.

Lack of trust has been an issue in both the public and private sectors (e.g., historically, the government has been reluctant to share with industry information that is classified). Companies often do not trust each other (or the government) with sensitive corporate information.[11] Anonymizing information is one way to alleviate concerns and build trust both between the government and industry and within industry. Issues such as these are crystallized in debates over the implications for information sharing of antitrust and freedom of information laws, which are covered in "(Perceived) Barriers to Information Sharing," below.

While most attention has been focused on sharing information with other members of a given ISAC, information shared across ISACs has the potential to be of much more value in identifying threats to the critical infrastructures of the United States and in analyzing trends. The PCIS has organized joint public-private meetings and developed white papers to highlight cross-sector information-sharing issues.[12] Identification of the key common elements in sharing might be a first step toward the development of a cross-industry sharing mechanism, since differences in jargon and culture across industries will compound the information sharing challenges that already exist.

With all of this uncertainty, it is not surprising that information sharing is evolving only slowly. Progress may also be constrained by the vehicles launched to achieve it: Both the ISACs and PCIS are limited by their membership, which includes private sector representatives who registered an early interest in critical infrastructure protection and early willingness to engage with the government on CIP issues. The ISACs and PCIS both include primarily large firms with much at stake—either from critical infrastructure risks or from the direction that CIP policy might take. The symposium's broad range of participants underscored that making progress on information sharing calls for addressing multiple issues affecting the public and private interests.

[11]The weak security of the government's own computer systems is often cited as a deterrent to information sharing. Many companies in the private sector fear that sensitive corporate information shared with the government may be compromised by hackers able to break into the government's computer systems.

[12]A PCIS working group has proposed the creation of an ISAC policy management board, to be staffed with representatives from each ISAC that will "facilitate the coordination and dissemination of the standardized information sharing documentation" (Information Sharing White Paper, September 5, 2001).

(PERCEIVED) BARRIERS TO INFORMATION SHARING

Phil Reitinger laments, "I wish that government and industry were as good at sharing information as hackers are." Corporations point to a number of legal concerns that hinder full participation in information-sharing activities. Corporations fear they could be liable if they provide flawed information to the ISAC. What happens if the information is valid but the ISAC prepares a flawed analysis that causes harm to members? What happens if a member of the ISAC fails to protect anonymous or proprietary data? What if a member fails to share or disclose information that could have prevented or minimized an attack? What happens if one member fails to implement adequate security measures and by that failure causes harm to another member of the ISAC? These difficult questions have raised awareness about the importance of ISAC membership agreements and the need to allocate risk among the ISAC, its members, and the service provider. While these issues are being examined in the context of ISAC formation and operation, two other legal concerns are perceived as impediments to successful information sharing between the private sector and the government and within the private sector: (1) the Freedom of Information Act (FOIA) and (2) antitrust laws.

Fear of FOIA and antitrust concerns are the two main factors often invoked as the reasons for lack of progress on information sharing. Corporations fear that information shared with the government may be released to third parties under a Freedom of Information Act request. Most FOIA concerns are based on an unwillingness to trust the government with information provided to it. Antitrust concerns stem from the potential for collaborative exchanges of information among competitors on pricing or production levels or customer allocation, joint endorsement of particular suppliers/vendors, or singling out or otherwise damaging a particular competitor. Public interest advocates, however, are skeptical that these barriers really stand in the way of information sharing. They believe that the current FOIA and antitrust laws are adequate to protect industry and the general public and that they encourage information sharing. This section outlines both sides of the FOIA and antitrust debates. Since drafting of this report began, a provision of the Homeland Security Act of 2002 (HSA)[13] protects some critical information infrastructure data from disclosure under FOIA. It is too soon to know what this will mean in practice, but it makes some of the discussion moot. Nevertheless, the fundamental issues remain, and there is always the possibility of new legislation.[14]

---

[13]PL 107-296.

[14]On March 12, 2003, the Restoration of Freedom of Information Act of 2003 (S. 609) was introduced in the Senate. Supporters of the bill argue that "FOIA provisions passed last year as part of the Homeland Security Act are too broad and could undermine public access

Freedom of Information Act[15]

What Is the Freedom of Information Act?[16]

Congress enacted the FOIA (5 U.S.C. 552) in 1966. FOIA is an information disclosure mechanism whose basic purpose is to ensure that certain records in the possession of the U.S. government are accessible to the people.[17] The Supreme Court has said that the motivation behind FOIA is "to ensure an informed citizenry vital to the functioning of a democratic society, and to hold the governors accountable to the governed."[18] In accomplishing that end, as the Court has also said, "[d]isclosure, not secrecy, is the dominant objective."[19]

FOIA requires all agencies of the U.S. government to disclose information upon receiving a written request, except for information protected from disclosure by nine statutory exemptions.[20] Of the nine specific statutory exemptions that are contained in the act, it has been argued that exemption 4 might be available to protect information on critical infrastructure protection disclosed to the government by a private party. For information to come within the scope of exemption 4, it must be shown that the information is (A) a trade secret or (B) information that is (1) commercial or financial, (2) obtained from a person, and (3) privileged or confidential.[21] The latter category of information (commercial information that is privileged or confidential) is directly relevant to the issue of cybersecurity information. Opponents to creating an additional FOIA exemption for cybersecurity information argue that exemption 4 should be sufficient because most information submitted by the private sector to

---

to information about the government and public safety" (Dan Verton, 2003, "Progress on Info Sharing Threatened by Changes to FOIA Law," *Computerworld.* March 19).

[15]The focus in this report is information voluntarily provided by the private sector to the federal government.

[16]This section is largely adapted from a presentation by David Sobel at the symposium.

[17]See <http://www.usdoj.gov/04foia/referenceguidemay99.htm#intro>.

[18]*NLRB* v. *Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978).

[19]*Department of the Air Force* v. *Rose*, 425 U.S. 352 (1976).

[20]The nine statutory exemptions are classified documents; internal agency rules and practices; information that is prohibited from disclosure by another law; trade secrets and other confidential business information; interagency or intra-agency communications that are protected by legal privileges; information involving matters of personal privacy; certain information compiled for law enforcement purposes; information relating to the supervision of financial institutions; and geological information on wells. See <http://www.pueblo.gsa.gov/cic_text/fed_prog/foia/foia.pdf>.

[21]Exemption 4 is described in the Department of Justice's Freedom of Information Act Guide, May 2002, available online at <http://www.usdoj.gov/oip/exemption4.htm>.

a government agency is assumed to be commercial information, broadly defined. Cybersecurity-related information may be commercial in nature, but is it always "privileged or confidential"? According to the D.C. Circuit Court decision in the *National Parks* case, commercial or financial information is deemed to be confidential if disclosure would (1) impair the government's ability to obtain the necessary information in the future or (2) cause substantial harm to the competitive position of the person from whom the information was obtained.[22]

The Argument for Expanding FOIA Exemptions

Given that the purpose of FOIA is to ensure that records in the possession of the government are accessible to the public, private sector companies have expressed concern that critical infrastructure information shared with the government might be released to third parties via an FOIA request. Attempts to prevent disclosure by private entities could result in disclosure—for instance, an FOIA request for information on all entities with a certain type of vulnerability—and could not be responded to with a reverse FOIA suit without the plaintiff implicitly identifying itself as having the vulnerability. A recent letter from the National Security Telecommunications Advisory Committee (NSTAC) to the President said, "to properly protect our critical national infrastructure and respond to attacks in a timely manner, private sector entities must be able to freely exchange critical infrastructure protection information with each other and the government. Real or perceived barriers to sharing the information must be removed."[23] Some companies, such as those represented on NSTAC, argue that it is not clear that the existing exemptions (exemption 4 in particular) would provide the certainty of protection needed before they would release sensitive information to the government. Even if the information is protected, companies argue that it requires costly legal action to block the intended disclosure of the information—this represents money, time, and resources spent (see below for actions available to requesters of information). They do not have confidence that information shared with the government—including sensitive or proprietary information and vulnerabilities—will be kept secure. Finally, because past court rulings and interpretations can be reversed and do not stay constant over time, companies tend not to trust case law even though it may seem to protect the information today. In addition, companies fear that future

[22]*National Parks and Conservation Association* v. *Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974).
[23]Copy of letter shown by David Sobel at the symposium.

rulings and interpretations could result in the release of previously submitted information.

The President's Commission on Critical Infrastructure Protection, realizing that companies might not be willing to participate in information sharing activities without special protection, called for a new statutory exemption from the FOIA for critical infrastructure information.[24] Congress has considered two bills to respond to the concerns of the private sector. Senator Bennett introduced S. 1456,[25] the Critical Infrastructure Information Security Act of 2001. One of the goals of the bill is to "encourage the secure disclosure and protected exchange of critical infrastructure information." Section 5 of that bill states that critical infrastructure information shall not be made available under section 552 of title 5, U.S. Code (FOIA). Representatives Davis and Moran introduced the Cyber Security Information Act of 2001 (H.R. 2435) to "encourage the secure disclosure and protected exchange of information about cybersecurity problems, solutions, test practices and test results, and related matters in connection with critical infrastructure protection." Section 4 states that cybersecurity information shall be exempt from disclosure under section 552(a) of title 5, United States Code (FOIA), by any federal entity, agency, and authority. The legislation creating a new Department of Homeland Security exempts "critical infrastructure information voluntarily submitted to a covered Federal agency for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose"[26] from disclosure under FOIA.

The Argument Against Expanding FOIA[27]

Opponents suggest that case law shows that the existing FOIA exemptions are sufficient to protect critical infrastructure information; they say efforts to amend FOIA (e.g., through a new cybersecurity exemption) are based largely on a misperception of the current law. Many would argue that ensuring the government is able to obtain critical infrastructure information from the private sector on a voluntary basis comes within

---

[24]President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations*. Washington, D.C., p. 32.

[25]Both bills are pending in committee. The latest major action on the Senate bill was October 9, 2001, and July 10, 2001, for the House bill.

[26]CRS Summary of Homeland Security Act of 2002, available at <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05005:@@@D&summ2=m&>.

[27]This section largely adapted from a presentation by David Sobel at the symposium.

the purview of exemption 4. The courts have found that where information is voluntarily submitted to a government agency, it is exempt from the disclosure if the submitter can show that it does not customarily release the information to the public.[28] David Sobel, general counsel of the Electronic Privacy Information Center, argues that the case law indicates that courts tend to defer to the wishes of the private sector submitter of the information and will protect the confidentiality of information that the submitter does not itself make public.

Even before the new Homeland Security Act of 2002, the legal protections available to the private sector submitter did not end with the above case law. Because of general industry concerns about disclosure of information submitted to government agencies, President Reagan in 1987 issued Executive Order 12600 (Pre-disclosure Notification Procedures for Confidential Commercial Information). This EO requires all federal agencies to implement regulations that provide procedures for the notification to the submitter of private sector information if a FOIA request is received for that information. Once that procedure is triggered, if a request is received for the information and the agency decides that there is no legal basis for withholding it, the agency is required to provide an opportunity for the submitter to offer objections to the proposed release. EO 12600 is yet another layer of protection (and at least a delay) that is available to private sector submitters under existing law. In addition, the Supreme Court has recognized that the private sector submitter has standing to file what is called a "reverse FOIA" lawsuit to block the intended disclosure of the information.[29] Finally, the U.S. Attorney General issued a new FOIA guidance memorandum[30] on October 12, 2001, that establishes a new standard that the Justice Department will apply when determining whether or not to defend agency decisions to withhold requests for information. That standard states that when there is a "sound legal basis" (in contrast to "foreseeable harm," as stated in the earlier standard) for with-

---

[28]*Critical Mass Energy Project* v. *Nuclear Regulatory Commission*, 975 F.2d 871 (D.C. Cir. 1992) (en banc), cert. Denied, 113 S.Ct. 1579 (1993). In this case, Critical Mass had requested information from the Nuclear Regulatory Commission concerning the results of inspection reports dealing with nuclear plant safety compliance. This information, revealing potential vulnerabilities at a nuclear power plant, is similar to the types of information involved in critical infrastructure protection. The court in this case concluded that because the nuclear power companies would not voluntarily release to the public this information, which they considered confidential, it was not subject to disclosure. This was an en banc decision of the full D.C. Circuit and further appellate review was denied by the Supreme Court, which is significant because the D.C. Circuit is where 95 percent of the FOIA litigation takes place, and this is the circuit court that is deferred to by all of the other circuits.

[29]*GTE Sylvania, Inc.* v. *Consumers Union*, 445 U.S. 375 (1980).

[30]The FOIA Post is available online at <http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>.

holding the information, the Justice Department will defend that agency determination in court.

The American Civil Liberties Union (ACLU) sent a letter to Senators Lieberman and Thompson urging them to oppose Senator Bennett's bill to amend the FOIA.[31] The ACLU argues that when the courts have debated the public's need for disclosure against the harms of disclosure under FOIA, they have shown deference to industry concerns for confidentiality. They suggest further that an all-encompassing CIP exemption would undermine security, rather than enhance it, because it would allow companies to shield from the public the actions they are not taking to protect their infrastructures from attack.

According to Mr. Sobel, no one has identified what type of critical infrastructure information would escape the protection afforded by FOIA's Exemption 4. He asserts that the current FOIA law is sufficient both to enable CIP-related information sharing between the private and public sectors and to protect collected information.

Can the Government Protect CIP Information?

Glenn Schlarman, from the Office of Management and Budget, argues that the Bennett bill and the Davis-Moran bill were not addressing (at least on the FOIA exemption side) the reality of the issue that information can be protected once it is in the government's possession. These bills—and presumably the Homeland Security Act of 2002—address the perception that the government will not protect it or cannot protect it. He argues that the *Critical Mass* case is the "law of the land," which means that voluntarily provided, customarily protected industry information is exempt under FOIA. The problem, according to Mr. Schlarman, is that government personnel who respond to FOIA requests do not read the Department of Justice Office of Information and Privacy case law on FOIA to know what is exempt today. Although the (pre-HSA) law has been sufficient to protect CIP-related information, he suggests it is not clear that agencies know how to protect it. A key issue is whether government agencies have processes in place to protect the information from inappropriate or accidental disclosure.[32] Hence, Mr. Sobel suggests that a better

[31]See <http://www.aclu.org/congress/l040302b.html>. The ACLU sent a similar letter to Representatives Burton and Waxman urging them to oppose H.R. 2435; see <http://www.aclu.org/congress/l040302c.html>.

[32]For example, corporations fear that their sensitive proprietary information shared with the government might be leaked or misused by a government employee who migrates to a job with the corporation's competitor.

approach is to educate the employees in federal agencies who respond to the FOIA requests about the types of information that cannot be released under existing law.

Antitrust

Many companies fear that sharing CIP-related data with competitors could be viewed as a violation of the antitrust provisions of the Sherman Antitrust Act (15 U.S.C.).

Understanding Antitrust[33]

The goal of antitrust law is to promote competition in the marketplace. Therefore, to prohibit restraint of trade, the antitrust law seeks to discourage collusion—inappropriate collective action—and inappropriate exclusion.[34] Collusion occurs when rival firms act jointly to raise prices and reduce output, thereby harming consumers and the economy as a whole. Exclusion occurs when competitive constraints normally offered by rivals are removed, thus making it possible for a firm to exercise market power.

While information sharing among competitors in its own right is not illegal, it can be unlawful if it contributes to anticompetitive conduct either through an actual agreement (e.g., on price) or to the facilitation of coordinated behavior. For example, a joint venture of competitors could establish a standard for computer security that excluded one provider.[35] The "Antitrust Guidelines for Collaborations Among Competitors," issued in 2000 by the Federal Trade Commission and the Department of Justice, stressed that the sharing of information among competitors may be procompetitive and may be reasonably necessary to achieve a procompetitive benefit. If the information is reasonably necessary for achieving procompetitive efficiencies, those efficiencies are taken into account in assessing the overall effect on competition.

If the information to be shared could be competitively sensitive—typically that means information on price, costs, future business initiatives, and the like—then certain factors can serve as guideposts in trying to determine whether information sharing is likely to facilitate collusion.

---

[33]This section, "Understanding Antitrust," is excerpted from a presentation by William E. Cohen at the symposium.

[34]Some forms of exclusion are acceptable under the law, such as protection of intellectual property rights to prevent their use by others, or not permitting access to valuable assets, which is permitted in all but a few circumstances.

[35]See *Addamax* v. *Open Software Foundation, Inc.*, 152 F.3d 48 (1st Cir. 1998).

Who is receiving the information? If only one side of the partnership is using the information, then collusion concerns might have merit. How old is the information? Sharing contingent or future information is generally more troubling than sharing historical information, since it could be used to help in achieving agreement among competitors or in coordinating their conduct. How specific is the information? Information that identifies the conduct of individual firms is likely to raise greater concern than information that is aggregated. For example, information reviewing a particular firm's pricing conduct may identify individual disclaimers and discourage them from cutting a collusive price. Finally, how accessible is the information? Sharing unique information is more likely to raise concerns than sharing information that is already publicly available.

For example, standards setting—which can be relevant to critical infrastructure protection—illustrates that not all collective action is considered bad from an antitrust perspective. Setting standards is, by its nature, inherently a collective activity carried out industry-wide, but how it is done determines whether it serves to facilitate price setting or other anticompetitive behavior, which may be aimed against the buying public or a competitor.

The Argument That an Antitrust Exemption Is Needed

Many in the private sector are concerned that sharing CIP-related information may expose participating companies to antitrust enforcement actions. In addition, many are concerned that determination of the safe harbors for CIP-related information sharing is a complex, expensive, and risky process that will discourage smaller firms from CIP-related information sharing. Further, although formal advice from the government can be obtained in the form of a "business review letter" (see next section), that mechanism has its limitations[36] and does not provide absolute immunity from government enforcement actions or private litigation. Concerns of this nature have led Congress occasionally to pass limited antitrust exemptions to combat perceived antitrust risk. One example is

[36]First, over time, a business review letter can become outdated and may no longer be relied on. Second, the letter is only as good as the facts presented. If a firm departs from the stated facts, it would be required to get a supplemental letter or risk losing protection. Finally, while the letter may provide substantial protection with regard to federal enforcement agencies, there is always the possibility of private litigation. A business review letter is not binding on any private litigants. A clear statement from the federal government that it does not view a particular set of facts as being in violation of antitrust laws will strengthen the case of a firm in antitrust litigation. However, even if a firm wins in litigation, it still has to bear the transaction costs of the lawsuit.

the National Cooperative Research Act of 1984,[37] amended and renamed the National Cooperative Research and Production Act of 1993.

The President's Commission on Critical Infrastructure Protection suggested that firms should be offered limited assurances and guidelines to protect them from antitrust enforcement actions.[38] The congressional bills mentioned earlier (H.R. 2435 and S. 1456) include language that would exempt companies that share information about computer viruses and other network vulnerabilities from antitrust prosecution.

The Argument That Antitrust Offers Sufficient Protection

Opponents to creating a new antitrust exemption argue that a new exemption is not needed to protect firms sharing critical infrastructure protection information from allegations of anticompetitive behavior.[39] They further argue that experience with antitrust exemptions in other contexts reveals practical problems with exemptions that may cause more harm than good. For example, if a blanket exemption were granted, people working to protect critical infrastructures could (try to) agree to raise prices 20 percent. They could also (try to) agree to share relevant technology only with each other and not with anyone offering a competing product. Although most industry officials would agree that such conduct is not protected by a new exemption, it is important to recognize the possibility of such consequences. Past efforts to develop exemptions from antitrust (e.g., research cooperation) indicate that conduct can be exempt so long as it does not involve price fixing or boycott activities. The American Bar Association's Antitrust Section has voiced its opposition to further narrowing of exemptions.[40]

Some decrease in uncertainty can be obtained via a business review letter. This procedure allows firms to get formal advice from the Department of Justice (DOJ) on whether proposed future conduct would be viewed as anticompetitive. Under this procedure, DOJ indicates whether, on the basis of the facts presented in the request, it currently has any

---

[37]15 U.S.C. §§ 4301-05.

[38]President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations.* Washington, D.C., p. 32.

[39]For examples of authority addressing the antitrust treatment of the type of information exchange or standard setting discussed in the text, see *Antitrust Law Developments* (5th ed.) 114.

[40]See, for example, <http://www.abanet.org/antitrust/tele97.html>, which notes that "the American Bar Association Section of Antitrust Law disfavors antitrust exemptions directed to narrow industry categories." See also <http://www.abanet.org/antitrust/coalitionact.html>; <http://www.abanet.org/antitrust/agmerger.html>; <http://www.abanet.org/antitrust/basebl97.html>; and <http://www.abanet.org/antitrust/hcact97.html>.

BOX 2.2
EPRI Business Review Letter

In October 2000, the Electric Power Research Institute, Inc. (EPRI) received a business review letter from the Department of Justice regarding a proposed information exchange program designed to reduce computer-based security risks posed by the increasing interconnection, interdependence, and computerization of their systems. EPRI indicated that the energy companies planned to exchange two principal types of information: best practices (including methodologies for conducting vulnerability assessments, stress tests, and plans to identify, alert, and prevent cybersecurity breaches) and product vulnerability information.

The business review letter announced that the DOJ had no intention to challenge the information-sharing arrangements proposed by EPRI. DOJ found that anticompetitive harm was unlikely, provided that the information was confined to physical and cybersecurity issues and did not provide company-specific information related to pricing or any agreements on purchasing decisions or any recommendations in favor of or against the products of particular vendors. The letter adds, "To the extent that the information exchanges result in more efficient means of reducing cybersecurity costs, and thus savings redound to the benefit of consumers, the information exchanges could be procompetitive in effect."[1]

[1]The U.S. DOJ business review letter to EPRI is available online at <http://www.usdoj.gov/atr/public/busreview/6614.htm>.

intention of bringing an enforcement action. DOJ has issued several business review letters[41] (see Box 2.2) relevant to critical infrastructure protection activities, indicating that the proposed information sharing arrangements would not be viewed as a violation of antitrust laws. For example, two business review letters announced that the government had no intention to challenge efforts to develop solutions to Y2K problems, including the sharing of test results and information on proposed solutions. Several DOJ business review letters noted the potential procompetitive benefits of information sharing that created databases to help industry members avoid fraud or high credit risks.

CONCLUDING OBSERVATIONS

Symposium participants noted that trust (with respect to how the information will be used, how it will not be used, how it will be protected

[41]A list of the business review letters issued by the Department of Justice is available online at <http://www.usdoj.gov/atr/public/busreview/letters.htm>.

from disclosure, and whether legal tools can be used by the government and private parties against those sharing information) among those sharing information is the most important prerequisite for achieving successful protection of the nation's critical information infrastructure. The development of trust is necessary to achieve an atmosphere of openness and cooperation that can lead to sharing of vulnerabilities, best practices, and other critical information. While the passage of legislation will not automatically create trust, many believe it would create an environment where trust could develop.

Mr. Sobel argues that passing legislation to remove a perceived (as opposed to a real) barrier is a bad way to make policy, and the Antitrust Section of the American Bar Association's steady opposition to antitrust exemptions, for example, corroborates that point of view. Legislation carries risks and costs as well as benefits, and the changes over the past year underscore the importance of considering the total effect, as well as the implications of any one piece of legislation.

No major reform to the Freedom of Information Act is explicitly required to allow for CIP-related information sharing between the private sector and the public sector. However, there is some risk and a perception that proprietary CIP-related information shared between private sector firms and federal government entities may be disclosed to third parties under FOIA. The new HSA provision reduces any such risk. There needs to be greater education and awareness on FOIA in the federal agencies when staff are responding to FOIA requests and in the private sector where this information is held. To lower apprehension in the private sector, the government should examine its processes and monitor them to ensure they will protect private information and should make sure its employees are appropriately trained.

Like FOIA, the existing antitrust law does not prevent the private sector from sharing information on cyberthreats within and between sectors. However, also as with FOIA, there are persistent perception problems and the need for better education and awareness about the law.

3

Liability for Unsecured Systems and Networks

The existing legal framework for critical infrastructure protection consists of a patchwork of state and federal laws that are generally aimed at deterring certain types of conduct on computer networks. In addition, there are laws aimed at deterring certain types of conduct, including protection of electronic information pertaining to individual consumers and patients, for specific sectors, such as the Gramm-Leach-Bliley (GLB) Act[1] for the financial services sector and the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[2] for the health services sector. There are no comparable regulations, however, that require entities to conform to any specific practices designed to promote critical infrastructure protection. Symposium participants differed on whether it would be more effective to target hackers and other perpetrators (for the intentional harm caused) or vendors/service providers (for harm caused through negligence). This chapter explores the legal theories supporting Internet-related liability.

CRIMINAL LAW

The purpose of criminal law is generally to deter future crime and punish perpetrators. Criminal threats to critical information infrastruc-

[1]15 USC, Subchapter I, Sec. 6801-6809. PL 106-102.
[2]PL 104-191.

tures include unauthorized access to computer networks (either from an insider or an outside hacker), malicious code (such as viruses and worms), and distributed denial-of-service attacks. The conventional wisdom is that prosecution of computer crimes will help reduce the number of future computer attacks. This approach depends on the private sector entities—the owners of the information infrastructures—to report criminal computer activities. However, to use prosecution as a deterrent, the attack and subsequent prosecution must be publicized. This may be acceptable when criminals are caught in the process of attempting an attack (which is therefore rendered unsuccessful) but may not be desirable when the attack succeeds. Craig Silliman suggests that a victim's decision to report a computer attack to law enforcement depends on a careful balancing of interests. For example, an ISP differentiates itself based on the quality and service of its networks; a single advertised attack could lead to a loss of customers and revenue. In addition, information in the public domain about the vulnerability of a network could lead to copycat attacks. Hence, it would take a large number of prosecutions, Mr. Silliman argues, to compensate an ISP for the corresponding bad publicity. These concerns—echoed by companies in many industries (e.g., financial institutions)—have contributed to private information-sharing efforts (such as ISACs and CERT) to reduce attacks and to detect and prevent the successful conclusion of an attack.

Domestic Jurisdiction

Congress has passed a number of laws related to computer crime.[3] These laws are generally focused on hackers and other individuals who use computer networks for illegal purposes.[4] This section provides a brief overview of the key computer crime laws.[5]

---

[3]Many states also have computer crime laws that may affect critical information infrastructure protection.

[4]Many of the attacks that occur today are the result of malicious or indifferent acts by individuals (often referred to as "script kiddies"). They generally do not have the sophistication to develop their own attacks, but rely on programs ("scripts") written by others and/or other ready-made tools to launch network attacks. An in-depth analysis might be helpful to consider a variety of issues surrounding these hacker kits such as whether such kits are protected under the First Amendment rights (e.g., bomb-making is protected, so arguably hacker kits should be as well); whether these kits are circumvention tools; when it is appropriate to use these kits (e.g., security firms that use them to conduct audits for insurance purposes).

[5]There are many laws that pertain to conduct on computer networks that are not designed solely for online environments (e.g., the Espionage Act, 18 U.S.C. Sec. 793, 794, and 798; Wire Fraud, 18 U.S.C. Sec. 1343; and the Economic Espionage Act, 18 U.S.C. Sec. 1831 et al.). The laws cited in this section are all part of Title 18, "Crimes and Criminal Procedures."

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) of 1986 (18 U.S.C. § 1030) was the first federal law specifically directed at computer crime. It was initially aimed at protecting "federal interest" computers as well as computers used by financial institutions but now protects any computer used in interstate commerce. The CFAA imposes penalties on individuals who knowingly and with intent to defraud gain unauthorized access to computers. For example, in *United States* v. *Morris*[6] (an early case demonstrating some of the challenges associated with criminal computer prosecutions), the court found Morris liable for damages caused by his actions because he *knowingly* accessed a computer even if he did not *intentionally* cause harm.[7] Although the CFAA does not include provisions for critical information infrastructure protection per se, it has played a major role in prohibiting and sanctioning cyberattacks.[8] Congress has continued to amend the CFAA over the last several years to increase its effectiveness as the threat and technology have evolved.[9]

Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 (ECPA; 18 U.S.C. § 2701) updated the legal framework for electronic surveillance of oral and wire communications established in Title III (the Omnibus Crime Control and Safe Streets Act of 1968) to include electronic communications.[10] ECPA provides criminal and civil penalties for accessing and obtaining or altering without permission stored electronic communica-

---

[6]*U.S.* v. *Morris*, 928 F.2d 504 (2d Cir. 1991).

[7]Sarah Faulkner. 2000. "Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks," *Journal of Computer & Information Law*, Vol. 18: 1019-1047.

[8]For example, in *U.S.* v. *David L. Smith* (D. N.J. May 1, 2001), Mr. Smith was convicted under 18 U.S.C. 1030(a)(5) for launching the Melissa virus (see <http://www.usdoj.gov/criminal/cybercrime/melissaSent.htm>) and in *U.S.* v. *Bret McDanel* (C.D. Cal June 25, 2002), Mr. McDanel was convicted under CFAA for maliciously bombarding a company computer system with thousands of e-mail messages (see <http://www.usdoj.gov/criminal/cybercrime/mcdanelConvict.htm >).

[9]The U.S. House of Representatives recently approved H.R. 3482, the Cyber Security Enhancement Act, which raises the penalty for computer crime to a maximum of life imprisonment. The bill was received in the Senate and read twice and then referred to the Committee on the Judiciary on July 16, 2002. For more information, see <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03482:@@@D&summ2=m&>.

[10]For more information on electronic surveillance, see Computer Science and Telecommunications Board, National Research Council. 1996. *Cryptography's Role in Securing the Information Society*. National Academy Press, Washington, D.C., Appendix D. Available online at <http://www.cstb.org/pub_crisis>.

tions. It also governs what an applicant must do to be granted access to evidence of computer crime possessed by ISPs. The unlawful access to stored communications provision, like the CFAA, protects the critical information infrastructure by enabling the prosecution of individuals who attempt to halt the flow of information to or from electronic storage systems.

Fraud and Related Activity in Connection with Access Devices

Section 1029[11] in Title 18 of the U.S. Code is the "federal statute condemning various crimes involving . . . access devices."[12] The law defines an access device as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or . . . other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value. . . ."[13] Section 1029 provides for penalties ranging from fines to—in some cases—imprisonment for up to 20 years.

Wire and Electronic Communications Interception and Interception of Oral Communications

Section 2511 in Title 18 of the U.S. Code "provides specific criminal and civil penalties for individuals (law enforcement officials and private citizens alike) who conduct electronic or wire surveillance of communications . . . in a manner that is not legally authorized. Legal authorization for such surveillance is provided for specific circumstances in law enforcement and foreign intelligence collection. . . ."[14] Section 2511 includes what is referred to as the one-party consent provision, which allows federal law enforcement officials to monitor telephone conversations without obtaining a court order provided they obtain the consent to do so from one of the parties engaged in the conversations.

---

[11]The Access Device Law was primarily developed for low-tech prosecutions, such as credit card fraud, but has since been adopted for use in more complex cases involving computers.

[12]Charles Doyle. 2002. *The USA PATRIOT Act: A Legal Analysis* (RL31377). Washington, D.C.: Congressional Research Service. Available online at <http://www.fas.org/irp/crs/RL31377.pdf>.

[13]The text of 18 U.S.C. 1029 can be found online at <http://www.usdoj.gov/criminal/cybercrime/usc1029.htm>.

[14]Computer Science and Telecommunications Board, National Research Council. 1996. *Cryptography's Role in Securing the Information Society*. National Academy Press, Washington, D.C., p. 396. Available online at <http://books.nap.edu/html/crisis/>.

USA PATRIOT Act

The USA PATRIOT Act of 2001,[15] designed as a collection of amendments to existing laws, includes a number of provisions related to critical infrastructure protection: revisions to CFAA (increased penalties for hackers who damage protected computers; a new offense for damaging computers used for national security; and an expansion of the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce); increased information sharing; strengthened criminal laws against terrorism; and enhancements to the government's legal authorities to conduct electronic surveillance.

International Jurisdiction

The nature of modern communications, including the Internet, makes international cooperation in cybersecurity of increasing importance. The perpetrators of many recent cybercrimes (such as the "I Love You" virus and the distributed denial-of-service attacks in February 2000) were hackers in foreign countries. The recent case of *U.S.* v. *Gorshkov*,[16] in which an FBI agent conducted a cross-border search of a Russian computer to obtain evidence to indict a Russian citizen on extortion charges, is an example of how courts look at cross-border searches in the current environment and how it might become the norm in the absence of formal international coordination.

Increasing cross-border criminal activity highlights the need for common international standards and objectives for cybersecurity. Different countries have different laws and practices, making prosecution of these criminals very difficult.[17] In August 2000, Sofaer and Goodman (Center

---

[15]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, PL 107-56.

[16]*U.S.* v. *Gorshkov*, 2001 WL 1024026 (W.D.Wash.). After a series of computer hacker intrusions into U.S. businesses, the FBI identified a Russian as one of the intruders. The FBI lured him to the United States on the pretext of a job interview, during which the defendant was asked to prove his computer hacking and security skills. The defendant logged into his home computer network to access computer hacker tools. The FBI were able to obtain the defendant's userid and password to his home computer by using a tool to capture all keystrokes on the computer provided during the interview. The userid and password allowed the FBI to download the information contained on the defendant's home computer, which confirmed that the defendant was involved in the computer hacker intrusions. At issue is whether the FBI violated the defendant's fourth amendment rights by breaking into his space. The court found that the defendant should not have had an expectation of privacy during the interview; hence he intended to disclose the userid and password.

[17]One notable exception is the arrest and prosecution of Ehud Tenebaum, an Israeli citizen, for his part in the Solar Sunrise cyberattacks. For more information on Solar Sunrise, see <http://www.sans.org/newlook/resources/IDFAQ/solar_sunrise.htm>.

for International Security and Cooperation, Stanford University) proposed a multilateral convention on cybercrime and terrorism that would encourage international cooperation.[18] The Council of Europe developed the Convention on Cybercrime (with the United States participating as an observer), which was signed (as of December 2001) by 26 members of the European Union as well as the United States, Canada, and Japan.[19]

Jack Goldsmith, professor of law at the University of Chicago Law School, argues that remote cross-border searches and seizures are a necessary tool in fighting cybercrimes.[20] Such measures, he asserts, are not prohibited by existing norms of territorial sovereignty and furthermore are not without precedent. There remains a debate about when and how a nation can attempt to enforce its own laws to affect those outside its own territory, and for that reason enforcement is still an ambiguous concept that should be clarified as sovereign governments adjust to the realities of new technology.[21] Box 3.1 provides a general discussion of criminal liability with respect to international cybercrime.

CIVIL LIABILITY

Elliot Turrini, former assistant U.S. attorney from the District of New Jersey, argues that criminal law alone is not sufficient to deter intruders and prevent cybercrime. Civil liability, he argues, is "essential to insure proper incentives to create an optimal computer crime strategy." Although tort-based liability with regard to CIP is not well developed at present, many experts believe that a few CIP-related liability suits could

---

[18]Abraham D. Sofaer and Seymour E. Goodman. 2000. *A Proposal for an International Convention on Cyber Crime and Terrorism*. Stanford, Calif: Center for International Security and Cooperation. Their proposal calls for adoption of laws making certain cyberactivities criminal, enforcement of laws or extradition to the United States for prosecution, cooperation in investigating criminal activities, and participation in efforts to adopt and implement standards and practices to enhance security.

[19]The European Convention is somewhat controversial in the cybersecurity arena. Some experts argue that the Convention has several major flaws, including these: It does not include all the states that should be included; it is restricted to criminal law cooperation; and it does not encourage cooperation in the development of standards and practices that would make cybercommunication safer. Information on the Convention is available at <http://www.coe.int>.

[20]Jack L. Goldsmith, "The Internet and the Legitimacy of Remote Cross-Border Searches," University of Chicago Law School, October 2001.

[21]For a discussion of the relationship between global information networks and local values (political, economic, and cultural norms), see Computer Science and Telecommunications Board, National Research Council. 2001. *Global Networks and Local Values: A Comparative Look at Germany and the United States*. National Academy Press, Washington, D.C. Available online at <http://www.cstb.org/pub_globalnetworks>.

BOX 3.1
Offshore Cybercrime and Jurisdiction
by
Jack Goldsmith
Professor of Law, University of Chicago Law School

The anonymity made possible by cyberspace is one reason why attacks on critical infrastructures from hackers, cybercriminals, and cyberterrorists are hard to stop. Another reason has to do with borders. When these activities take place from abroad, they are hard to stop for a different, independent reason.

A nation's power to enforce its laws is limited by territory. The *Restatement (Third) of Foreign Relations Law* states these limits as follows: "It is universally recognized, as a corollary of state sovereignty, that officials in one state may not exercise their functions in the territory of another state without the latter's consent."[1] The *Restatement* adds that one state's law enforcement officials "can engage in criminal investigation in [another] state only with the state's consent."[2]

Even with the territorial limits of enforcement jurisdiction, nations can often do a good job of controlling Internet transmissions from abroad by regulating persons and property within the territory. They can, for example, seize the foreign content provider's local assets, penalize in-state end-users severely, regulate in-state hardware or software through which offending transactions are made, and regulate Internet access providers and local financial intermediaries that facilitate unwanted Internet transactions.[3] In these and other ways, a territorial government exercising power solely within its territory can indirectly regulate offshore content providers by raising their costs, often significantly.

Unfortunately, these forms of end-user and intermediary regulations tend not to work well with respect to the cybercrimes and cyberterrorism committed from abroad. Because these crimes are (usually) one-time, discrete events, it is hard for local Internet intermediaries to identify and screen out the pertinent cross-border data flows. Moreover, there is a special need in this context to secure evidence of the crime immediately. Pseudonymity is relatively easy to achieve in the commission of these crimes. And perhaps most importantly, evidence of the crime can be destroyed relatively quickly.

For these reasons, enforcement authorities face two distinct jurisdictional challenges with respect to cybercrimes and cyberterrorism committed from abroad. The first challenge concerns evidence. Authorities often must take immediate steps to identify the computer sources of the criminal activity and seize (or at least freeze) information on the computers relevant to the crime before all records of the crime are erased. The second challenge concerns prosecution. Authorities must secure the presence of the offshore perpetrator so they can punish him.

There are basically three ways to achieve these goals, consistent with the principle that enforcement jurisdiction is territorial.

Cooperation by Treaty

The nation subject to the attack can cooperate with the nation (or nations) from which, or through which, the attack occurs. Officials in the originating state(s) can assist officials in the target state in identifying, freezing, and retrieving evidence related to the crime and in apprehending the author of the crime and either

continued

BOX 3.1 Continued

bringing him to justice in the originating state or extraditing him to the subject state for prosecution.

This, in a nutshell, is the strategy of the Council of Europe draft Cybercrime Convention. In addition to harmonizing domestic definitions of cybercrime, the convention aims to enhance fast and effective international cooperation in the enforcement of cybercrime. It requires each nation to enact laws authorizing expedited searches, seizures, and preservations of computer data within the territory. It also provides for a system for rapid enforcement assistance. For example, the convention contemplates that nations where the crime originates will, at the request of the nation where the crime is causing damage, preserve and disclose stored computer data. It also contemplates that each treaty signatory will establish a round-the-clock point of contact to ensure immediate assistance for the purposes of cross-border information requests. Finally, the treaty contemplates extradition of criminals from the nation where the attacks originated to the nation where the attacks occurred.

There are at least four problems with this approach. First, treaties take years, and sometimes decades, to draft and ratify. The Council of Europe convention has not yet been ratified, and it will take years before major nations outside Europe ratify it (assuming they ever do). Second, any nation that does not ratify the treaty (and there will be many) can serve as a haven for cybercriminals and cyberterrorists. For the treaty to work, State parties will need to impose significant collateral sanctions on nations that fail to ratify, implement, or enforce the convention. Fourth, the convention does not authorize remote cross-border searches (i.e., unilateral searches by one nation on computers in another nation for the purpose of seizing and freezing evidence). Assuming that the convention eventually comes into force, it will be necessary for a nation pursuing a cyberterrorist to consult with local officials before seizing, storing, and freezing data on computers located in their countries. Even with the contemplated round-the-clock consultation and mutual assistance machinery, this extra and unwieldy step will give cybercriminals precious time to cover their tracks.

Informal Cooperation

Even in the absence of treaties, enforcement authorities from many nations cooperate in the fight against cybercrime by (1) swapping information and (2) cooperating in the seizure of evidence on local computers.

Informal cooperation is crucial and does not require lengthy treaty processes. But it is uncertain. In the absence of an official treaty framework, many nations do not provide adequate cooperation. Moreover, extradition of cybercriminals is difficult to do in the absence of a treaty. This is because of the principal of double criminality, which requires as a precondition to extradition that the allegations be a crime in both the rendering and receiving state. Laws against cybercrimes are underdeveloped in most nations and not harmonized across nations. A treaty regime can, over time, rectify these shortcomings (as the European treaty aims to do). But in the meantime, extradition for cybercrimes is difficult. Consider the fate of the author of the “I Love You” virus, which caused over $10 billion in damage around the world. He was not prosecuted in the Philippines because that country lacked adequate criminal laws. And because he did not violate Philippine law, the

double criminality principle precluded him from being extradited to other countries pursuant to general extradition treaties.

Cross-Border Searches and Seizures

The nation attacked can also act unilaterally. Sitting at their desks in one country, law enforcement officials can take unilateral steps on computer networks to trace the origins of the cyberattack and explore, freeze, and store relevant data located on a computer in the country where the crime originated. These actions are known as remote cross-border searches and seizures.

There are two problems with these unilateral acts. First, many believe they violate the principle of territorial sovereignty and thus violate international law. (In "The Internet and the Legitimacy of Remote Cross-Border Searches,"[4] I argue, contrary to conventional wisdom, that cross-border searches and seizures are consistent with international law.) And second, cross-border searches cannot produce the criminal defendant himself.

---

[1]Restatement (Third) of the Foreign Relations Law of the United States 432, comment b.

[2]Ibid.

[3]For an elaboration of these truncated points, see Jack L. Goldsmith, "Against Cyberanarchy," 65 *University of Chicago Law Review* 1199 (1998); Jack L. Goldsmith, "The Internet and the Abiding Significance of Territorial Sovereignty," 5 *Indiana Journal of Global Legal Studies* 475 (1998).

[4]Jack L. Goldsmith, "The Internet and the Legitimacy of Remote Cross-Border Searches," University of Chicago Law School, October 2001.

change the cost-benefit analysis of securing critical infrastructures. Civil law is intended to deter undesirable or wrongful conduct and compensate those harmed by such conduct. An important component of civil liability is that it would allow a victim to recover losses from third parties if such parties were negligent or engaged in intentional misconduct and such negligence or misconduct was the proximate cause of the loss. In the Internet environment, such third parties may be the only source of recovery,[22] since criminal law offers no compensation to the victim if the computer criminal cannot be identified or is judgment-proof (a likely scenario given the anonymity of the Internet and the lack of financial

[22]Civil lawsuits may be ineffective at recovering losses against third parties located outside the United States. As noted earlier, the European Convention on Cybercrime is limited to criminal law cooperation.

assets of many computer hackers).[23] The ability to impose civil damages on a third party, such as a communications carrier or a service provider who is proven to be negligent, could motivate that party to invest the necessary resources in improving security (e.g., by closing known software bugs to help deter hackers). Civil liability can arise from contract law, tort law, or regulation.

Contract Law

Contracts are agreements between two parties that create an obligation to do, or not do, a particular thing. If one party breaches its contractual obligations, the law provides a remedy to the aggrieved party.

Contract law is generally viewed as the only basis for bringing computer-related cases because other theories of liability are inapplicable for several reasons: (1) damages from computer crimes are almost always monetary, and courts have traditionally denied negligence claims for purely economic losses (see "Tort Law" section);[24] (2) there is no specific standard of conduct for negligence-based claims; and (3) the intervening criminal act, not the network owner's negligence, is generally viewed as the proximate cause of the harm. By contrast, liability between two entities is easily facilitated by contract. Say, for example, Company A contracts with ISP B to provide network services. If ISP B fails to uphold its contractual bargains, then company A can seek remedy in court. In this way, contracts can be a positive force in helping secure critical infrastructures.

Contract law, however, often fails to provide an adequate remedy for third parties. Suppose a hacker breaks into Company A's inadequately secured network and then uses Company A's network to launch an attack against Company B. The attack against Company B disables its networks, thereby causing Company B to fail to deliver promised services to its customers.[25] If Company B is not in privity with Company A (i.e., the two companies do not have a contractual relationship), Company B cannot seek remedy for business losses from Company A under contract law. Company B is often referred to as the "downstream" victim in this type of computer attack. This scenario is quite common in distributed denial-of-service attacks. Hence, the limitations of contract law have caused com-

---

[23]Erin E. Kenneally. 2000. "The Byte Stops Here: Duty and Liability for Negligent Internet Security," *Computer Security Journal*, 16(2).

[24]David Gripman. 1997. "The Doors Are Locked But the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem," *The John Marshall Journal of Computer and Information Law* 16(1):167.

[25]Ibid.

mentators to suggest the use of tort law as a model for computer-related cases.

Tort Law

A tort is a wrongful act other than a breach of contract for which relief may be obtained in the form of damages or an injunction. The purpose of tort law is to deter wrongful conduct and compensate those harmed. While contract law rests in large part on obligations imposed by negotiation or bargain, tort law rests seminally on obligations imposed by law (either case law or federal or state regulation).[26] For example, in the case of a distributed denial-of-service attack, there is no question that the hacker who intentionally caused harm should be held responsible in tort. The question, however, is whether tort liability should also apply to entities (companies, vendors, service providers, universities, or individuals) whose systems or products were used or accessed in the course of a computer attack and who failed to take reasonable steps prior to the attack to protect against misuse of their networks. To date, no U.S. court has addressed the issue of liability for failure to secure a computer network adequately.[27] If tort law is found to apply to computer security, then the potential for civil liability lawsuits (with the likelihood of monetary damages) could encourage companies to invest in computer security measures. It would also influence decisions about computing system development. As a consequence, the ability of tort law to motivate action on critical information infrastructure protection is one possible avenue to explore.

A key conceptual question is whether tort law should allow recovery of damages from a company whose networks were not properly secured and then were used by a third party to cause harm. Generally, to recover damages in tort, the plaintiff must show that the defendant was negligent. Negligence has four basic elements: (1) a legal duty; (2) a breach of that duty (i.e., a failure to conform one's conduct to the required standard of care, such as "reasonable care");[28] (3) causation (i.e., the damage was the

---

[26]Sarah Faulkner. 2000. "Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks," *Journal of Computer & Information Law*, 18:1019-1047.

[27]Erin E. Kenneally. 2000. "The Byte Stops Here: Duty and Liability for Negligent Internet Security," *Computer Security Journal*, 16(2).

[28]Reasonable care is often defined as "the degree of care that a reasonable person would exercise under the circumstances." David Gripman. 1997. "The Doors Are Locked but the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem," *The John Marshall Journal of Computer and Information Law* 16(1):167.

proximate cause or foreseeable consequence of the risk created by the defendant's act or omission); and (4) actual damage. Before liability will be imposed, a plaintiff must substantiate all of the necessary elements to support its claim.

Under existing law, a plaintiff would have some difficulty meeting all of the required elements in the computer security context. Although a corporation might be deemed to have an existing legal duty to protect the information of its customers or clients (especially if it is a financial institution or a custodian of medical records),[29] currently no legal duty exists between a service provider and other unrelated or "downstream" parties on the Internet. If such a duty were to be recognized, it would have to be based on (1) a public policy determination that the victim needs legal redress, (2) the foreseeability of risk of harm to the victim, (3) the defendants' ability to control or minimize the risk of harm, and (4) the determination that the defendant is the party best positioned to protect against the harm.[30]

With regard to the foreseeability of harm to third parties in the network environment, several cases demonstrate that this question is inextricably related to the question of whether the defendant knew or should have known that certain illegal or wrongful conduct was, in fact, occurring on its networks (and not just "likely" to occur). These cases—although decided in the very different contexts of copyright infringement and defamation law—also suggest that holding defendants liable, either directly or indirectly, for harm caused as a result of known and unaddressed computer security vulnerabilities would be a reasonable extension of traditional legal principles. As indicated in the cases set forth in Box 3.2, if a corporation (or service provider) knows or has reason to know that its computer networks are being used to cause harm, and it has the capacity to stop such harm from occurring, the corporation may be required to take action to avoid liability, especially if it derives a financial or other benefit from allowing its networks to be accessed by others. Clearly, however, the determination as to the "capacity to control" the unwanted network behavior will be a matter of significant dispute.

As to the fourth factor, proponents of tort liability argue that the

---

[29]It could be argued that financial institutions have an existing duty under the Gramm-Leach-Bliley implementing regulations to provide immediate and effective incident response to protect the confidentiality of consumer data maintained on their own networks. These regulations, however, would not apply to unregulated parties whose networks are being used to cause harm.

[30]Kimberly Keifer and Randy Sabett. 2002. "Openness of Internet Creates Potential for Corporate Information Security Liability," *Electronic Commerce and Law Report*, Vol. 7, No. 24, June 12, p. 10.

BOX 3.2
Liability Based on Knowledge of Misconduct on Computer Networks

***Cubby* v. *CompuServe*[1]**

In October 1991, a federal judge in New York found that CompuServe was a distributor of general online information services and was therefore not liable for defamatory messages carried on one of the 150 computer bulletin boards on the service. The court found that CompuServe had no contractual relationship with the bulletin boards on its service and that an intermediate entity known as CIS had accepted the contractual responsibility to edit the bulletin board that had carried the defamatory messages. The court also noted that CompuServe received no compensation from the bulletin board and had no opportunity to review the contents of the bulletin board before the defamatory comments were published.

The court concluded that CompuServe was the modern equivalent of the corner news vendor selling numerous newspapers and magazines. As such, CompuServe could not be held responsible for defamatory information carried on individual bulletin boards. The court indicated that the network administrator could only be held civilly liable if he "knew or should have known" about improper or illegal network traffic. The court also observed that if a network administrator is viewed as a publisher, he is held to a higher level of responsibility. Moreover, the court observed that while CompuServe had received some information about problems on the bulletin board system in question, that information was not sufficient to prompt a further inquiry. Thus, the nature of the traffic played a significant role.

***Stratton Oakmont* v. *Prodigy*[2]**

In 1995, a New York state court came to the opposite conclusion as the court in *Cubby* v. *Compuserve*, finding that Prodigy could be held responsible for defamatory messages posted by one of the users of its service. At the time, this case expanded the potential liability of commercial online computer service providers, by determining that Prodigy could be held liable as a publisher of defamatory material for information posted on its network even though Prodigy maintained it was nothing more than a passive conduit of information and therefore should be treated only as a distributor (like a newsstand or a library) of news or information. In determining that Prodigy knew or should have known about the content of the defamatory material posted on Prodigy bulletin boards, the court recognized that Prodigy had put into effect a series of content review policies and had utilized editorial software to screen messages uploaded to the network. Accordingly, Prodigy did have affirmative responsibility for the contents of the messages posted by Prodigy users. The ultimate decision in this case, however, was superseded by the principles of liability and safe harbor contained in the Communications Decency Act of 1996.

***RTC* v. *Netcom*[3]**

In November 1995 a federal judge in California ruled that an Internet service provider could be held liable for contributory infringement for copyrighted material it made available online if it had notice of the copyrighted nature of the material and refused to delete it from its archives.

continued

BOX 3.2 Continued

RTC was the exclusive licensee to certain unpublished copyrighted works. RTC and its licensees maintain extensive security over these materials, which are central to the advanced spiritual development of Church of Scientology members. When RTC discovered some of its materials being posted in text file format on the Internet in late 1994 and 1995, it brought three lawsuits against the posters of the materials and the owners of the bulletin boards posting the materials. In two of the cases, Netcom and another ISP were named as defendants after they refused to remove the copyrighted information contained in the notice from RTC.

Netcom moved for summary judgment, arguing that they could not be held liable under principles of direct, contributory, or vicarious liability. The court partially agreed, granting summary judgment on the direct and vicarious copyright infringement liability theories. However, the court held that Netcom might be found liable for contributory infringement since, despite warnings from the RTC, it allowed new postings by the defendants and did not remove prior postings. On August 4, 1996, the RTC and Netcom[4] announced that their litigation had been settled on undisclosed terms. After the settlement, Netcom posted new guidelines for protecting intellectual property on its Internet service, allowing copyright holders to complain to Netcom about alleged postings of their copyrighted material. Of course, the legal duty to refrain from participating in copyright infringement flows directly from the Copyright Act.

***A&M Records, Inc.* v. *Napster, Inc.*[5]**

The decision of the Court of Appeals for the Ninth Circuit in the Napster litigation again demonstrates that operators of computer networks can be held liable for misconduct that occurs on such networks if they know or should know of the illegal uses. In *Napster*, the defendants created a file-sharing system that allowed individual users to, among other things, share copyrighted music files. In its suit against Napster for copyright infringements, the plaintiffs contended that Napster should be liable under theories of contributory and vicarious copyright infringement. As to contributory infringement, one key question was whether Napster knew or had reason to know of the direct infringement committed by Napster's users. On that issue, the court, relying on the prior Netcom decision, concluded that Napster had both actual and constructive knowledge that its users were engaged in illegal activities. Similarly, with regard to the issue of vicarious liability, the court concluded that Napster could be held liable for the activities of users on its network because of Napster's failure to police its system to rid it of illegal uses and the fact that Napster benefited financially from the continuing availability of illegal activities on its network.

Cyber Promotions* v. *Apex Global Information Services

The suggestion that there may be best practices with regard to online computer security is found in *Cyber Promotions* v. *Apex Global Information Services (AGIS)*.[6] In this case, AGIS had contracted to be the Internet service provider for Cyber Promotions. At the time of the contract, AGIS knew that Cyber Promotions regularly sent unsolicited commercial e-mail ("spam"), and it imposed a 30-day without cause termination provision in the contract. In September 1997, only 6 months after the contract was signed, AGIS suffered a massive flood attack direct-

ed at Cyber Promotions that completely consumed AGIS's bandwidth. AGIS responded by immediately terminating Cyber Promotions' use of its service.

Cyber Promotions then filed a temporary restraining order (TRO) and preliminary injunction. In granting the TRO against AGIS, the court noted that security requirements evolve, and AGIS had not taken significant steps to deal with ping attacks. The court noted that the only security step taken by AGIS was to remove Cyber Promotions from its network; AGIS had not hired a security expert or attempted to install a router to control potentially hostile ping attacks. The court's basic approach to AGIS was this: "Other ISPs are able to mitigate retaliatory actions by pingers, why not you?" The TRO was granted and AGIS was directed to reinstate service to Cyber Promotions. This result appears to have been substantially influenced by the fact that the court noted that AGIS had not taken the same measures as other reputable Internet service providers had taken to mitigate similar attacks.

---

[1]*Cubby* v. *CompuServe*, 776 F. Supp. 135 (S.D.N.Y. 1991).
[2]*Stratton Oakmont* v. *PRODIGY*, 1995 WL 323710 (N.Y.Sup.Ct.).
[3]*RTC* v. *NETCOM* 3, 907 F. Supp. 1361 (N.D.Cal. 11/21/95).
[4]*RTC* v. *NETCOM* 3, 907 F. Supp. 1361, at 14.
[5]*A&M RECORDS, Inc.* v. *NAPSTER, Inc.*, 239 F.3d 1004 (9th Cir. 2001).
[6]1997 WL 634384 (E.D. Pa. 1997).

companies that control the computer networks are in the best position to implement appropriate security measures[31] and are therefore the "lowest-cost avoiders." This cost-benefit analysis owes its origins to Judge Learned Hand's equation B < PL, in *United States* v. *Carroll Towing Co*.[32] According to Hand's logic, a party is negligent if the cost (B) of taking adequate measures to prevent harm is less than the monetary loss (L) multiplied by the probability (P) of its occurring.[33]

However, courts have traditionally limited third-party liability in two ways: (1) by excluding damages in negligence actions for purely eco-

---

[31]Alan Charles Raul, Frank R. Volpe, and Gabriel S. Meyer. 2001. "Liability for Computer Glitches and Online Security Lapses," *BNA Electronic Commerce Law Report*, 6(31):849.
[32]*United States* v. *Carroll Towing Co.*, 159 F.2d 169, 173-74 (2d Cir. 1947).
[33]See Alan Charles Raul, Frank R. Volpe, and Gabriel S. Meyer. 2001. "Liability for Computer Glitches and Online Security Lapses," *BNA Electronic Commerce Law Report*, 6(31):849 and Erin E. Kenneally. 2000. "The Byte Stops Here: Duty and Liability for Negligent Internet Security," *Computer Security Journal*, 16(2).
[34]Margaret Jane Radin. 2001. "Distributed Denial of Service Attacks: Who Pays?," <http://www.mazunetworks.com/white_papers/radin-print.html>.

nomic losses[34] and (2) by holding that intervening criminal acts break the chain of causation such that any breach of duty by the defendant would not be deemed the proximate cause of the harm to the plaintiff. The economic loss doctrine prohibits parties from recovering financial losses, absent injury to person or property, under tort law.[35] Many courts, however, are beginning to reject the economic loss doctrine. For example, in *People Express Airline* v. *Consolidated Rail Corporation*, the New Jersey Supreme Court concluded that "a defendant who has breached his duty of care to avoid the risk of economic injury to particularly foreseeable plaintiffs may be held liable for actual economic losses that are proximately caused by its breach of duty.[36] Similarly, if a court found that the likelihood of misconduct on networks was so great, the fact of the "intervening" criminal act would not necessarily be sufficient to break the chain of causation.

Standards and Best Practices

As a motivating factor for industry to adopt best practices, tort law can be a significant complement to standard-setting, because compliance with industry-wide standards is usually an acceptable demonstration of due care. If tort liability were recognized in this area, implementing security standards would be a way for a company to minimize its liability. Gripman argues that corporations have "a duty to select and implement security measures, to monitor the security measures' effectiveness, and to maintain and adapt the security measures according to changing security needs."[37] However, today there is no such duty and no nationally recog-

---

[35]Sarah Faulkner. 2000. "Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks," *Journal of Computer & Information Law*, 18:1019-1047.

[36]In *People Express Airlines* v. *Consolidated Rail Corporation*, 495 A.2d 107 (N.J. 1985), a railway accident caused a tank of flammable liquid to spill and ignite near the plaintiff's business. The fire caused no physical damage, but the plaintiff's business operations were interrupted, causing severe financial loss. The court rejected the economic loss doctrine and allowed the plaintiff corporation to prosecute its claim for purely economic loss.

[37]David Gripman. 1997. "The Doors Are Locked But the Thieves and Vandals Are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem," *The John Marshall Journal of Computer and Information Law* 16(1):167.

[38]The International Organization for Standardization (ISO) adopted in August 2000 the Code of Practice for Information Security Management (also known as ISO 17799), which is based on the British standard BS 7799. The standard has faced criticism from several countries and security experts, who argue that ISO 17799 is too vague because it focuses on general policies and best practices rather than concrete mechanisms for auditing compliance. However, some insurance companies, such as AIG, are using ISO 17799 as a basis to measure the security of cyber insurance policy holders. An analysis of ISO 17799 conducted by the Information Technology Laboratory of the National Institute of Standards and Technologies is available at <http://csrc.nist.gov/publications/secpubs/otherpubs/

nized standard of care[38] among computer security experts. Adopting such a standard is not a simple process due to the evolving nature of security vulnerabilities and the wide variety of the size and resources of individuals and entities that have an Internet presence. For example, applying security patches promptly may be one component required for demonstrating "reasonable care," but how often should patches be applied? Should a corporation be deemed negligent if its security policy is to search for and apply patches once a month but the corporation's servers were hacked in the third week after a patch was released? Determining the duty that a corporation should have is complicated by the fact that although a patch may close one vulnerability, it could open a new vulnerability when installed in a local environment. Should a corporation be deemed negligent if it installs a patch that leaves the system more vulnerable?

Eric Benhamou suggests that the one action that firms should take immediately is to begin sharing best practices (including attack scenarios and practices to protect against these attacks). Establishment of operational best practices for network administrators and users (combined with ongoing training and enforcement of the practices through intrusion detection tests) is one possible way of increasing computer security. The CERT Coordination Center at Carnegie Mellon University (a federally funded research and development center) and the SANS Institute are two examples of organizations working to develop and disseminate suggested best practices for computer security. Even with such organizations, adopting good security practices will not happen overnight, and implementation will vary.

In addition to playing a role in tort liability determinations, best practices can also serve as a benchmark against which firms can be audited. Audits, a normal part of business management, can be beneficial in the computer security arena. A firm is more likely to avoid litigation or reduce its liability if it is routinely audited and if its auditors apply well-accepted principles of testing and analysis, which do not yet exist in the security environment. Moreover, by forcing a corporation to understand what it will be audited for, auditing serves to educate the corporation on

---

reviso-faq.pdf>. Meanwhile, industry-specific standards are emerging. For example, Gramm-Leach-Bliley, implemented by the SEC, imposes rules that financial institutions must follow. The Health Insurance Portability and Accountability Act outlines the responsibilities that health care providers and insurers have with respect to security measures to protect electronic information.

[39]For example, the government recently announced that it was creating a security seal of approval that consists of a set of software standards that all DoD computers must meet. See "Government's Seal of Security," *Wired News*, July 16, 2002, <http://www.wired.com/news/politics/0,1283,53901,00.html>.

what is expected of it. Audits or certification programs[39] would also serve as a mark of acceptance for the corporation that will help it gain customer acceptance for its products and services and could result in reduced insurance premiums.

If a liability regime is imposed, entities may still be held negligent even if they comply with industry standards. In *T.J. Hooper* v. *Northern Barge Corporation*,[40] two barges towed by two tugboats sank in a storm. The barge owners sued the tugboat owners, claiming negligence and noting that the tugboats did not have weather radios aboard. The tugboat owners countered by noting that weather radios were not the industry norm. Judge Learned Hand found the tugboat owners liable for half the damages even though the use of weather radios had not become standard industry practice. He observed: "Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. . . . Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission." This case shows that the meaning of "reasonable care" is never static and must constantly be reevaluated as technology changes. Industry's failure to develop a standard or to adapt the standard to changes in technology could lead courts to develop their own standard.

Given the relatively novel nature of liability for insecure computer systems, one option is to create a safe harbor (immunity from tort liability) for corporations that comply with standards that are disseminated by a designated body. Care must be taken, however, to ensure that the establishment of best practices and associated safe harbor provisions does not deteriorate into a substitution of ritual for effective practices. In rapidly evolving areas, procedures or rituals may be all that can be standardized. Hence, although a liability regime could result in more compliance with the procedures and policies set forth in applicable standards, it may not actually improve network security. A corporation that is given safe harbor may not have sufficient incentive to surpass the prevailing standard (e.g., by implementing security policies, such as aggressive local testing of patches, that would provide it with a better level of protection) or to develop innovative solutions (e.g., to detect and resist computer attacks). Moreover, any improvement in network security achieved through a liability regime also could result in increased corporate liability for failing to follow sound information security procedures, even when data, systems, and networks are not actually put at risk.

Should all entities in the Internet community be held to the same standard of care with respect to computer network security? Legal liability

[40] 60 F.2d 737 (2d Cir. 1932).

often depends on which actors are best positioned to prevent the harmful activities (in this case, computer attacks). The committee has found it useful to examine the potential duty owed by a few key players: Internet service providers, vendors, universities and colleges, and individual users (see Box 3.3).

BOX 3.3
Assigning Liability to Key Players

Internet Service Providers

Distributed denial-of-service (DDOS) attacks[1] can be inbound to or outbound from the ISP's[2] network. Inbound DDOS attacks are launched from outside the ISP and either pass through or terminate on the ISP's customers. Outbound attacks are launched from computers connected to the ISP's network. An ISP can connect several thousands of high-bandwidth, always-on computers to the Internet. These computers as a group are prime targets for hackers, who can use them as zombies to launch an attack through the ISP's network to other targets on the Internet. When such an attack is launched, who is liable for damages?

ISPs are in a unique position to prevent or contain the harm caused through DDOS attacks in that they can cut off certain computer network attacks when these attacks enter the ISP's network. The high-capacity communications links and the powerful routers (switches) used by ISPs within their networks are much better positioned to deal with large volumes of DDOS packets than are the links and routers used by many end customers. This is particularly true if some changes are made to both the technical protocols used to move packets through the Internet and the routers (switches) that sort and route those packets. While ISPs could detect and cut off attacks, they have little incentive to do so today. Implementing better network security measures would cost the ISPs more money and could slow overall network performance, resulting in customer dissatisfaction. To efficiently and effectively identify packets as belonging to a DDOS, some changes (e.g., implementation of mechanisms that make it possible to reliably identify the origin of a packet and the route it has taken) might be required that reduce the anonymity enjoyed by Internet users today. In addition, some attacks are difficult to detect, analyze, and respond to, thus requiring advanced network management systems. The ISPs are largely unregulated,[3] and there are no formal standards imposed upon them by regulatory bodies for such things as the security, trustworthiness, or reliability of the services they provide.[4] ISPs' policies on incident response vary at the discretion of each ISP and its own best estimates of what may be required of it in a competitive marketplace, by its target customers, in the future.

Given that ISPs know (or should know) about the risk and have the capability to mitigate DDOS attacks, some experts believe that ISPs should face significant liability if their systems are insecure. However, some service providers argue that they should receive immunity for hostile traffic flowing through their networks.[5]

continued

BOX 3.3 Continued

Vendors[6]

Should vendors (hardware and software) be liable for developing products with extensive security flaws? Do companies that knowingly use defective products incur liability if their systems are used to launch a downstream attack? For example, hackers know that one particular hardware vendor ships routers in an insecure state. Because of this insecurity, companies know that they need to boot up the router and configure it before it is attached to the Internet. However, in one case, a summer intern did not know about the policy and attached the default-configured router to the Internet before reconfiguring the router. Within 30 seconds, a hacker broke into the company's network. Who should be held accountable—the vendor who knowingly shipped an insecure product or the company whose employee did not follow the company's established procedure? Certain vendors recognize that this is an instance of marketplace failure—that is, the marketplace does not reward those who invest resources in building more secure products. Customers want more features delivered more quickly. If there was a market demand for more secure products, vendors argue that they would change their approach.[7]

Some experts have called for vendors to be held liable for releasing products with security holes. Applying a strict liability standard for the computer security context seems unfair because software development is never a perfect process and most IT environments are too complex and diverse to ensure that a given product will perform exactly the same in every case. However, the CSTB report *Computers at Risk* notes that one way to reduce the frequency and severity of errors is through the use of tools and testing methods prior to the release of a software product. If the use of such tools and testing methods were part of industry-accepted best practices, vendors could be held liable for negligence if such tests are not performed. Accordingly, allowing vendors to be held liable for negligence would change the cost-benefit calculation to encourage the development and delivery of more secure computer products. Because such liability raises costs, vendors have lobbied against it (and for such measures as UCITA, which contains liability). However, there is some case law that supports the concept of vendor liability in connection with consumer products (*Shaw* v. *Toshiba*).

Universities and Colleges

Many universities have rather open, large-scale, high-capacity networks that can serve as a base from which hackers can launch attacks. Although some larger, well-funded universities and colleges have the resources and technical knowledge to implement appropriate security measures, not all do. In addition, providing an open environment that encourages information sharing and intellectual exploration is highly valued as an important role of U.S. educational institutions, and some security strategies would inhibit network-based interactions. Hence, it is not clear whether universities and colleges should face liability for failure to secure their computer networks. One approach is for the large research universities to set an example and play a lead role in designing and implementing secure computer network environments for all universities and colleges.

Individual Users

In the new age of broadband computing, home users represent a major source of potential security hazards. Should home users be liable if they do not take certain steps (e.g., apply software patches, install a firewall, or use antivirus software) to secure their computers? Most users simply buy a preinstalled PC or install their computer with default settings chosen by the software vendor. Typically, these default-configured installations do not provide any level of computer security. Therefore, it can be easy for a hacker to break into a home user's computer and use it as a zombie computer in a distributed denial-of-service attack. The average user does not necessarily have the knowledge to secure his or her home computer and may not even be aware of the risks.[8] Furthermore, even if the vast majority of end users were to proactively learn about and implement effective computer and network security measures, hackers would still be able to launch attacks with the remaining unprotected zombies.

"The average user is essentially clueless about how to prevent his computer from being taken over, so assigning liability to him would be pointless," argues Hal Varian.[9] While currently available "personal firewalls" (software on the user's home computer that is supposed to protect it from network attacks) are considered highly ineffective by the majority of the network security community, very effective stand-alone firewalls for small (e.g., home or small-office/home-office) networks need not be expensive or complex and can be configured to be very protective by default. The marginal cost of manufacturing a cable or DSL modem with one of these firewall devices integrated with it (i.e., sharing a chassis, power supply, or network interface) would presumably be very low. An effective firewall, conservatively configured, could largely prevent home computers from being attacked over the Internet no matter how security-poor the default software configuration of those computers. Yet, no supplier of broadband Internet services to the home is providing such integrated boxes to its users. Most experts agree that liability should be assigned to those entities that are best positioned to control the risks. However, it is not clear that home users yet have the initiative, education, or resources to maintain an adequately secured network. In the home user context, the service providers may be the least-cost avoider.

---

[1]The intent of a distributed denial of service attack is to reduce the availability of a computer network or resource below the level needed to support critical processing or communication. An attacker exploits security vulnerabilities to compromise one or more systems (often called "zombies"), which are then used to launch an attack against the target.

[2]This discussion focuses on ISPs with retail customers. ISPs whose business focuses on backbone connectivity and transport may not have directly connected end users, and they may face a different kind of legal context.

[3]The North American Network Operators Group is an educational forum that promotes the exchange of technical information and coordination among network operators in the United States. For more information, see <http://www.nanog.org>.

[4]The decision by many enterprises to implement multihoming arrangements (connecting the enterprise network to more than one ISP and routing traffic based on real-time availability

continued

BOX 3.3 Continued

and performance of connections) highlights the perception that ISPs do not deliver adequate and reliable service. See, for example, <http://www.routescience.com> or <http://www.sockeye.com>.

[5]Representative Bob Goodlatte introduced the On-line Criminal Liability Standardization Act of 2002. According to the Congressional Research Service summary, this act proposes to amend "the Federal criminal code to provide that no interactive computer service provider shall be liable for an offense against the United States arising from transmitting, storing, distributing, or otherwise making available material provided by another person. Waives such liability limitation where the defendant intended that the service be used in the commission of the offense. States that a provider does not have such intent unless: (1) an employee or agent has such intent; and (2) the conduct constituting the offense was authorized, requested, commanded, performed, or tolerated by one or more members of the board of directors or by a high managerial agent acting for the benefit of the provider within the scope of his or her office or employment." See <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03716:@@@D&summ2=m&> for more information.

[6]The committee is not addressing the provision in the USA PATRIOT Act that confers narrow immunity on vendors. It is a clarification of the CFAA, explaining that CFAA is aimed at hackers as perpetrators, not at vendors who may have noted the vulnerabilities.

[7]In response to calls for more secure software products, Microsoft launched the Trustworthy Computing Initiative in January 2002, which is purported to ensure the security and reliability of its software. The Sustainable Computing Consortium is a collaborative effort formed in May 2002 by industry and academia to drive improvements in software quality and security. See <http://www.microsoft.com/PressPass/exec/craig/05-01trustworthywp.asp> and <http://www.sustainablecomputing.org/> for more information.

[8]However, the FTC and other consumer-oriented agencies have launched a significant education campaign starring Dewie the Turtle, designed to increase the security awareness of the average home user. See <http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html>. The National Strategy to Secure Cyberspace also focuses on increasing the information security awareness of home users.

[9]Hal R. Varian. "Managing Online Security Risks." *New York Times*, June 1, 2000.

REGULATION

Often, Congress passes broad legislation that calls for implementing regulations to be promulgated by administrative agencies with oversight authority over certain regulated industries.[41] Direct regulation typically involves prescriptions and proscriptions (e.g., X is allowed but Y is not). An entity that fails to conform to the prescribed or proscribed conduct could face criminal liability. Broadly speaking, regulation that may relate to CIIP could come from any combination of four imperatives: efficient economic conduct, national security, public health and safety, and consumer protection. The purpose of economic regulation is to control

[41]The Administrative Procedures Act defines the processes for rule-making followed by various agencies.

behavior (e.g., supra-competitive pricing) associated with market power or monopoly. Regulation associated with national security and with public health and safety recognizes the obligations of providers of products and services to stakeholders beyond their direct customers. Consumer protection regulation places the regulator in the role of a surrogate for efficiently protecting direct consumers' interests (acting on behalf of those direct customers).

Telecommunications,[42] electric power, and other critical infrastructures have historically been regulated as utilities.[43] The regulatory status of these industries reflects perceived public interest, and it provides a basis for other government-industry interactions. An example relevant to CIIP is the rise of national security/emergency preparedness activities in telecommunications and the establishment of the Network Reliability and Interoperability Council, composed of industry representatives and staffed by the Federal Communications Commission. As those developments illustrate, regulation can be associated with certain kinds of reporting and the establishment of and conformance to certain performance standards, both of which have been sought for CIIP.

An entirely different category of regulation—consumer protection regulation—also contributes to CIIP, albeit indirectly, because such regulations target major users or suppliers of the critical information infrastructure. For example, the Gramm-Leach-Bliley (GLB) Act,[44] which gave rise to regulations implemented by several government agencies (including the banking agencies, the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC)), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[45] which gave rise to regulations under the jurisdiction of the Department of Health and Human Services, outline the responsibilities of financial institutions and health care providers and insurers, respectively, with regard to protecting consumer privacy. These acts and their implementing regulations speak to security measures that the institutions should implement to protect consumer information stored in their computer databases. On May 17, 2002, the FTC issued the Safeguards Rule, which implements the safeguard

---

[42]The telecommunications sector was regulated by the Communications Act of 1934 as amended by the Telecommunications Act of 1996. PL 104-104, February 8, 1996.

[43]The Defense Production Act of 1950 is an example of a regulation imposed on the private sector to ensure availability of industrial resources for national security purposes. For more information, see Congressional Research Service, "Defense Production Act: Purpose and Scope," June 22, 2001. Lee Zeichner argues that the DPA could be extended to critical infrastructure protection (Lee M. Zeichner. "Use of the Defense Production Act of 1950 for Critical Infrastructure Protection," 2001).

[44]15 USC, Subchapter I, Sec. 6801-6809. PL 106-102.

[45]PL 104-191.

provisions required by the Gramm-Leach-Bliley Act. The Safeguards Rule requires covered entities to implement a comprehensive information security program by May 23, 2003, to ensure the security, confidentiality, and integrity of nonpublic customer information against both internal and external threats. Institutions that fail to comply could face potential FTC enforcement actions and potential liability under state consumer protection laws or common law claims (such as negligence).[46] Recent FTC settlements[47] have established "reasonable security" as a written, comprehensive information security program that (1) designates appropriate personnel accountable for information security, (2) assesses security risks, taking into account, among other things, employee training, (3) implements reasonable security safeguards to control risks, and (4) adjusts the information security program in response to regular testing and monitoring. The GLB implementing regulations and recent FTC actions go a long way to setting the stage for best practices and may give rise to a de facto industry standard for negligence liability.[48] However, a number of questions remain about the FTC's de facto security standard. It is not clear whether ISO 17799 meets these requirements. Nor is it known what types of documentation, training, and supervision are necessary to meet the standard. The Microsoft settlement appears to indicate that damage is not necessary to trigger an FTC inquiry and the imposition of its security standard. Clearly, though, the recent FTC actions, combined with the GLB and HIPAA regulations, confirm that companies can no longer continue to address security issues informally.[49]

---

[46]GLB and HIPAA regulations have caused a seismic shift in the financial and health care industries (similar to the effect of Y2K on the computer industry) as institutions scramble to comply with the detailed requirements. If similar legislation could be passed in the CIIP arena, it might have equally extraordinary results. However, one major difference between CIIP and these other regulations is that CIIP does not have an immediately apparent benefit. In the case of Y2K, entire networks would purportedly have crashed if fixes were not put in place. In the case of HIPAA, Medicare payments will be withheld and other penalties may be imposed if HIPAA is not heeded. In the case of CIIP, we are largely dealing with what-if scenarios.

[47]Microsoft Corporation, File No. 012 3240, August 8, 2002, and Eli Lilly, File No. 012 3214, January 18, 2002. See the FTC Web site for more information: <http://www.ftc.gov>.

[48]Although not a precedent, the case of Ziff Davis Media Inc. shows how states (like the FTC) can use promises in privacy policies as a lever to enforce good security practices. The remedy includes a specific set of security provisions. For more information see <http://www.oag.state.ny.us/press/2002/aug/aug28a_02.html>.

[49]One potential consequence of the recent FTC actions might be efforts by a company to explicitly disclaim the suitability of its software for use in certain industries or applications, such as health care. Although the software may not differ substantially from what would normally be used, the disclaimer could be a shield to protect the company from threats or application of regulations or liability. It is not clear that such concerns are applicable in the CIIP arena, given that the information infrastructure is holistic and larger than one single industry.

The SEC, with a mission to protect investors and the securities markets,[50] oversees activities relating to traded securities. Its interests in avoiding fraud—a major consumer protection interest generally—have led to regulations requiring companies to disclose certain kinds of information about what they do and their circumstances, some of which relate to measures affecting the security and stability of a company's information infrastructure.[51] Disclosure is a common vehicle for consumer protection; it helps consumers protect themselves.[52]

One way to encourage companies to protect the critical infrastructures that they own and operate is to adopt disclosure agreements similar to those used during Y2K. In 1997, proposed legislation was introduced in Congress to require publicly traded companies to disclose certain information related to Y2K remediation and risk management status (via disclosure of Form 10Ks to the SEC). The SEC then published Staff Legal Bulletin No. 5, which reminded public companies, investment advisers, and investment companies to consider their disclosure obligations relating to anticipated costs, problems, and uncertainties associated with Y2K. The SEC released Interpretation No. 33-7558 in 1998, which superseded the staff legal bulletin. William J. Semancik, director of the Laboratory for Telecommunications Sciences at the National Security Agency, suggests that if we believe it is crucial that a company be up and operating for the sake of the country, then perhaps that company should be required to disclose the steps it is taking so the public can verify that the company is fulfilling its fiduciary responsibility.

Consumer protection is also the umbrella under which regulation of product quality falls. For CIIP, issues arise for the security dimension of the quality of computing and communications hardware and software. In the 1990s, both case law and efforts to revise the Uniform Commercial Code to address software more effectively progressed, but the eventual proposals for the Uniform Computer Information Transactions Act (UCITA), which would alter state law on contracts, were so controversial—in part because of allegations that they tipped the balance of power too far toward vendors—that they bogged down its passage in all the states but Maryland and Virginia.[53] The effort itself, though, illustrates

[50]The SEC's jurisdiction arises from the Securities Act of 1933 and the Securities Exchange Act of 1934. Other laws also shape the SEC's mission, notably including the Public Utility Holding Company Act of 1935, which provides reporting requirements for electric power and natural gas utilities.

[51]The SEC's reporting requirements for Y2K are an illustration.

[52]Sometimes a consumer's options may be limited, but disclosure may illuminate problems that will motivate parties to come up with alternatives.

[53]On August 2, 2002, a group of legal experts proposed several amendments to UCITA to address concerns about consumer rights. It is not clear whether the amendments will

the potential for lawmaking to influence vendor responsibilities under the law and to reframe liability.

As this brief overview illustrates, regulations relevant to CIIP are a patchwork. That situation will complicate any efforts to develop a regulatory framework (rationale, legal basis, agency oversight) for critical infrastructure protection. Hank Perritt, CSTB member and dean and professor of law at Illinois Institute of Technology, Chicago-Kent College of Law, suggests that regulation is really about a fundamental choice: whether the need for a robust, reliable, critical information infrastructure is better met by a highly centralized approach—the model for which is AT&T as it existed in 1965—or whether it is better served by a highly decentralized and very market-oriented and loosely regulated approach (such as is exemplified by the Internet).[54] Given how the economy and the information infrastructure have evolved, we have a decentralized system today. Any changes would have many ramifications. Many (including the current administration and the Internet community, which is often described as cyberlibertarian) view regulation by the government as interference in the market economy. On September 11, the Internet was very resilient (due in large part to a fair amount of redundancy),[55] which shows that a decentralized model does not necessarily produce a less robust infrastructure. A decentralized scenario does not foreclose the possibility of the law having more bite but, rather, offers a choice of instruments that are not necessarily regulatory. For example, Mr. Perritt suggests that contract and tort law could ratchet up the cost of having an insecure network, and this disincentive could be further strengthened through regulation, without eliminating competition or decentralization.

Regulatory compliance and the desire to avoid new regulations serve both to require and to motivate all parties to pay more serious attention to securing the nation's critical infrastructure against cybercrime and attack. The mere threat of such regulation could motivate vendors and corporations to self-regulate, providing their own standards and audit policies. The heightened interest in ISACs in 2002 is an indicator that the private sector is moving toward self-regulation. The government could periodically review such self-regulation efforts and provide reports showing deficiencies that would need to be corrected by a given deadline if regulation is to be avoided.

---

appease the many critics of the bill, including the Consumers Union and the Electronic Freedom Foundation. See <http://zdnet.com.com/2100-1104-948194.html>.

[54]This is not to suggest that centralization implies regulated and that decentralization implies loosely regulated.

[55]Computer Science and Telecommunications Board, National Research Council. 2003. *Internet Under Crisis Conditions: Learning from September 11*. National Academies Press, Washington, D.C.

4

Moving Forward

The law, which is mainly a tool for implementing policy, does not exist in a vacuum. The legal framework for critical information infrastructure protection must be considered in the larger context of the business, social, and technical environment. Phil Reitinger, former deputy chief of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, argues that critical information infrastructure requires a multidisciplinary response. First, he suggests, we need technical solutions. Vendors have to produce more secure products, and systems and customers have to demand and implement better security. Second, we need management solutions. Companies must adopt and share best practices. The third approach recommended by Mr. Reitinger is to develop public education[1] efforts to help all users better understand computer ethics (just as throwing a stone through a neighbor's window is wrong, so is breaking into someone else's computer system). Reducing nuisance attacks will allow government to focus resources on the greater threat. Finally, he proposes that we need knowledge solutions. The private sector and law enforcement must gather and share information about threats, vulnerabilities, and remedies. He argues, "[w]e have got to figure out how we can spread the information and better secure systems while protecting privacy and not increasing the threat."

[1]Education efforts most likely would need to be international in scope, given that a large number of computer-related problems originate overseas; recent incidents have come from countries such as Russia, the Philippines, and Romania.

MOTIVATING THE PRIVATE SECTOR

The U.S. government has historically relied on appeals to patriotism or threats of impending cyberattacks to encourage private sector entities to increase security initiatives. However, successful corporations focus on activities that contribute to increased profits, increased opportunities for profit, reduced constraints, and/or reduced risk. As Eric Benhamou observed, there is a tendency to "have a positive outlook on how technology will be created . . . and the concern about threats is very, very secondary, certainly no more than afterthoughts." That situation is compounded, suggests Milo Medin (formerly the chief technology officer for Excite@Home), by rapid Internet growth and competition, which have resulted in an environment where reducing expenses trumps infrastructure protection initiatives. This section looks briefly at the incentive problem that complicates policy making for critical information infrastructure protection.

Market Failure?

Eric Benhamou argues that there are several factors that complicate efforts to improve security. First, he points to an imbalance between the low cost of the tools to perpetrate an attack and the high cost of the defense mechanisms needed to protect against these attacks. Second, he notes that there are indeed well-known technical vulnerabilities inside many infrastructures, but enough hasn't been done to fix them because doing so is very hard. Third, implementation of a strong security policy conflicts with efforts to promote open communication environments. Mr. Benhamou observed that another complicating factor is an IT culture that favors speed and performance over lengthy security procedures and practices.[2] Finally, most of the technical vulnerabilities can only be overcome through collective, concerted action—something that has proven hard in numerous contexts, such as contending with gray-market resellers.

---

[2]Studies such as *Trust in Cyberspace* conclude that many vulnerabilities in large, networked information systems are not attributed to poor computer security per se, but to inadequate software engineering methodology and practices and insufficient consideration of robustness in system architectures. Companies often fail to follow standard security practices, such as implementing and enforcing access controls, implementing patches on a timely basis, and implementing normal preventative and diagnostic technologies such as firewalls and intrusion detection systems (Computer Science and Telecommunications Board. 1999. *Trust in Cyberspace*. National Academy Press, Washington, D.C.). For a discussion of the specific actions that can improve computer security, see Computer Science and Telecommunications Board. 2002. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. National Academy Press, Washington, D.C.

Externalities are common in computer network security and, as with pollution, they yield societal problems without motivating sufficient private action. There are a number of reasons—not mutually exclusive—why infrastructure owners may choose not to invest more heavily in security measures. In the absence of good data, itself a problem, one can speculate, and each of the potential reasons illuminates a different aspect of the situation. First, security measures may not be very effective—or effective enough to warrant the investment. Government investments in research and development of computer security measures may be a partial answer to this problem, and legislative and administrative activity through 2002 point to increasing support for such R&D.[3] Second, losses from security breaches may not be very large, or they may be covered by insurance (see next section) or self-insurance.[4] Third, losses from security breaches may be large but can be dealt with only if large numbers of parties coordinate to make the needed investments. Kunreuther and Heal[5] argue that computer network security is an example of interdependent security; the incentive that one conscientious network owner has to invest in security measures is reduced if the owner believes that other connected networks are insecure, which would undermine the impact of the conscientious owner's measures.[6] They argue that a set of positive and negative economic incentives (e.g., insurance, taxation, liability, standards, and coordinating mechanisms) needs to be developed. Fourth, losses from security breaches may be large, but each party expects others to make the needed investments.[7] When the cost of poor security is not borne by the source, there is no incentive for the problems to be fixed. In the present context, one might ask why each party apparently attempts to shift the

[3]See, for example, the Cyber Security Research and Development Act (PL 107-305).

[4]Some have argued, for example, that progress may not happen without catastrophic loss.

[5]Howard Kunreuther and Geoffrey Heal, "Interdependent Security: The Case of Identical Agents," at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=306405>.

[6]A reviewer observed that a person's incentives to invest in security is *increased* if others also invest in security (i.e., that investments in security are *complements*) may not always be true. Investments by one information infrastructure player may be at least a partial *substitute* for investments by another. For example, residential users of cable modems have been encouraged to install firewall software to compensate for the vulnerability they incur as a result of cable-Internet system designs; a different approach by cable system operators would diminish the investment needed by residential users, but if more residential users make this investment, it lowers the incentive for the cable operator.

[7]From this perspective, software vendors may create bugs, but their customers and distributors bear the cost of dealing with them; Internet service providers sell access to the entire Internet but guarantee only their part of the network; or individual users can create security hazards but bear no consequences of their actions.

investment burden to others. One possible answer is that a user cannot easily identify the source of the underinvestment that led to the security breach (e.g., whether it was due to the user's software, the ISP, the backbone to which the ISP is connected, or software used by others). In other words, the security breach may be a result of decisions made by parties that are outside the control of the party making the investment. Finally, losses from security breaches may be large, but assigning liability[8] for them is difficult. Another complicating factor is that computer network externalities are international in scope.

Dr. Semancik argues that there is no economic theory that can calculate the actual benefit from the deployment of computer security technology (i.e., that a certain investment will increase security by some amount). Part of the difficulty with cost-benefit analysis is that the cost of security breaches is not widely available or known—this is part of the data problem noted above. Companies are hesitant to disclose costs because of the effect it might have on shareholder value and/or confidence and associated risks of litigation. A related problem is that the large numbers associated with the cost of publicized national incidents such as distributed denial-of-service attacks are considered suspect because they depend on simple assumptions about the behavior of large numbers of parties and on a simple aggregation of resulting cost projections.[9]

The economics of computer security is currently a hot research topic; May 2002 saw an important national workshop on this topic co-located with a large technical conference.[10] One approach recommended by Dr. Semancik at the symposium is to develop economic models of computer security that would help corporations build a case for investments in security technology. These would vary among industries, yielding sets of investment curves for given levels of security and costs. This kind of research could bring together industry and government. Another option is to use the threat of liability—based on the tort law model that holds companies accountable to a duty of reasonable care—to create an incen-

[8]It should also be recognized that under some circumstances increasing the legal liability of attackers (tort-based liability of players was discussed in Chapter 3), including increasing the ability to enforce such liability, might actually *reduce* the amount of security in which participants invest. If perpetrators can be more effectively caught and convicted, the need for security may decrease. At the same time, causation may also run in the other direction: Actions that make it easier to prevent attacks may make it more difficult to convict perpetrators.

[9]Of course, they are used by vendors and policy makers to encourage more action, because exhortations often sound more compelling when statistics are invoked.

[10]Workshop on Economics and Information Security, University of California at Berkeley, May 17-18, 2002. Information is available online at <http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/>.

tive to improve network security (see Chapter 3). Ultimately the development of a risk-management model for computer network security will be driven by insurance, legal liability, and market forces.[11]

Insurance: Motivator for Good Behavior

Ty R. Sagalow, executive vice president and chief operating officer of American International Group, Inc. (AIG), eBusiness Risk Solutions, argues that the insurance industry can play a role "in motivating the private sector to protect our national infrastructures and to guard against cyberattacks." Insurance rewards good behavior by making insurance available or unavailable and increasing or decreasing a company's premiums. Insurance companies transfer the risk of a loss from the balance sheet of the company to the insurance carrier.

To qualify for insurance, companies must prove they are an acceptable risk. Sagalow suggests three components to managing risk: people, policies, and technology. First, he suggests that companies must have dedicated technology personnel, commitment from the board, and an active crisis management team. Corporate policies should be ISO 17799-compliant and should include regular ongoing training of all employees (including management). Sagalow noted that although no single standard (including ISO 17799) has emerged, a single standard would have a positive effect. He acknowledged that it might be necessary to develop industry-specific standards rather than relying on one all-encompassing standard, such as ISO 17799. Finally, companies must employ appropriate security measures. Examples include firewalls, antivirus software (updated daily), intrusion detection systems, monitoring/log review, scans, and regular backups. Most insurance carriers require companies to undergo an independent security evaluation of their network defenses before granting a policy. Many policies also require companies to pass ongoing random red-team intrusion detection tests in order to maintain coverage. The insurance premium often depends on the security measures implemented.

Although policies vary, AIG manages the following risks in its cyber-insurance packages: legal liability to others (arising out of a denial-of-service attack; transmission of a computer virus; libel, slander, or copyright infringement caused by the content of the company's Web page); damage, destruction, or corruption of data; loss of revenue due to a DDOS

[11]Kevin J. Soo Hoo, "How Much Is Enough? A Risk Management Approach to Computer Security," Workshop on Economics and Information Security, University of California at Berkeley, May 2002.

attack; loss of or damage to reputation; and loss of market capitalization and resulting shareholder lawsuits.

The paucity of data on cyberrelated losses makes it difficult to accurately price cyberinsurance policies. Mr. Sagalow noted, for example, that it was hard to quantify damage due to a DDOS attack (e.g., potential lost customers and damage to reputation). In spite of the dearth of data, the Insurance Information Institute expects cyber insurance to be a $2.5 billion market by 2005.[12]

R&D to Alter the Costs of Security

Wm. A. Wulf, president of the National Academy of Engineering, noted that "very little progress has been made in computer security, and there is no community of scholars, academic researchers doing basic long term research in computer security." A contributor to this problem is the lack of a funding agency that focuses on creating a cadre of researchers in computer security. Dr. Wulf argues that "without a long term basic research base, we are not going to make a lot of progress in this area."

Mr. Benhamou reported that PITAC contemplated recommending increased funding in fundamental R&D in the field of computer network security, specifically calling for research focusing on protecting and securing the information infrastructure and creating hacker-proof networks. Meanwhile, the Office of Science and Technology Policy has moved to coordinate and plan for research relating to CIP and homeland security aid, while the major funders of computer science R&D have been exploring ways to increase their attention to these issues.[13] Industry and the intelligence community, suggests Mr. Benhamou, must engage in focused information sharing to develop an understanding of the sophistication of the existing infrastructure, to create scenarios, and to formulate a corresponding defense. Such interaction has been encouraged by Richard Clarke, the former cybersecurity czar. Harriet Pearson, chief privacy of-

---

[12]"Internet Companies Seek Insurance Against 'Denial of Service,'" *E-Commerce Times*, July 30, 2002, at <http://www.newsfactor.com/perl/printer/18804/>.

[13]The National Strategy to Secure Cyberspace recommends that (1) the director of the OSTP coordinate the development of a federal R&D agenda; (2) DHS ensure that coordination mechanisms exist among among academic, industry, and government R&D efforts; and (3) the private sector focus near-term R&D efforts on highly secure and trustworthy operating systems. The National Strategy is available online at <http://www.whitehouse.gov/pcipb>. The National Science Foundation has engaged a computer scientist to coordinate its homeland security-relevant R&D. Also, there is federal support for the new Institute for Information Infrastructure Protection, involving individuals previously associated with federal critical information infrastructure protection programs, which is working to develop a national R&D agenda.

ficer of IBM, referred to research into autonomic computing networks (also called "self-healing networks"), in which the network detects intrusions and takes actions to shield itself. Such research may lead to lower-cost computer network security solutions, benefiting industry and improving the protection of critical infrastructures. But it raises challenging technical and legal issues in a world featuring interconnections among networks administered by a growing number and variety of parties in differing jurisdictions.

Awareness

Mr. Benhamou reported on the rise in recognition of critical infrastructure concerns in Silicon Valley. That region, a leader in the production and use of information infrastructure, has dealt recently with acute energy infrastructure problems and with a long-term rise in computer crime; it also features many companies with international operations, which raise additional concerns about vulnerabilities and their exploitation. Mr. Benhamou noted that many Silicon Valley firms have been the target of attacks on information infrastructure by Nigerian organized crime groups, for example, and individual executives have been targeted by terrorist groups. These incidents make clear that the stereotypical teenaged hacker is not the main concern. The highly publicized distributed denial-of-service attacks and worm incidents of 2000-2001 were seen as costly to victims, whose attention to Y2K had already underscored dependence on the information infrastructure. Thefts of or damage to intellectual property also have been growing for corporations.[14] Against this backdrop, the events of September 11 heightened awareness and concern, and they spurred consideration of enhanced communication and coordination at three levels—within enterprises, within and among industries, and between industry and government—to respond to threats to infrastructure. A lingering challenge is how to achieve a greater understanding of the problem and possible solutions in smaller companies, particularly those that cannot afford an information technology support staff. Small businesses often are not aware that they need better computer security than what they have—if they have any at all. Frederick R. Chang, president and CEO of SBC Technology Resources, Inc., argues that the convergence of the voice and data networks compounds the problem and suggests possible solutions (see Box 4.1). The new awareness extends to an understanding that the practices that have helped companies to thrive,

[14]Harriet Pearson also commented on an increase in corporate attention to security, referring to discussions she had been having with companies in the Midwest.

BOX 4.1
Network Convergence and CIIP

The convergence of the public switched telephone network (PSTN) with new communications technologies has created a complex telecommunications environment. With deregulation of the telecommunications industry, there are new entrants supplying broadband connectivity to the local and long-distance markets.

Traditional telecommunications companies have a heritage of five nines, 99.999 percent availability, which equates to five minutes of downtime per year. The expectation is that a customer will always get a dial tone when he picks up the telephone. As a result of many factors (competition, speed to market, profitability and so forth), the Internet, wireless networks, and the next generation network are not being built to the same survivable standards as the PSTN. On the other hand, the rise of packet-switching technology—including to support telephone service—introduces a different approach that can often provide as good or better robustness and reliability through alternatives for data paths relative to what the PSTN provides through failure-resistant equipment. Some of the consequences are very important for crisis situations. For example, the nature of the PSTN is such that, if one can get a dial tone at all, some fairly good service quality guarantees come with it; however "poor service is better than nothing" is not a choice the user has. By contrast, the packet-based best-efforts character of the Internet may be able to get *some* signal through under very adverse conditions. Whether availability of a poor signal that is still usable for some purposes should be taken into account when measuring network availability is a fairly subtle question.[1]

Mr. Chang suggested that more effort be made to leverage experience in telephony to enhance telecommunications robustness. For example, some of the lessons and experiences from the NSTAC and NCC (including structure, procedures, coordination of planning, approaches to interconnection, and so on) could be applied to the data network. In addition, it is important that the security and robustness lessons learned by the data network (e.g., virtual private networks, firewalls, and authentication technologies) be employed in the PSTN's digital initiatives such as voice over IP. These groups, along with the Network Reliability and Interoperability Council, are already reaching out to nontelephony providers, but there may be limits to how broad their reach can be.

NOTE: Adapted from a presentation by Frederick R. Chang, president and CEO of SBC Technology Resources, Inc.

[1]Experience with cellular service availability on September 11 suggests that people might prefer a poor voice signal to no signal. For further discussion, see Computer Science and Telecommunications Board, National Research Council, 2000, *The Internet's Coming of Age*, National Academy Press , Washington, D.C. and Computer Science and Telecommunications Board, National Research Council, 2003, *The Internet Under Crisis Conditions: Learning from September 11,* National Academies Press, Washington, D.C.

such as support for accessing corporate information networks and resources from afar, contribute risk as well as benefit. These practices provide a new, and more challenging, baseline for critical infrastructure protection than that of a few years ago.

Although awareness is a prerequisite to action, it does not guarantee it. As Mr. Benhamou describes, many experiences show that solo action can be costly—by, for example, attracting lawsuits from parties concerned about harm to their equity interests—and collective action is hard to achieve. Progress may begin within the corporation, for example by protecting whistle-blowers and by bringing in and supporting the work of professional risk managers. Ms. Pearson argued for thinking through how to simplify systems to facilitate control over information. Mr. Benhamou pointed to the financial-reporting disclosures associated with Y2K as an example of a positive incentive—a combination of disclosure and accountability—that could be replicated for motivating protection of critical information infrastructure.[15] He noted that companies may understand the risks associated with, say, problems in the Domain Name System that may interfere with their use of the Internet and associated e-commerce, but that these companies are seldom called to account for how they prepare for possible problems. Of course, in some instances bad press leads to calls for accounting for preparedness (or responses), and avoidance of bad press can itself be a motivator.

SECURITY AND PRIVACY TENSIONS

Historically, the debate about security and privacy in the United States has been characterized as a zero-sum game—more security implies less privacy. Prior to September 11, the debate had begun to shift toward a realization that the security of information systems and the protection of personal data and privacy are mutually reinforcing and compatible goals. The OECD's *Guidelines for Security of Information Systems*[16] states:

> [S]ecurity of information systems may assist in the protection of personal data and privacy. . . . Similarly, protection of personal data and

[15]James Dempsey, deputy director of the Center for Democracy and Technology, noted that there are disagreements about what should be disclosed and to whom. For example, Senator Bennett has called for more public disclosure by companies about their information system vulnerabilities while at the same time promoting less public disclosure through support of a FOIA exemption for critical infrastructure information. Dempsey called for more debate to set the rules.

[16]Organization for Economic Cooperation and Development, 1992. *Guidelines for Security of Information Systems*. Available at <http://www.oecd.org/EN/document/0,,EN-document-43-nodirectorate-no-24-10249-13,00.html>.

> privacy . . . may serve to enhance the security of information systems. The use of information systems to collect, store and cross-reference personal data has increased the need to protect such systems from unauthorized access and use. . . . It is possible that certain measures adopted for the security of information systems might be misused so as to violate the privacy of individuals. For example, an individual using the system might be monitored for a non-security-related purpose or information about the user made available through the user verification process might permit computerised linking of the user's financial, employment, medical and other personal data.

In the wake of September 11, the increasing number of measures aimed at protecting homeland security has fostered an increase in surveillance and intelligence-gathering activities, arousing concerns among privacy advocates. The discussion at the symposium anticipated changes that came into effect in 2002.

Whitfield Diffie noted that anonymity is a very powerful technique for protecting privacy. The decentralized and stateless design of the Internet is particularly suitable for anonymous behavior. Although anonymous actions can ensure privacy, they should not be used as the sole means for ensuring privacy as they also allow for harmful activities, such as spamming, slander, and harmful attacks without fear of reprisal. Security dictates that one should be able to detect and catch individuals conducting illegal behavior, such as hacking, conspiring for terrorist acts, and conducting fraud. For example, without trustworthy source information and/or trustworthy data regarding the route that a packet has taken from source to destination, it is difficult to defend against denial-of-service attacks. Today, it is easy to insert a phony source address into an Internet IP packet and, unless the originating ISP takes some action to reject packets originated by its users that don't match the IP addresses assigned to those users, the source IP address cannot be used to push back attacks. Likewise, routers do not add any metadata to IP packets that pass through them to indicate the route that has been taken. Legitimate needs for privacy (such as the posting of anonymous bulletin board items) should be allowed, but the ability to conduct harmful anonymous behavior without responsibility and repercussions—in the name of privacy—should not.

James Dempsey observed that better system security might reduce the need for surveillance and other potential intrusions into privacy.[17] However, surveillance can be a valuable tool in combating terrorists and hackers. The ability to track and monitor suspected terrorists and hackers and their supporters cannot be understated—it can lead to valuable clues

[17]This is an argument about substitution, as discussed earlier in the chapter.

and trails, and it can lead to the evidence needed to catch and convict guilty parties. On the other hand, it is important to ensure adequate protections are in place so that surveillance can be conducted without loss of privacy. Collected information must be secured, protected, and prevented from being used against people except for the intended purpose of catching and incriminating hackers and terrorists. While better system security may not reduce the need for surveillance, properly conducted surveillance for legitimate purposes should not result in a loss of privacy.

However, the crisis-management mentality in the aftermath of September 11 once again pushed aside issues of privacy and civil liberties. Although the July 2002 version of the OECD computer security guidelines mentions privacy—"Efforts to enhance the security of information systems and networks should be consistent with the values of democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy"[18]—it no longer emphasizes the mutual and compatible nature of privacy and security. Within the United States, a number of legislative and procedural initiatives, beginning with the USA PATRIOT Act, appear to have elevated attention to security. Congressional hearings, editorials, Web sites, and so on have sustained discussions about the support for different objectives. Technical mechanisms have been proposed to aid government efforts to promote security, and the law is seen more and more as the lever for balancing interests. It is increasingly difficult to separate law (or technology or business practice) relating to CIIP from that pertaining to homeland security. As a result, given popular concern about homeland security, many experts fear that privacy may suffer.

At the symposium, speakers and participants argued that the seriousness and urgency of the problem make it even more important to consider the value of privacy in crafting a solution. For example, Harriett Pearson noted that a researcher at the IBM Privacy Research Institute has developed a technology called "privacy preserving data mining," which allows information to be mined for patterns while preserving personally identifiable information. James Dempsey's presentation (see Box 4.2 for excerpts) eloquently captures the tension that continues to impinge on CIIP policy making.

[18]OECD. 2002. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Available at <http://www.oecd.org/pdf/M00033000/M00033182.pdf>.

BOX 4.2
Privacy and Security

[A]s a privacy advocate, I find I often have to overcome certain barriers to communication. . . . [I]n coming forward and criticizing some of the things that are being done, and saying that the privacy issues are not properly being taken account of, I sometimes find myself accused of not appreciating the nature of the threat, or not appreciating the urgency of the situation. I want to start out by putting that aside: . . . I care about the privacy issues precisely because I believe that this threat is so serious. . . . I think there is a fairly high likelihood that some of us in this room in the coming months and years will be victims of terrorist attacks, or will have family members who are. I see this as a very long term problem and a risk and a threat. But the seriousness of the risk, the urgency of the problem, only makes it more important that we get the solution right. It doesn't tell us what the solution will be. All too often—particularly I have seen this recently in the legislative debate—the urgency of the threat is taken as an excuse for not engaging in the kind of dialogue and faith and examination that is necessary. I will commend the National Academies, the National Academy of Engineering, and the Computer Sciences and Telecommunications Board for taking on this project and trying to engage in some practical, rational discourse.

Privacy in this debate is a value . . . that we share as part of our society, along with the other values that we have, including the value of security. The privacy advocates come to this debate and help us ask the questions that we need to ask: Are we doing the right things or not?

Now, at this point it is clear that the systems that we are dependent upon are not secure. They are vulnerable to attack. They are possibly a point to be attacked, in combination . . . with physical attacks. Obviously we are facing people who are very clever, very thoughtful, very patient. We obviously need to build greater security into our systems. The difficult questions [are] what do we do, and second, how do we create the incentives to achieve the goals that we have? . . . [W]hat are the incentives?

NOTE: Adapted from a presentation by James Dempsey.

A TRUST NETWORK

A common theme at the symposium was the importance of trust. Trust provides the foundation for approaches based on procedure or business practice, as opposed to law or technical mechanisms.

- Frederick R. Chang, "[O]ne of the successes you saw in the NSTAC and the NCC was that the people who were responsible for essentially the

nation's infrastructure were together. There was information sharing. They established trust."

- Lieutenant General Kelley, ". . . trust is absolutely key to establishing this two-way dialogue."
- Ronald L. Dick, "the government protects the nation's most critical infrastructures by building and promoting a coalition of trust . . . amongst all government agencies, between the government and the private sector, amongst different interests within the private sector itself and in concert with the greater international community. . . . InfraGard expands direct contact with the private sector and infrastructure owners and operators to build one thing: trust. . . ."
- James Dempsey, ". . . in some of the legislation that is being proposed, the question of what should be kept secret and what should be shared and how you define this trust network is completely missing, completely left discretionary."
- Philip R. Reitinger, "I think information sharing really only works effectively when it is voluntary. When people say, I want to share information, that means that information sharing has to be based on trust. You have to build trust."
- Glenn Schlarman, "Trust is important and the entity providing information has to get something of value in return or else that will be the first and last time they share."

Trust is not a new concept; it has been a central component of the government's CIP efforts over the past several years. John G. Grimes, chair of the Industry Executive Subcommittee of NSTAC and vice president of Raytheon Co., argued that trust is a simple concept that is very difficult to implement in reality. He reported that at NSTAC—often cited as an example of a successful public-private partnership for CIP information sharing—it took time and energy to break down the walls and build a trust network.

So, why have past efforts failed to build trust between partners? One argument is that the government's message to the private sector has varied, ranging from national security to the economic delivery of vital services to mixed messages in between. The transition from a focus on CIP to the larger concept of homeland security compounds the challenge of communicating what is wanted and why; it presents a bigger picture, which can be a good thing, but it may also make the objective so big and unfocused as to cause confusion.

The second problem is that the government interface within the private sector on CIP issues is quite confusing and not necessarily user friendly. The private sector, for example, often does not know which government entity it should be dealing with on CIP matters, whom it

should be sharing information with, or whom it can depend on within the government for up-to-date information. So far, one can argue that possible focal points include the Department of Homeland Security, FBI/NIPC, CIAO, the new Cybersecurity Board, and a mix of other government agencies: the FTC, FCC, SEC, DOE, DOD, and more. The new Department of Homeland Security is further altering the government landscape.[19] It may centralize some federal responsibilities for CIP, although it seems clear that others will remain distributed among many agencies. After this major organizational change is set in motion, the government should clearly and consistently explain to the private sector what its objectives are for CIP, how it has organized itself to accomplish those objectives, who is responsible for what (e.g., what are the information flows), what kind of information should be shared and in what form, and why all of this is important (i.e., what the threat is and how the proposed actions will address the threat). This message should clearly and consistently articulate what protections already exist for information sharing and what safe harbors exist (or will be established) to encourage information sharing in light of FOIA and antitrust concerns in the private sector. A clear and consistent message from the government to the private sector will go a long way toward building the trust that is necessary to protect the nation's critical information infrastructures.

[19]Observers note that the recent government-wide cybersecurity reorganization has increased confusion about where to go to report cybercrime incidents (Michael Fitzgerald, 2003, "Homeland Cybersecurity Efforts Doubled," *Security Focus,* March 11).

Appendixes

A

Committee Member and Staff Biographies

COMMITTEE MEMBERS

Stewart D. Personick (NAE), *Chair*, is an expert in telecommunications and information networking technologies and applications. Dr. Personick is currently the E. Warren Colehower Chair Professor at Drexel University and director of the Center for Telecommunications and Information Networking. He spent the first 15 years of his career at Bell Laboratories and at TRW, doing research and managing research in fiber-optics technologies and applications for telecommunications. Dr. Personick spent the next 15 years of his career at Bellcore (which became Telcordia Technologies, Inc.) doing research, research management, and management of systems engineering programs directed at emerging and next-generation telecommunications technologies and applications. He has played an active role over the last 10 years in the formulation of policy issues relating to the evolution and use of information infrastructures. For 5 years, he served as a member, and for 1 year as chair, of the Federal Networking Council Advisory Committee. He served as chair of the National Research Council committee that produced the report *Commercial Multimedia Technologies for 21st Century Army Battlefields*. In addition, Dr. Personick was a member of the CSTB committee that produced the report *Making IT Better*. He has served as a reviewer or the review referee for several other CSTB committee reports and is a member of the Board on Army Science and Technology (BAST).

Michael Collins, director of information technology at Lockheed Martin, is responsible for working strategic information technology issues that cross the corporation's diverse technical landscape. He is responsible for identifying emerging technology and ensuring its integration into the corporation. Mr. Collins has responsibility for tracking and integrating internal research and development (IR&D) plans across all corporate line-of-business areas. He manages an annual $20 million corporate R&D program with the GE Corporate Research and Development Labs and is caretaker of the strategic partnership between GE and Lockheed Martin. He is also the focal point for the corporation's R&D interface with Sandia National Laboratories that Lockheed Martin is under contract to operate. In that role Mr. Collins manages a $3 million corporate R&D program under the Shared Vision Program. He serves as executive director for the corporation's focus teams in advanced software technology, information fusion, information assurance, knowledge management system integration, and virtual environments. Mr. Collins also is the working interface between the corporation and the President's National Security and Telecommunications Advisory Committee (NSTAC).

William J. Cook is a partner at Freeborn and Peters. He is an experienced litigator (90 trials) with an international practice focused on technology issues. Mr. Cook specializes in information security law, computer and network security liability issues, intellectual property litigation, Internet and Web liability and commerce issues, e-commerce transactions, and competitive intelligence issues surrounding corporate efforts to monitor their competitive environment and the resulting liability issues. Prior to that he spent 16 years as an aassistant U.S. attorney in Chicago. From 1987 to October 1991, he prosecuted computer and telecommunications technology fraud and the illegal transfer of controlled technologies from the United States. He has lectured and written extensively on computer and telecommunications laws, vulnerabilities, and proactive countermeasures and criminal and civil liability for misappropriation of intellectual property. He teaches Internet and Web law as an adjunct professor at the University of Illinois Law School. As a member of the Illinois Attorney General's Commission on Electronic Commerce and Crime Committee, Mr. Cook assisted in drafting Illinois's Digital Signature Act. Mr. Cook has testified as an expert on Internet law and liability before the U.S. House of Representatives' Judiciary Committee, the Illinois State Assembly forum, and the Federal Communications Commission. He assisted with the British Department of Trade and Industry's formation of the British Computer Misuse Act of 1990.

Deborah Hurley is the director of the Harvard Information Infrastructure Project at Harvard University, adjunct lecturer in Public Policy at the John F. Kennedy School of Government, and a senior research associate in the Belfer Center for Science and International Affairs. From 1988 through 1996, Ms. Hurley was an official of the Organization for Economic Cooperation and Development (OECD), where she had responsibility for legal, economic, social, and technological issues related to information and communications technologies, biotechnology, environmental and energy technologies, technology policy, and other advanced technology fields. As the administrator in the Information, Computer and Communications Policy Division of OECD's Directorate for Science, Technology and Industry, she focused on identifying emerging issues related to protection of personal data and privacy, security of information systems, cryptography technology and policy, and protection of intellectual property. Ms. Hurley, after writing the seminal report on information network security for the OECD member nations in 1989, was responsible for the drafting, negotiation, and adoption by OECD member countries of the 1992 OECD Guidelines for Security of Information Systems. Ms. Hurley also initiated the OECD activities on cryptography technologies and policy in the early 1990s. She is a member of the Advisory Committee to the U.S. State Department on International Communications and Information Policy and co-chair of its Working Group on Security, Encryption and Export Controls. Ms. Hurley is a member of the board of directors of the Electronic Privacy Information Center (EPIC). She has been appointed to a 3-year term (2000-2003) as a member of the Advisory Committee on International Science of the American Association for the Advancement of Science. She served as chair of the 2001 Computers, Freedom and Privacy Conference (CFP 2001). Ms. Hurley is the author, with Viktor Mayer-Schönberger, of "Globalization of Communications" and "Information Policy and Governance" in John Donahue and Joseph Nye, Jr., eds., *Governance in a Globalizing World* (Brookings Institution Press, 2000). Other recent publications include *The First 100 Feet: Options for Internet and Broadband Access*, edited with James H. Keller (The MIT Press, 1999), and "Security and Privacy Laws: The Showstoppers of the Global Information Society," in *Masters of the Wired World* (Pitman Publishing, 1999).

Daniel Schutzer is vice president and director of external standards and advanced technology with the emerging technologies group at Citigroup. Dr. Schutzer is a member of the Financial Services Technology Consortium Board and is on the advisory board of the National Academy of Sciences. He was a member of the CSTB committee that produced *The Internet's Coming of Age* and has participated in other CSTB activities. He

currently has responsibility for interfacing with external organizations and standards bodies and for representing Citibank. This includes coordinating technology with business goals and priorities and keeping Citibank up to date with the latest technology and standards advances. Dr. Schutzer's projects include electronic banking and electronic commerce, bill presentment and payment, risk management, customer behavior modeling and mathematical marketing, and new product design. Advanced technologies under investigation include agent technology, machine learning, multimedia, biometrics, image and voice processing, and high-performance computing. Currently, he teaches part-time at Iona College in New Rochelle, New York, and at George Washington University in Washington, D.C. He holds a B.S.E.E. from the College of City of New York and an M.S.E.E. and Ph.D from Syracuse University. He has authored over 65 publications and 7 books.

W. David Sincoskie (NAE) is vice president of the Internet Architecture Research Lab at Telcordia Technologies, Inc. He has extensive experience with computer networking and communications technologies. Dr. Sincoskie helped the Defense Advanced Research Projects Agency (DARPA) with its long-range research strategy by participating in the information science and technology study group from 1994 to 1998. In the summer of 1995, he participated in a study that led to the creation of DARPA's program in active networks. In 1996, Dr. Sincoskie chaired a study on network management and survivability. In 1998, he co-chaired a study on smart objects. Before Telcordia, Dr. Sincoskie was project director for the NSFNet network access points in San Francisco and Chicago. He served on the Internet Architecture Board from 1993 to 1995. In 1991, he formed and led Bellcore's collaborations on local asynchronous transfer mode (ATM) with Apple, Digital, Hewlett-Packard, Sun Microsystems, and Xerox Palo Alto Research Center, resulting in the first publication of specifications for a new generation of LANs based on ATM technology, in 1992. He is a member of the National Academy of Engineering, elected for contributions in packet switching for integrated networks, and a fellow of the Institute of Electrical and Electronics Engineers. Dr. Sincoskie served on the CSTB committee that produced *Evolving the High Performance Computing and Communications Initiative to Support the Nation's Information Infrastructure*. Dr. Sincoskie is also an adjunct professor of computer and information science at the University of Pennsylvania.

Richard R. Verma serves as foreign policy advisor to Senator Harry Reid of Nevada. Mr. Verma is also an international affairs fellow with the Council on Foreign Relations. Previously, he was an attorney at Steptoe and Johnson, LLP, where his practice focused on U.S. trade sanctions,

export controls, and trade policy matters. He advised numerous clients on the legal issues surrounding critical infrastructure protection, information-sharing mechanisms, and U.S. government restrictions pertaining to the export of dual-use goods and technologies. Mr. Verma led the first-of-its-kind global study on the import, export, and use of encryption regulation in over 92 countries and oversaw the preparation of a 42-country guide on digital signatures, online privacy, and online consumer protection. He has represented a number of clients before the U.S. Congress and several administrative agencies. He drafted H.R. 2404, the Personal Medical Information Protection Act of 1999. Mr. Verma served as a law clerk to the Honorable John O. Marsh, Jr., the former secretary of the army, and worked as a field representative in Bucharest, Romania, for the National Democratic Institute for International Affairs. He received his B.S. from Lehigh University, a J.D. from American University, and an LLM in international and comparative law from Georgetown University Law Center.

Marc J. Zwillinger is a partner in the Washington office of Sonnenschein Nath & Rosenthal, where he leads the firm's Cyberlaw and Information Security efforts. Previously, Mr. Zwillinger was a partner at Kirkland & Ellis and was the leader of the Cyberlaw and Information Security practice group and a member of the firm's Technology Committee. Prior to joining Kirkland & Ellis, he worked in the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice. At the Department of Justice, he coordinated the investigations of several high-profile computer crime cases, including the 1997 penetration of U.S. military computer systems by an Israeli hacker ("Solar Sunrise"), the denial-of-service attacks that hit e-commerce sites in February 2000, and the "I Love You" virus. He also investigated and prosecuted cases involving violations of the Economic Espionage Act of 1996 (EEA) and was responsible for coordinating the Department of Justice's approval for charges filed nationwide under the EEA. He personally represented the government in *United States* v. *P.Y. Yang, et al.*, the first EEA case successfully tried in the United States. In private practice, he now provides advice and counsel on protecting the confidentiality, availability, and integrity of proprietary information and conducts internal investigations and litigation for companies that have suffered a breach of computer security or loss of trade secret technology. He also helps companies to assess and limit their risk resulting from e-commerce-related activities. He has lectured to a wide variety of audiences on topics related to computer crime and economic espionage and serves as an adjunct professor of cyberlaw at the Columbus School of Law at the Catholic University of America. He received a J.D., magna cum laude, from Harvard Law School in 1994 and then clerked for Judge Mark L. Wolf of the United States

District Court, District of Massachusetts. Prior to practicing law, Mr. Zwillinger received a bachelor's degree in political science from Tufts University in 1991.

STAFF

Cynthia A. Patterson is a study director and program officer with the Computer Science and Telecommunications Board of the National Academies. She is currently involved in several CSTB projects, including a project that explores the intersection of geospatial information and computer science research communities and a congressionally mandated study on Internet navigation and the Domain Name System. Ms. Patterson is also working on a joint study with the Board on Earth Sciences and Resources and the Board on Atmospheric Sciences and Climate on public-private partnerships in the provision of weather and climate services. Prior to joining CSTB, Ms. Patterson completed an M.Sc. at the Sam Nunn School of International Affairs at the Georgia Institute of Technology. Her graduate work was supported by the Department of Defense and Science Applications International Corporation. In a previous life, Ms. Patterson was employed by IBM as an IT consultant for both federal government and private industry clients. Her work included application development, database administration, network administration, and project management. She received a B.Sc. in computer science from the University of Missouri-Rolla.

D.C. Drake joined CSTB in September 1999. He is currently handling a number of projects, including the Internet after 9-11 and a research agenda for counterterrorism. He came to Washington in January 1999 after finishing a master's degree in international politics and communications at the University of Kentucky. Mr. Drake earned a B.A. in international relations and German from Rhodes College in 1996. He has worked for the Hanns-Seidl Foundation in Munich, Germany, and in Washington, D.C., for the National Conference of State Legislatures' International Programs Office and for the majority staff of the Senate Foreign Relations Committee.

B

Symposium Agenda

Opening Address

Wm A. Wulf
President, National Academy of Engineering

Setting the Stage

Eric Benhamou
Chairman, 3Com Corporation
"The Internet as a Critical Infrastructure"

Philip R. Reitinger
Deputy chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice
"Critical Infrastructure Protection: The Law Enforcement Perspective"

John G. Grimes
Chair, Industry Executive Subcommittee, National Security Telecommunications Advisory Council (NSTAC) and vice president, Raytheon Company
"NSTAC: A Proven Industry-Government Partnership to Protect Critical Information Infrastructures"

Colonel Timothy Gibson (U.S. Army)
Director of technology, Joint Task Force-Computer Network Operations
"Vulnerabilities of Military Information Infrastructures and the Consequences: DDOS Case Study"

James Dempsey
Deputy director, Center for Democracy and Technology
"Protecting Information Infrastructure, Protecting Personal Information and Expression"

Information Sharing: What, When, How, and with Whom?

Lieutenant General (retired) David J. Kelley
Vice president of Information Operations, Lockheed Martin
"Overcoming Reluctance: Cooperation Between the Government and Private Sectors"

William E. Cohen
Assistant general counsel for policy studies, Federal Trade Commission
"Understanding Antitrust: A Vehicle for Maintaining Market Forces"

David Sobel
General counsel, Electronic Privacy Information Center
"Freedom of Information Act: Public Safety Confronts Public Information"

Legal Issues

Henry (Hank) Perritt, Jr.
Dean and professor of law, Illinois Institute of Technology, Chicago-Kent College of Law
"The Many Legal Faces of CIP"

Craig Silliman
Director of the network and facilities legal team, WorldCom
"The View from an ISP"

Elliot Turrini
Assistant U.S. attorney, U.S. Department of Justice
"Criminal Law and Critical Information Infrastructure Protection"

The Role of Privacy and Civil Liberties in Protecting Critical Infrastructures

Richard M. Smith
Chief technology officer, Privacy Foundation
"The View from a Privacy Advocate"

Harriet Pearson
Chief privacy officer, IBM
"The View from the Private Sector"

Organizing for Action

Ronald L. Dick
Director, National Infrastructure Protection Center, Federal Bureau of Investigation
"Public-Private Partnership: Keys to Success"

Captain J. Katharine Burton (U.S. Navy)
Assistant deputy manager, National Communications System
"The Telecommunications Infrastructure During a National Emergency: Lessons from September 11th"

Judith Miller
Partner, Williams & Connolly LLP
"Regulating Government Intervention in the Information Age"

Glenn Schlarman
Office of Management and Budget
"Defense of the Homeland: How Government Agencies Can Work Together"

Motivating the Private Sector

Frederick R. Chang
President and CEO, SBC Technology Resources, Inc.
"Economic Incentives"

William J. Semancik
Director, Laboratory for Telecommunications Sciences, National Security Agency
"Building the Case for Economically Sound Investments in Security"

Ty R. Sagalow
Executive vice president and chief operating officer, American International Group, Inc., eBusiness Risk Solutions
"Cyber Insurance: Improving Security Through Risk Management"

Milo Medin
Chief technology officer, Excite@Home
"Protection Efforts Meet Business Pressures"

Herbert H. Yan
Director, Allegheny Energy Supply Co. LLC
"Comparative Perspective from the Energy Business"

Creative Alternatives

Steven M. Bellovin
Fellow, AT&T Research

Whitfield Diffie
Distinguished engineer, Sun Microsystems