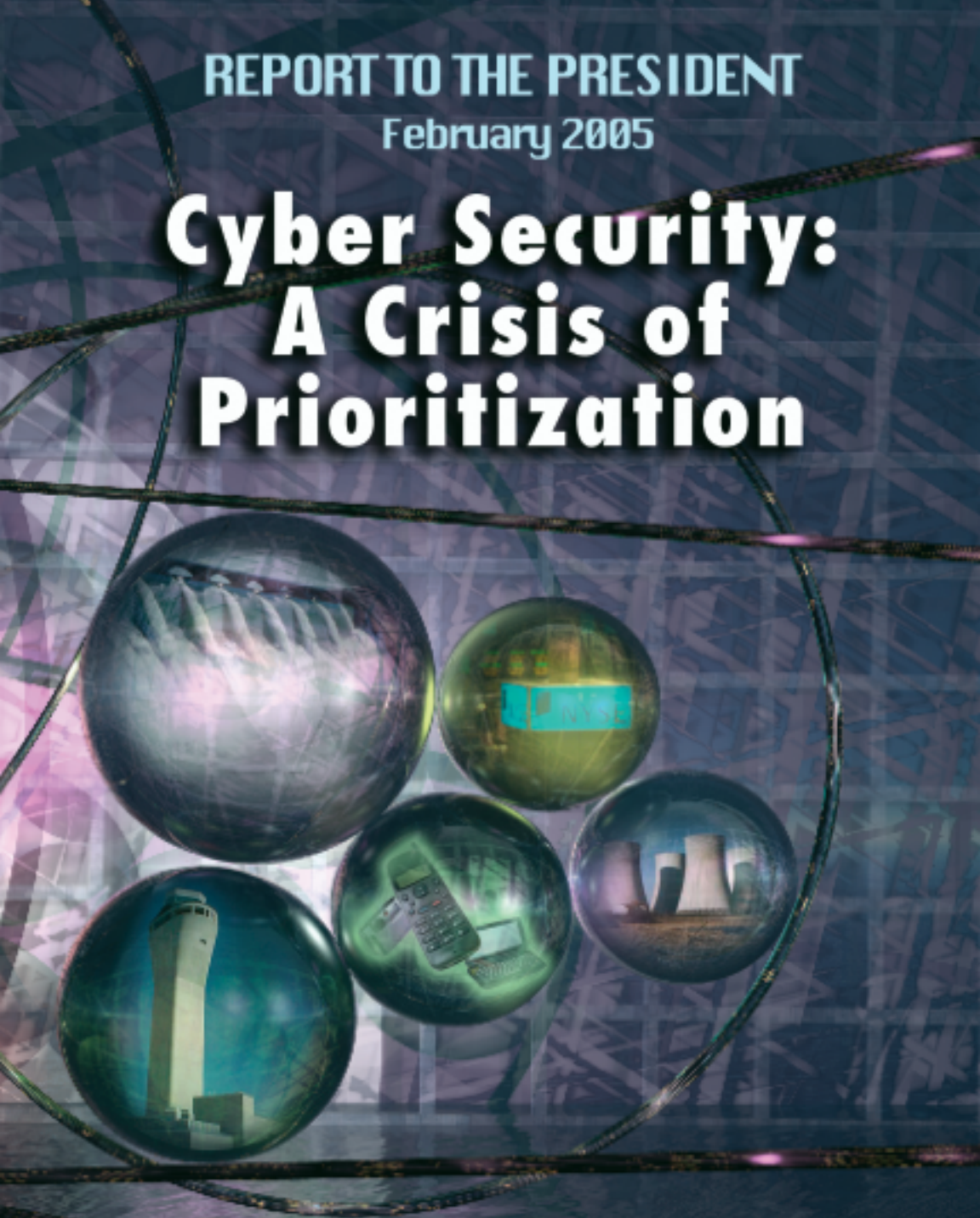
CERIAS Tech Report 2005-137
Report to the President on Cyber Security: A Crisis of Prioritization
by PITAC, Eugene Spafford
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

REPORT TO THE PRESIDENT

February 2005

Cyber Security: A Crisis of Prioritization



President's Information Technology Advisory Committee

Ordering Copies of PITAC Reports

This report is published by the National Coordination Office for Information Technology Research and Development. To request additional copies or copies of other PITAC reports, please contact:

National Coordination Office
for Information Technology Research and Development
4201 Wilson Blvd., Suite II-405
Arlington, Virginia 22230
(703) 292-4873
Fax: (703) 292-9097
Email: nco@nitrd.gov

PITAC documents are also available on the NCO Web site:
http://www.nitrd.gov

REPORT TO THE PRESIDENT

Cyber Security: A Crisis of Prioritization

President's Information Technology Advisory Committee

FEBRUARY 2005

President's Information Technology Advisory Committee

Co-Chairs:

Marc R. Benioff
Edward D. Lazowska

Members:

Ruzena Bajcsy
J. Carter Beese, Jr.
Pedro Celis
Patricia Thomas Evans
Manuel A. Fernandez
Luis E. Fiallo
José-Marie Griffiths
William J. Hannigan
Jonathan C. Javitt
Judith L. Klavans
F. Thomson Leighton
Harold Mortazavian
Randall D. Mott
Peter M. Neupert
Eli M. Noam
David A. Patterson
Alice G. Quintanilla
Daniel A. Reed
Eugene H. Spafford
David H. Staelin
Peter S. Tippett
Geoffrey Yang

February 28, 2005

The Honorable George W. Bush
President of the United States
The White House
Washington, D.C. 20500

Dear Mr. President:

We submit to you the enclosed report entitled *Cyber Security: A Crisis of Prioritization.* For nearly a year, the President's Information Technology Advisory Committee (PITAC) has studied the security of the information technology (IT) infrastructure of the United States, which is essential to national and homeland security as well as everyday life.

The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects. Thus, it is a prime target for cyber terrorism as well as criminal acts. The IT infrastructure encompasses not only the best-known uses of the public Internet – e-commerce, communication, and Web services – but also the less visible systems and connections of the Nation's critical infrastructures such as power grids, air traffic control systems, financial systems, and military and intelligence systems. The growing dependence of these critical infrastructures on the IT infrastructure means that the former cannot be secure if the latter is not.

Although current technical approaches address some of our immediate needs, they do not provide adequate computer and network security. Fundamentally different architectures and technologies are needed so that the IT infrastructure as a whole can become secure.

c/o National Coordination Office for Information Technology Research & Development
4201 Wilson Boulevard . Suite II-405 . Arlington, VA 22230
703-292-4873 (ITRD) . FAX (703) 292-9097 . nco@nitrd.gov . www.nitrd.gov

Page 2
February 28, 2005

Historically, the Federal government has played a vital, irreplaceable role in providing support for fundamental, long-term IT R&D, generating technologies that gave rise to the multibillion-dollar IT industry. The PITAC's review of current Federally supported R&D in cyber security finds an imbalance, however, in the current cyber security R&D portfolio: most support is for short-term, defense-oriented research; there is relatively little support for fundamental research to address the larger security vulnerabilities of the civilian IT infrastructure, which supports defense systems as well. Therefore, PITAC urges changes in the Federal government's cyber security R&D portfolio to:

- Increase Federal support for fundamental research in civilian cyber security by $90 million annually at NSF and by substantial amounts at agencies such as DARPA and DHS to support work in 10 high-priority areas identified by PITAC.
- Intensify Federal efforts to promote recruitment and retention of cyber security researchers and students at research universities, with an aim of doubling this profession's numbers by the end of the decade.
- Provide increased support for the rapid transfer of Federally developed cutting-edge cyber security technologies to the private sector.
- Strengthen the coordination of the Interagency Working Group on Critical Information Infrastructure Protection and integrate it under the Networking and Information Technology Research and Development (NITRD) Program.

These actions will lead the way toward improving the Nation's cyber security, thereby promoting the security and prosperity of our citizens. We would be pleased to discuss this report with you and members of your Administration.

Sincerely,

Marc R. Benioff
PITAC Co-Chair

Edward D. Lazowska
PITAC Co-Chair

President's Information Technology Advisory Committee

CO-CHAIRS

Marc R. Benioff
Chairman and CEO
Salesforce.com, Inc.

Edward D. Lazowska, Ph.D.
Bill & Melinda Gates Chair
Department of Computer Science & Engineering
University of Washington

MEMBERS

Ruzena Bajcsy, Ph.D.
Director, Center for Information Technology Research in the Interest of Society (CITRIS) and Professor
University of California, Berkeley

J. Carter Beese, Jr.
President
Riggs Capital Partners

Pedro Celis, Ph.D.
Software Architect
Microsoft Corporation

Patricia Thomas Evans
President and CEO
Global Systems Consulting Corporation

Manuel A. Fernandez
Managing Director
SI Ventures/Gartner

Luis E. Fiallo
President
Fiallo and Associates, LLC

José-Marie Griffiths, Ph.D.
Professor and Dean
School of Information and Library Science
University of North Carolina at Chapel Hill

William J. Hannigan
President
AT&T

Jonathan C. Javitt, M.D., M.P.H.
Senior Fellow
Potomac Institute for Policy Studies

Judith L. Klavans, Ph.D.
Director of Research, Center for the Advanced Study of Language and Research Professor
College of Library and Information Science
University of Maryland

F. Thomson Leighton, Ph.D.
Chief Scientist
Akamai Technologies, and
Professor of Applied Mathematics
Massachusetts Institute of Technology

Harold Mortazavian, Ph.D.
President and CEO
Advanced Scientific Research, Inc.

Randall D. Mott
Senior Vice President and CIO
Dell Computer Corporation

Peter M. Neupert
Consultant

Eli M. Noam, Ph.D.
Professor and Director of the Columbia Institute for Tele-Information
Columbia University

David A. Patterson, Ph.D.
Professor and E.H. and M.E. Pardee Chair of Computer Science
University of California, Berkeley

Alice G. Quintanilla
President and CEO
Information Assets Management, Inc.

Daniel A. Reed, Ph.D.
Chancellor's Eminent Professor, Vice Chancellor for Information Technology and CIO, and Director, Institute for Renaissance Computing
University of North Carolina at Chapel Hill

Eugene H. Spafford, Ph.D.
Professor and Director, Center for Education and Research in Information Assurance and Security (CERIAS)
Purdue University

David H. Staelin, Sc.D.
Professor of Electrical Engineering
Massachusetts Institute of Technology

Peter S. Tippett, M.D., Ph.D.
CTO and Vice-Chairman
TruSecure Corporation

Geoffrey Yang
Managing Director
Redpoint Ventures

CYBER SECURITY SUBCOMMITTEE

CHAIR

F. Thomson Leighton

MEMBERS

J. Carter Beese, Jr.
Patricia Thomas Evans
Luis E. Fiallo
Harold Mortazavian
David A. Patterson
Alice G. Quintanilla
Eugene H. Spafford
Peter S. Tippett
Geoffrey Yang

About PITAC and This Report

The President's Information Technology Advisory Committee (PITAC) is appointed by the President to provide independent expert advice on maintaining America's preeminence in advanced information technology (IT). PITAC members are IT leaders in industry and academia with expertise relevant to critical elements of the national IT infrastructure such as high-performance computing, large-scale networking, and high-assurance software and systems design. The Committee's studies help guide the Administration's efforts to accelerate the development and adoption of information technologies vital for American prosperity in the 21st century.

Chartered by Congress under the High-Performance Computing Act of 1991 (Public Law 102-194) and the Next Generation Internet Act of 1998 (Public Law 105-305) and formally renewed through Presidential Executive Orders, PITAC is a Federally chartered advisory committee operating under the Federal Advisory Committee Act (FACA) (Public Law 92-463) and other Federal laws governing such activities.

The PITAC chose cyber security as one of three topics for evaluation. The Director of the Office of Science and Technology Policy then provided a formal charge, asking PITAC members to concentrate their efforts on the focus, balance, and effectiveness of current Federal cyber security research and development (R&D) activities (see Appendix A). To conduct this examination, PITAC established the Subcommittee on Cyber Security, whose work culminated in this report, *Cyber Security: A Crisis of Prioritization.*

PITAC found that the Nation's IT infrastructure – integral to national and homeland security and everyday life – is highly vulnerable to attack. While existing technologies can address some vulnerabilities, fundamentally new architectures and technologies are needed to address the larger structural insecurities of an infrastructure developed in a more trusting time when mass cyber attacks were not foreseen. PITAC offers four findings and recommendations on how the Federal government can foster the development of new architectures and technologies to secure the Nation's IT infrastructure for the 21st century.

Outlined in the Executive Summary and discussed in detail in Chapter 4, the report's findings and recommendations were developed by PITAC over almost a year of study. The Subcommittee was briefed by cyber security experts in the Federal government, academia, and industry; reviewed the current literature; and obtained public input at PITAC meetings and a town hall meeting and through written submissions (see Appendix B for the Cyber Security Subcommittee Fact-Finding Process). The Subcommittee's draft findings and recommendations were reviewed by the PITAC on November 19, 2004 and the final report was approved at its January 12, 2005 meeting.

Table of Contents

PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE v

ABOUT PITAC AND THIS REPORT vii

TABLE OF CONTENTS ix

1 EXECUTIVE SUMMARY 1

Background 1

Summary of Findings and Recommendations 2

2 CYBER SECURITY: A PROBLEM OF NATIONAL IMPORTANCE .5

Trusting Systems in a Dangerous World 5

The Information Technology Infrastructure Is 'Critical' 5

Ubiquitous Interconnectivity = Widespread Vulnerability 7

Software Is a Major Vulnerability 9

Attacks and Vulnerabilities Are Growing Rapidly 9

Endless Patching Is Not the Answer 11

Fundamentally New Security Models, Methods Needed 12

Central Role for Federal R&D 13

Figure 1: Role of Federal R&D in Creating IT Industry 16

A Note on Non-Technology Aspects of Cyber Security 18

3 FEDERAL CYBER SECURITY RESEARCH AND DEVELOPMENT: CURRENT PRIORITIES, FUTURE IMPACTS 19

Cyber Security R&D in the Military and Intelligence Sectors 19

Federal Investments in Civilian Cyber Security R&D 21

The Relationship Between Military/Intelligence and Civilian Cyber Space 22

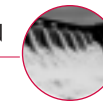
An Assessment of Current Federal Efforts 23

4 FINDINGS AND RECOMMENDATIONS 25

A Crisis of Prioritization 25

Finding and Recommendation 1: Federal Funding for Fundamental Research in Civilian Cyber Security 25

Finding and Recommendation 2: Cyber Security Research Community . . .30
Finding and Recommendation 3: Technology Transfer Efforts 32
Finding and Recommendation 4: Coordination and Oversight of Federal Cyber Security R&D 34
Cyber Security Research Priorities 37
1. Authentication Technologies 37
2. Secure Fundamental Protocols 38
3. Secure Software Engineering and Software Assurance 39
4. Holistic System Security 40
5. Monitoring and Detection 41
6. Mitigation and Recovery Methodologies 42
7. Cyber Forensics: Catching Criminals and Deterring Criminal Activities 43
8. Modeling and Testbeds for New Technologies 44
9. Metrics, Benchmarks, and Best Practices 45
10. Non-Technology Issues That Can Compromise Cyber Security . . .46
APPENDIX A: CHARGE TO PITAC 47
APPENDIX B: CYBER SECURITY SUBCOMMITTEE FACT-FINDING PROCESS 49
APPENDIX C: SELECTED MAJOR REPORTS ON CYBER SECURITY RESEARCH AND DEVELOPMENT 52
APPENDIX D: ACRONYMS 55
ACKNOWLEDGEMENTS 58



1 Executive Summary

The information technology (IT) infrastructure of the United States, which is now vital for communication, commerce, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices. The PITAC finds that the Federal government needs to fundamentally improve its approach to cyber security to fulfill its responsibilities in this regard.

Background

The Nation's IT infrastructure has undergone a dramatic transformation over the last decade. Explosive growth in the use of networks to connect various IT systems has made it relatively easy to obtain information, to communicate, and to control these systems across great distances. Because of the tremendous productivity gains and new capabilities enabled by these networked systems, they have been incorporated into a vast number of civilian applications, including education, commerce, science and engineering, and entertainment. They have also been incorporated into virtually every sector of the Nation's critical infrastructure – including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.

At the same time, this revolution in connectivity has also increased the potential of those who would do harm, giving them the capability to do so from afar while armed with only a computer and the knowledge needed to identify and exploit vulnerabilities. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. Moreover, we are rapidly losing ground to those who do harm, as is indicated by the steadily mounting numbers of compromised networks and resulting financial losses.

Beyond economic repercussions, the risks to our Nation's security are clear. In addition to the potential for attacks on critical targets within our borders,

our national defense systems are at risk as well, because the military increasingly relies on ubiquitous communication and the networks that support it. The Global Information Grid (GIG), which is projected to cost as much as $100 billion and is intended to improve military communications by linking weapons, intelligence, and military personnel to each other, represents one such critical network. Since military networks interconnect with those in the civilian sector or use similar hardware or software, they are susceptible to any vulnerability in these other networks or technologies. Thus cyber security in the civilian and military sectors is intrinsically linked.

Although the large costs associated with cyber insecurity have only recently become manifest, the Nation's cyber security problems have been building for many years and will plague us for many years to come. They derive from a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short-term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems. Rather, fundamental, long-term research is required to develop entirely new approaches to cyber security. It is imperative that we take action before the situation worsens and the cost of inaction becomes even greater.

Summary of Findings and Recommendations

The PITAC's recommendations on cyber security, and the findings upon which those recommendations are based, are summarized below.

Issue 1: Federal Funding Levels for Fundamental Research in Civilian Cyber Security

Long-term, fundamental research in cyber security requires a significant investment by the Federal government because market forces direct private sector investment away from research and toward the application of existing technologies to develop marketable products. However, Federal funding for cyber security research has shifted from long-term, fundamental research toward shorter-term research and development, and from civilian research toward military and intelligence applications. Research in these domains is often classified and the results are thus unavailable for use in securing civilian IT infrastructure and commercial off-the-shelf (COTS) products in widespread use by both government and the civilian sector. These changes have been particularly dramatic at the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA); other agencies, such as the National Science Foundation (NSF) and the Department of Homeland Security (DHS), have not stepped in to fill the gaps that have been

created. As a result, investment in fundamental research in civilian cyber security is decreasing at the time when it is most desperately needed.

The PITAC finds that the Federal R&D budget provides inadequate funding for fundamental research in civilian cyber security, and recommends that the NSF budget in this area be increased by $90 million annually. Funding for fundamental research in civilian cyber security should also be substantially increased at other agencies, most notably DHS and DARPA. Funding should be allocated so that at least the ten specific areas listed in the "Cyber Security Research Priorities" section beginning on page 37 of Chapter 4 are appropriately addressed. Further increases in funding may be necessary depending on the Nation's future cyber security posture.

Issue 2: The Cyber Security Fundamental Research Community

Improving the Nation's cyber security posture requires highly trained people to develop, deploy, and incorporate new cyber security products and practices. The number of such highly trained people in the U.S. is too small given the magnitude of the challenge. At U.S. academic institutions today, the PITAC estimates, there are fewer than 250 active cyber security or cyber assurance specialists, many of whom lack either formal training or extensive professional experience in the field. In part, this situation exists because cyber security has historically been the focus of a small segment of the computer science and engineering research community. The situation has been exacerbated by the insufficient and unstable funding levels for long-term, civilian cyber security research, which universities depend upon to attract and retain faculty.

The PITAC finds that the Nation's cyber security research community is too small to adequately support the cyber security research and education programs necessary to protect the United States. The PITAC recommends that the Federal government intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the Federal government should increase and stabilize funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.

Issue 3: Translating Research into Effective Cyber Security for the Nation

Technology transfer enables the results of Federally supported R&D to be incorporated into products that are available for general use. There has been a long and successful history of Federally funded IT R&D being transferred into

products and best practices that are widely adopted in the private sector, in many cases spawning entirely new billion-dollar industries. Technology transfer has been particularly challenging in the area of cyber security, however, because the value of a good cyber security product to the consumer lies in the reduced incidence of successful attacks – a factor difficult to quantify in the short term as a return on investment.

The PITAC finds that current cyber security technology transfer efforts are not adequate to successfully transition Federal research investments into civilian sector best practices and products. As a result, the PITAC recommends that the Federal government strengthen its cyber security technology transfer partnership with the private sector. Specifically, the Federal government should place greater emphasis on the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated; jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased; fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies; and encourage Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.

Issue 4: Coordination and Oversight for Federal Cyber Security R&D

One of the key problems with the Federal government's current approach to cyber security is that the government-wide coordination of cyber security R&D is ineffective. Research agendas and programs are not systematically coordinated across agencies and, as a result, misconceptions among agencies regarding each others' programs and responsibilities have been allowed to develop, causing important priorities to be overlooked. In the absence of coordination, individual agencies focus on their individual missions and can lose sight of overarching national needs. Initiatives to strengthen and enlarge the cyber security research community and efforts to implement the results of R&D would be more effective and efficient with significantly stronger coordination across the Federal government.

The PITAC finds that the overall Federal cyber security R&D effort is currently unfocused and inefficient because of inadequate coordination and oversight. To remedy this situation, PITAC recommends that the Interagency Working Group on Critical Information Infrastructure Protection (CIIP) become the focal point for coordinating Federal cyber security R&D efforts. This working group should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.

2 Cyber Security: A Problem of National Importance

Trusting Systems in a Dangerous World

The Nation's information technology (IT) infrastructure, still evolving from U.S. technological innovations such as the personal computer and the Internet, today is a vast fabric of computers – from supercomputers to handheld devices – and interconnected networks enabling high-speed communications, information access, advanced computation, transactions, and automated processes relied upon in every sector of society. Because much of this infrastructure connects one way or another to the Internet, it embodies the Internet's original structural attributes of openness, inventiveness, and the assumption of good will.

These signature attributes have made the U.S. IT infrastructure an irresistible target for vandals and criminals worldwide. The PITAC believes that terrorists will inevitably follow suit, taking advantage of vulnerabilities including some that the Nation has not yet clearly recognized or addressed. The computers that manage critical U.S. facilities, infrastructures, and essential services can be targeted to set off systemwide failures, and these computers frequently are accessible from virtually anywhere in the world via the Internet.

The Information Technology Infrastructure Is 'Critical'

Most Americans see and use the components of the IT infrastructure – mainly desktop computers connected to the Internet – that enable e-mail, instant messaging, exchange and downloading of sound and images, online shopping, information searches, interactive games, and even telephony. Americans also work with the information technologies that drive day-to-day operations in industry and government and are relied upon by organizations large and small for a range of functions including design, manufacturing, inventory, sales, payroll, information storage and retrieval, education and training, and research and development. In fact, economists credit successful applications of information technologies throughout the economy for the spectacular gains in U.S. productivity over the last decade.

> The IT infrastructure of the United States is highly vulnerable to terrorist and criminal attacks.

Less visible, and certainly less well understood, is the fact that these technologies – computers, mass storage devices, high-speed networks and

network components such as routers and switches, systems and applications software, embedded and wireless devices, and the Internet itself – are now also essential to virtually all of the Nation's critical infrastructures. Computing systems control the management of power plants, dams, the North American power grid, air traffic control systems, food and energy distribution, and the financial system, to name only some. The reliance of these sensitive physical installations and processes on the IT infrastructure makes that infrastructure itself critical and in the national interest to safeguard.

The electric power generation industry, for example, relies on a range of IT systems and capabilities. As in other industries, power companies implement business management systems for administrative and information services. But the power industry uses much more information technology. It relies on supervisory control and data acquisition (SCADA) systems to collect information about system operation, help regulate and control power generation, optimize power production, respond to changing power demands and system parameters, control distribution, and coordinate among the various generation and storage facilities within a power company system. Increasingly, SCADA systems are also used to integrate electric companies into regional or national power grids to optimize power production, minimize production and distribution costs, and provide backup services. This requires a private network that often includes links to the Internet. A cyber attack that disables key Internet nodes could disrupt the power network's communications. And if an entity within the private network is compromised, an attacker could gain direct control of the SCADA systems and their data and operation.

Computers, networks, and network components are now essential to virtually all of the Nation's critical infrastructures.

Today, the Internet also is used to manage essential services provided by business and government, such as electronic financial transactions, law enforcement dispatch and support, emergency response and community alerts, and military communications. Banks, for example, rely on extensive distributed Internet and information services, both for customer interaction and in interbank operations. To assure reliability and security of its most sensitive systems, the banking industry, like the power industry, uses private networks and is vulnerable to cyber attacks that cripple Internet nodes and/or result in unauthorized access to data and services. Such shared Internet links,

for example, enabled the "Slammer" worm to disable a major bank's ATM system and an airline's computer system, even though they were not directly connected to the Internet.

During a national emergency, it is imperative that the Nation's communications infrastructure be available for emergency response coordination. Today, that vital infrastructure is vulnerable to a variety of denial of service attacks, including the release of simple viruses and worms that can disrupt Internet communications as well as more sophisticated attacks in which modems from compromised servers are used to flood key parts of the telephone network (such as 911 services). The latter example demonstrates how a vulnerability in one system (e.g., the Internet) can be exploited to attack a totally separate system (e.g., the telephone network).

These examples illustrate how computing and computer communications have become integral to virtually every domain of activity in the U.S. today. Those systems are interconnected and interdependent in highly complex ways, which are often surprisingly fragile.

Ubiquitous Interconnectivity = Widespread Vulnerability

The Internet – now a global network of networks linking more than 300 million computers worldwide – was designed in a spirit of trust. Neither the protocols for network communication nor the software governing computing systems (nodes) connected to the network were architected to operate in an environment in which they are under attack. Indeed, the protocols used by the Internet today are derived from the protocols that were developed in the 1960s for the Federal government's experimental ARPANET. Only a few researchers used ARPANET and they were trusted to do no harm. The civilian networks, such as NSFNET, that developed from ARPANET into the Internet likewise did not incorporate security technologies at the system software or network protocol levels.

> Ubiquitous interconnectivity is the primary conduit for exploiting vulnerabilities on a widespread basis.

Ubiquitous interconnectedness – first exhibited by the Internet and further extended in local area networks, wide area networks, and wireless and hybrid networks – has generated whole new industries, rejuvenated productivity in older ones, and opened new avenues for discourse and education and an unprecedented era of collaborative science and engineering discovery

worldwide. That is indeed good news. The bad news is that ubiquitous interconnectivity provides the primary conduit for exploiting vulnerabilities on a widespread basis. Despite efforts in recent years to add security components to computing systems, networks, and software, the acts of a hostile party – whether a terrorist, an adversary nation, organized crime, or a mischievous hacker – can propagate far and wide, with damaging effects on a national or international scale. For example:

Acts of a hostile party can propagate far and wide.

- In the past several years, worms such as Code Red,[1] which defaces World Wide Web sites and/or launches distributed denial of service (DDoS) attacks,[2] and Slammer, which severely degraded the Bank of America's ATM network in January 2003, have caused damage estimated in the billions of dollars.
- The Department of Defense responded to the Code Red worm by disconnecting its unclassified network (NIPRnet) from the Internet to protect it from infection. This protective measure disabled the Army Corps of Engineers' control of the locks on the Mississippi River, since the NIPRnet was used to transmit commands to the locks through the Internet.
- By using a laptop computer and radio transmitter, a former contractor for an overseas wastewater system was able to assume command of hundreds of control systems that manage sewage and drinking water. Over a period of two months, hundreds of thousands of gallons of putrid sludge were intentionally released from the wastewater system.
- Many businesses are now being attacked by cyber extortionists who demand payment in return for not attacking the businesses' Web presence. Seventeen percent of the 100 companies surveyed in a 2004 poll by Carnegie Mellon University-*Information Week* reported being the target of some form of cyber extortion.

---

1 Most network worms spread by scanning the Internet, identifying vulnerable systems, and infecting those systems by installing themselves. Also see "Impact of Malicious Code" – September 2004, at http://www.computereconomics.com/.

2 A denial of service attack floods a target with artificial requests for service, thus rendering it unable to service legitimate ones. A distributed denial of service (DDoS) attack distributes the source of the artificial requests among many computers, thus greatly complicating the task of blocking a connection to eliminate a specific source of the artificial requests. The computers involved in a DDoS attack are generally the unwitting agents of the real attacker.

- Identity theft is a rapidly increasing problem for Internet users. One of the simplest methods of stealing a user's identity is known as "phishing," a technique that uses fake e-mail messages and fraudulent Web sites to fool recipients into divulging personal financial data. Consumers Union estimates that 1 percent of U.S. households fell victim to such attacks at a cost of $400 million in the first half of 2004.

Software Is a Major Vulnerability

Network connectivity provides "door-to-door" transportation for attackers, but vulnerabilities in the software residing in computers substantially compound the cyber security problem. As the PITAC noted in a 1999 report,[3] the software development methods that have been the norm fail to provide the high-quality, reliable, and secure software that the IT infrastructure requires. Software development is not yet a science or a rigorous discipline, and the development process by and large is not controlled to minimize the vulnerabilities that attackers exploit. Today, as with cancer, vulnerable software can be invaded and modified to cause damage to previously healthy software, and infected software can replicate itself and be carried across networks to cause damage in other systems. Like cancer, these damaging processes may be invisible to the lay person even though experts recognize that their threat is growing. And as in cancer, both preventive actions and research are critical, the former to minimize damage today and the latter to establish a foundation of knowledge and capabilities that will assist the cyber security professionals of tomorrow reduce risk and minimize damage for the long term.

Vulnerabilities in software that are introduced by mistake or poor practices are a serious problem today. In the future, the Nation may face an even more challenging problem as adversaries – both foreign and domestic – become increasingly sophisticated in their ability to insert malicious code into critical software.

Attacks and Vulnerabilities Are Growing Rapidly

Today, the threat clearly is growing. Most indicators and studies of the frequency, impact, scope, and cost of cyber security incidents – among both organizations and individuals – point to continuously increasing levels and varieties of attacks. The data show that the total number of attacks – including

[3] *Information Technology Research: Investing in Our Future.* President's Information Technology Advisory Committee, February 1999.

viruses, worms, cyber fraud, and insider attacks in corporations – is rising by over 20 percent annually, with many types of attacks doubling in number. For example, according to Deloitte's "2004 Global Security Survey," 83 percent of financial service organizations experienced compromised systems in 2003, more than double the percentage in 2001. Moreover, the reported level of security incidents almost certainly understates the actual level. There are few incentives – but strong disincentives – for large organizations to report incidents in a public forum. Targets of cyber attacks typically are concerned that widespread disclosure of their victimization could shake public confidence in their operations, not to mention attract other attackers.

Technology indicators and trends within large organizations clearly reflect rapid growth in the rate of cyber attacks.

Technology-oriented indicators clearly reflect the rapid growth in the rate of cyber attacks. For example, ICSA Labs reports that the monthly percentage of personal computers infected by a virus has grown from 1 percent in 1996 to over 10 percent in 2003. From January to June of 2004, the rate at which new hosts were compromised and incorporated into "bot armies" rose from well under 2,000 a day to more than 30,000 a day, according to the Symantec Internet Security Threat Report.[4] When compromised hosts are incorporated into bot armies, they can be used as platforms for launching denial of service attacks against a given target or to distribute "spam" e-mail without the knowledge or consent of the owners or operators.

Trends within large organizations are also disturbing. For example, the percentage of organizations that experienced virus disasters (defined as those with more than 25 simultaneous infections or with major impact from infection) has grown nearly every year over the last decade, with 92 percent of organizations reporting such incidents during 2003. Symantec reports that 40 percent of the networks controlled by the Fortune 100 companies were exploited to originate hostile worm traffic, despite the fact that these companies have taken a variety of protective measures. The cost, downtime, and days to recover from significant virus events have also trended upward for each of the past nine years, according to ICSA Labs data.

Meanwhile, the number of identified system and network vulnerabilities has also risen. The Computer Emergency Response Team Coordination

[4] http://enterprisesecurity.symantec.com/content.cfm?articleid=1539

Center (CERT/CC) at Carnegie Mellon University reports that 3,780 new electronic vulnerabilities were published in 2004, more than a 20-fold increase from 1995. Once published, most of the details of vulnerabilities are available for miscreants to begin attacking or developing attack tools and techniques, thus forcing users and organizations to scramble to assure that their defenses are adequate. The Symantec security threat report notes that in the first half of 2004, for example, the average time between the public disclosure of a vulnerability and the release of an associated exploit was 5.8 days, substantially reduced from the months estimated in prior years.

In fact, many IT system designs continue to incorporate characteristics that make these systems vulnerable to attack. In some instances, system designs may be pushing the state of the art, so their vulnerabilities may not be understood until they are deployed. In other instances, vulnerabilities may be designed into systems because the developers lack technical knowledge or fail to execute best practices. In this brief report, PITAC can point to only a few examples to provide the reader with a sense of the vulnerabilities of IT systems. But it is clear that that without action, IT vulnerabilities will become more severe, as computers, cell phones, and embedded systems proliferate globally and as expanding "always-on" high-speed or broadband connections enable attacks to propagate more rapidly and with more force than the occasionally connected low-bandwidth modems that were the norm until recently.

Endless Patching Is Not the Answer

A broad consensus among computer scientists is emerging that the approach of patching and retrofitting networks, computing systems, and software to "add" security and reliability may be necessary in the short run but is inadequate for addressing the Nation's cyber security needs. As computer security expert and PITAC member Eugene Spafford testified before the House Science Committee:

> Security cannot be easily or adequately added on after the fact and this greatly complicates our overall mission. The software and hardware being deployed today have been designed by individuals with little or no security training, using unsafe methods, and then poorly tested. This is being added to the fault-ridden infrastructure already in place and operated by personnel with insufficient awareness of the risks. Therefore,

> none of us should be surprised if we continue to see a rise in break-ins, defacements, and viruses in the years to come.[5]

Granted, our IT infrastructure may be less secure right now than it could be if all known security best practices were applied everywhere. But Professor Spafford's comment suggests that, even if all best practices were fully in place, in the absence of any fundamental new approaches we would still endlessly be patching and "plugging holes in the dike."

Fundamentally New Security Models, Methods Needed

We urgently need to expand our focus on short-term patching to also include longer-term development of new methods for designing and engineering secure systems. Addressing cyber security for the longer term requires a vigorous ongoing program of fundamental research to explore the science and develop the technologies necessary to design security into computing and networking systems and software from the ground up. Fundamental research is characterized by its potential for broad, rather than specific, application and includes farsighted, high-payoff research that provides the basis for technological progress.[6]

The vast majority of cyber security research conducted to date has been based on the concept of perimeter defense. In this model, what is "inside" an information system or network is protected from an "outside" attacker who tries to penetrate it to gain access to or control its data and system resources. However, once the perimeter is breached (whether by virtue of a technical weakness such as a software vulnerability or an operational weakness such as an employee being bribed or tricked to reveal a password), the attacker has entirely free rein and can compromise every system connected in a network with not much more effort than is required to compromise only one.

The weakness of the perimeter defense strategy has become painfully clear.

This weakness of the perimeter defense strategy has become painfully clear. But it is not the only problem with the model. The distinction between "outside" and "inside" breaks down amid the proliferation of wireless and

---

5 http://www.house.gov/science/hearings/full/oct10/spafford.htm

6 Adapted from National Research Council, *Assessment of Department of Defense Basic Research,* National Academies Press, 2005.

embedded technologies connected to networks and the increasing complexity of networked "systems of systems."

One element of a more realistic model for cyber security may be a principle of mutual suspicion: Every component of a system or network is always suspicious of every other component, and access to data and other resources must be constantly reauthorized. More generally, cyber security would be an integral part of the design process for any large, complex system or network. Security add-ons will always be necessary to fix some security problems, but ultimately there is no substitute for systemwide end-to-end security that is minimally intrusive.

Central Role for Federal R&D

"The National Strategy to Secure Cyberspace" states that the private sector has the most important role to play in cyber security. The PITAC agrees with this conclusion as it pertains to relatively short-term efforts to improve the security of today's systems and networks. But the Federal government has a vital, irreplaceable role to play as well. As at earlier stages of the digital revolution, Federal investment in fundamental research is required to fill the pipeline with new concepts, technologies, infrastructure prototypes, and trained personnel needed for the private sector to accomplish its cyber security mission. The Government can also promote technology transfer mechanisms that accelerate adoption of these new technologies by industry, in part by supporting the development of performance metrics, models, datasets, and testbeds so that new products and best practices can be evaluated.

Federally sponsored fundamental research is a unique national investment in the production of new knowledge that can be used across all sectors of society for the common good.

Federally sponsored fundamental research is a unique national investment in the production of new knowledge that can be broadly used across all sectors of society for the common good. Such research takes place primarily in universities and national laboratories. As for-profit entities, companies typically focus on short-term results or proprietary research that can provide

near-term competitive advantage. It is the mission of research universities to take the long-term view of a problem. Unclassified research performed in universities and national laboratories has the added benefit of creating trained talent in the field, as university graduates obtain employment in industry, universities, and government. University graduates who pursue advanced degrees in IT become the new generation of research leaders; other graduates frequently become involved in start-up companies, which have historically played critical roles in the IT industry. Research at universities also accelerates changes in the education of new college graduates, as researchers rapidly move new ideas into undergraduate courses and textbooks.

Fundamental research focuses on problems of extraordinary difficulty and complexity that often require a number of years to solve. As Figure 1 on pages 16 and 17 demonstrates, the Federal government has long played a central role in supporting fundamental research in information technology. The results of this research lie at the heart of many of today's billion-dollar information technology industries – industries that are transforming our lives, driving our economy, and enhancing our security. Fundamental research is a "public good" – hence the role of the Federal government in supporting it. The result of a highly effective interplay of Federally supported fundamental research, industry-supported applied research, and industry product development: The United States today is the world leader in information technology.

An expanded portfolio of Federal cyber security R&D efforts is required because today we simply do not know how to model, design, and build systems incorporating integral security attributes such as mutual suspicion – or any other fundamental security innovations. In addition, we face substantial new challenges from the constant stream of emerging technologies. For example, we do not fully understand the security ramifications of networks of embedded devices. In that context, a principle of mutual suspicion would have to consider controlled access to the subnetworks, the information stores, the devices that are interconnected, and the computing and communication resources of a given network. In our

An expanded portfolio of Federal cyber security R&D efforts is required because today we simply do not know how to model, design, and build systems incorporating integral security attributes.

current methods of software development, security is simply one more incremental requirement further burdening an already cumbersome, slow, and expensive process. The add-on approach will not address our fundamental need for far-sighted advances in systems and software technologies that provide innovative new approaches to the problem of security.

In the findings and recommendations in Chapter 4 of this report, we urge a rethinking of the Federal investment balance between military/intelligence and civilian cyber security R&D. In part, this is because the military and intelligence communities rely on the commercial Internet and commercial providers of computing systems and software for the bulk of their own operations.[7] It is only through fundamental research in civilian cyber security that we can hope to address the strategic and pervasive vulnerabilities of our national IT infrastructure.

We also underscore the importance of technology transfer because new concepts do not appear in products automatically. For this to happen, IT vendors must build into their products and services new security functionalities. But vendors respond to what users demand, and it is only recently that most users – corporations, government agencies, and individual users – have begun to care about cyber security. In the absence of significant demand for cyber security, IT vendors have mostly chosen to add new features for which customers are willing to pay. (Ironically, the addition of new features and added complexity often leads to the introduction of more security vulnerabilities.) This market-driven bias away from cyber security is the "valley of death" for cyber security noted by many analysts. R&D may provide the knowledge and the proof of operational feasibility, but in the absence of customer demand for the security that may be provided, vendors have little incentive to include new security technologies in their products.

In the findings and recommendations of this report, we urge a rethinking of the Federal investment balance between military/intelligence and civilian cyber security R&D.

7 Two examples from Operation Iraqi Freedom illustrate this reality: (1) more than 80 percent of the bandwidth used by the U.S. military was supplied by commercial providers, and (2) a large fraction of the IT systems deployed were shipped directly from commercial vendors. "U.S. Weaponization of Space: Implications for International Security," Theresa Hitchens, September 29, 2003. http://www.cdi.org/friendlyversion/printversion.cfm?documentID=1745.

Historic Role of Federally Supported Fundamental R&D

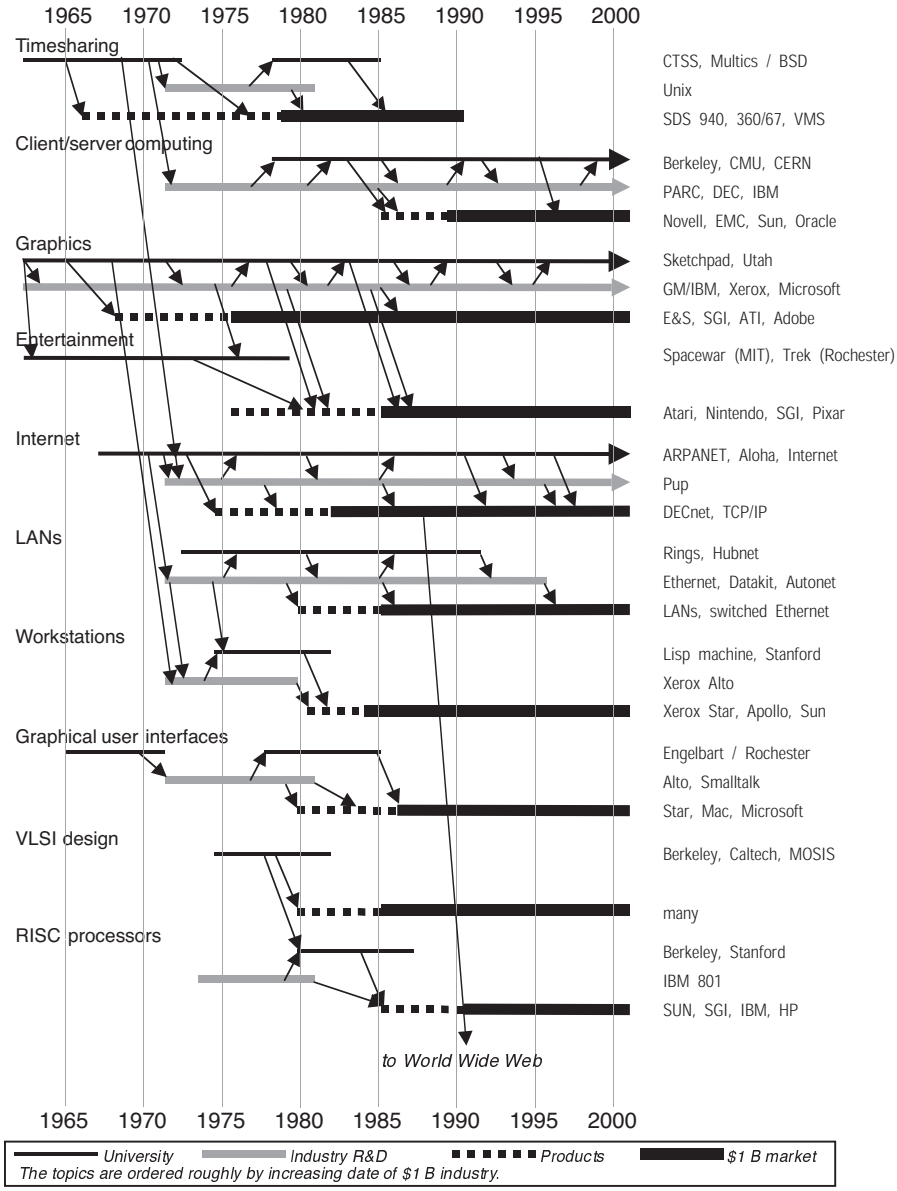
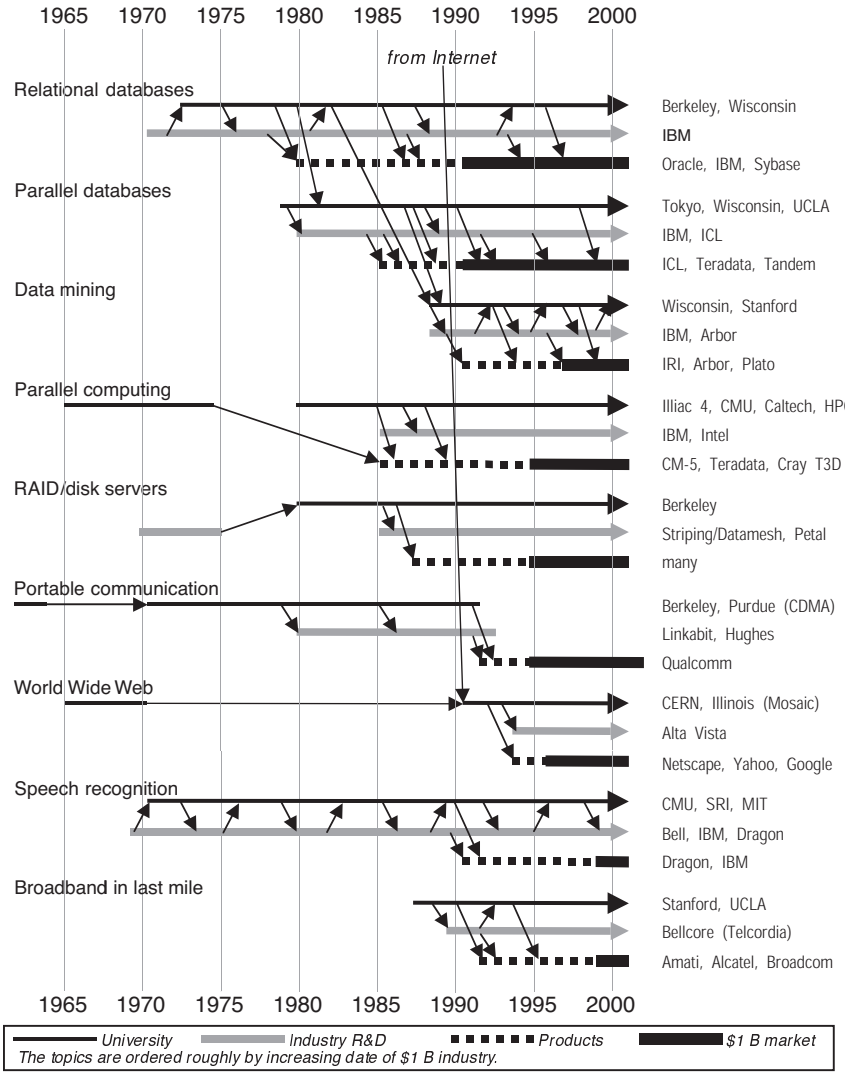


Figure 1

The role played by Federally sponsored fundamental research in information technology in creating billion-dollar segments of the IT industry. Reprinted with permission from *Innovation in Information Technology* (c) (2003) by the National Academy of Sciences, courtesy of the National Academies Press, Washington, D.C.

in Creating Billion-Dollar Segments of the IT Industry



A Note on Non-Technology Aspects of Cyber Security

PITAC recognizes that the development of technologies to counteract vulnerabilities or – better yet – designs that avoid vulnerabilities in the first place, constitute only one component, although arguably the most important component, of effective cyber security. We briefly point here to several facets of cyber security that require societal attention but are not addressed in this report:

Domestic and international law enforcement. A hostile party using an Internet-connected computer thousands of miles away can attack an Internet-connected computer in the United States as easily as if he or she were next door. It is often difficult to identify the perpetrator of such an attack, and even when a perpetrator is identified, criminal prosecution across national boundaries is problematic.

Education. We need to educate citizens that if they are going to use the Internet, they need to continually maintain and update the security on their systems so that they cannot be compromised, for example, to become agents in a DDoS attack or for "spam" distribution. We also need to educate corporations and organizations in best practices for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.

Information security. Information security refers to measures taken to protect or preserve information on a network as well as the network itself. Thus it also involves physical security, personnel security, criminal law and investigation, economics, and other issues. These factors need to be included in the curriculum for cyber security practitioners, and supporting law and technologies need to be made available.

Sociological issues. There are several areas relating to cyber security in which there may be conflicting interests and needs, and such tensions will need to be addressed as part on any comprehensive approach to cyber security. For example, as part of the effort to prevent attacks or to track down cyber criminals, it may be necessary to know the origin of data packets on the Internet, but such knowledge may be perceived by some to conflict with an individual's right to privacy or anonymity. To cite another example, what some nations or individuals may perceive as a necessary filtering of data may be perceived by others as unwanted censorship. Such issues involve ethics, law, and societal concerns as much as they do technology, and these non-technology issues make the cyber security problem even more challenging.

3 Federal Cyber Security Research and Development: Current Priorities, Future Impacts

To assess how well the Federal government is fulfilling its important role in providing support for cyber security R&D, the PITAC examined the current Federal cyber security R&D portfolio. As expected, Federal support for cyber security R&D is provided by the military, the intelligence community, and the civilian research sector. The Committee's analysis of agency investments found that the Federal government's historical focus on fundamental, unclassified R&D has changed in ways that place our long-term physical and economic security at risk.

Cyber Security R&D in the Military and Intelligence Sectors

Recognition of the potential benefits of communication between geographically distributed computing systems led the Defense Advanced Research Projects Agency (DARPA)[8] to develop the ARPANET, the forerunner of today's Internet. Today, the military's vision of ubiquitous connectivity has been dramatically realized.

The Armed Forces now critically depend on the networked IT systems that have amplified battlefield effectiveness and permanently transformed military strategy. However, the architecture of these networks and systems was defined in a different environment – an environment of trust. Today, ill-intended individuals, organizations, and governments can become armed with the knowledge and tools needed to compromise IT networks. As a result, the security of these networks of systems has become of paramount importance to the military.

The R&D budgets of the defense agencies reflect this urgency. The most sizable investment within the Department of Defense's cyber security programs is found at DARPA, though the research agencies of the Armed Forces have smaller but valuable cyber security programs as well. The Department of Defense's Office of the Director, Defense Research and Engineering provides coordination and oversight, in addition to supporting some cyber security research activities directly.

DARPA historically used a large portion of its budget to fund unclassified long-term fundamental research – in general, activities with a time horizon

[8] At the time, it was called the Advanced Research Projects Agency.

that exceeds five years. This provided DARPA with access to talented researchers in the Nation's finest research institutions and helped cultivate a community of scholars and professionals who developed the field. By FY 2004, however, very little, if any, of DARPA's substantial cyber security R&D investment[9] was directed towards fundamental research. Instead, DARPA now depends on NSF-supported researchers for the fundamental advances needed to develop new cyber security technologies to benefit the military. Additionally, the emergence of cyber warfare as a tool of the warfighter has led DARPA to classify more of its programs. The combined result is an overall shift in DARPA's portfolio towards classified and short-term research and development and away from its traditional support of unclassified longer-term R&D.

The Committee's analysis of agency investments found that the Federal government's historical focus on fundamental, unclassified R&D has changed in ways that place our long-term physical and economic security at risk.

Major support for cyber security research and development programs within the intelligence agencies is provided by the National Security Agency (NSA) and the Advanced Research and Development Activity (ARDA). NSA cyber security research – what the agency terms information assurance – is supported by its Information Assurance Research Group (R2). NSA allocates approximately $50 million to this work, with roughly 20 percent directed to fundamental research. Academic research accounts for only about six percent ($3 million), a level much reduced from prior years. While the majority of this research is unclassified, it is largely short-term.

Created by the intelligence community, ARDA supports the development of technologies to improve this community's information systems and networks. ARDA's cyber security research amounts to about $17 million, one third of which supports academic research and is mostly unclassified. However, ARDA typically classifies the results of this research once it is mature enough to incorporate into tools for the intelligence community.

The Department of Energy also invests in cyber security R&D, with virtually all of its work directed towards short-term and/or military and

[9] The data supplied to the PITAC by the Federal government indicate that the FY 2004 DARPA investment in cyber security is between $40 million and $150 million.

intelligence applications. This work is conducted principally at its national laboratories.

Federal Investments in Civilian Cyber Security R&D

Agencies supporting R&D that is not focused on military or intelligence applications – "civilian" research in this report – play a key role in the evolution of the Nation's IT infrastructure, including cyber security. These agencies include the National Science Foundation (NSF), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Department of Justice (DOJ).

NSF has the only substantial Federal civilian cyber security research program, an activity it has supported for many years. The majority of the work is undertaken at academic institutions and all of it is unclassified. Much of the research is considered fundamental, but the PITAC has noted a subtle change toward shorter-term activities.

In FY 2004, the agency's funding for cyber security programmatic activities totaled $76 million, of which support for research projects was approximately $58 million. The cornerstone of NSF's cyber security research activities is its Cyber Trust program; established in FY 2004, the program supports both individual cyber security researchers and research centers at academic institutions.

DHS plays a dual role, including both operational responsibilities – such as securing the Nation's borders, property, economy, and critical infrastructure – and R&D activities. R&D efforts are aimed at countering threats to the homeland by making evolutionary improvements to current capabilities and by developing revolutionary new capabilities. The varied and complex mission of the agency's Science and Technology Directorate, where its Cyber Security R&D program resides, includes responsibility for developing technologies to combat weapons of mass destruction such as radiological, nuclear, chemical, and biological threats. Most of DHS's approximately $1-billion science and technology budget is directed towards research, development, and demonstration projects in technologies to counter these threats. The Cyber Security R&D program was funded at only $18 million in FY 2004. DHS's cyber security R&D activities are largely unclassified and short-term (only about $1.5 million is

NSF has the only substantial Federal program in civilian cyber security research.

dedicated to long-term research), and some work is funded in partnership with NSF.

NIST's mission involves the development of measurements and standards – activities that play a key role in facilitating technology transfer – and its role in cyber security is focused on this type of work. NIST's FY 2004 budget for cyber security was $9.7 million. In the recently approved FY 2005 budget, cyber security funding for NIST's Computer Security Division was increased by $10 million. NIST also receives some funding from Federal agencies such as DHS and has partnered with others such as NSA. The Institute has historically collaborated closely with industry and has been increasing its involvement with academia. NIST's cyber security research program is primarily short-term in focus.

The DOJ's National Institute of Justice (NIJ) has a $7-million budget aimed at fighting electronic crime.

The Relationship Between Military/Intelligence and Civilian Cyber Space

Historically, the military and intelligence communities have derived enormous benefit from research funds invested in the civilian sector, primarily via strong support of long-term academic research by DARPA and NSA. However, the shift within both agencies towards support for short-term, classified research, and the concomitant reduction in support for the civilian research community, is leading to the erosion of that community's strength. Because many of the ideas, solutions, and talent in cyber security have traditionally come from the civilian research community, both the civilian and military sectors stand to lose from this new trend – an issue that the military and intelligence agencies themselves recognize. However, those agencies do not appear inclined to shift away from their current, more short-term mission-focused approach, and while the gap in support for the civilian cyber security R&D community could in theory be filled by other agencies, to date it has not.

The military and intelligence communities have derived enormous benefit from research funds invested in the civilian sector.

The Department of Defense's Global Information Grid (GIG), one of the most ambitious IT projects ever undertaken by the Federal government, illustrates the negative impacts of reduced R&D in civilian cyber security. To

improve U.S. military communications, the Pentagon plans to deploy the GIG, a multilayered network to link weapons, intelligence, and military personnel for "network-enhanced" warfare. While the cost of developing and deploying the GIG is not a matter of public record, a recent GAO report estimates that it will cost at least $21 billion through 2010, with significant additional expenditures beyond that date.[10]

The Defense Department intends the most sensitive portions of the GIG to be self-contained, reducing the military's potential exposure to the insecurities associated with the public IT infrastructure. However, some less sensitive portions of the GIG are expected to connect to the Internet, at least part of the time. Vulnerabilities are introduced whenever highly sensitive defense networks and civilian networks intersect, giving both communities a significant stake in cooperating to improve the security of the civilian IT infrastructure. Also, economic realities dictate that today's military networks and tomorrow's GIG use civilian commercial hardware and software, exposing those networks to the security vulnerabilities of such products. Thus, the success of the GIG as a secure IT infrastructure of the future – and the near-term success of today's military networks – depends in part on improvements in the security of the civilian IT infrastructure. Yet because the civilian R&D community has access only to the results of unclassified research, reduced support for this community will have a harmful impact on its ability to generate the fundamental discoveries upon which future generations of security products and practices will be based.

> The Committee's examination revealed pronounced shifts in favor of classifying military/intelligence cyber security R&D and in favor of short-term research.

An Assessment of Current Federal Efforts

The Committee's examination of the Federal cyber security R&D portfolio has revealed two disturbing trends: 1) a pronounced shift in favor of classifying military and intelligence R&D, rendering it unavailable to the civilian sector; and 2) an equally pronounced shift in both the military/intelligence and civilian sectors favoring short-term research over long-term fundamental research. These trends should concern policymakers because they threaten to constrict the pipeline of fundamental cyber security research that, as outlined in the previous chapter, is vital to securing the Nation's IT infrastructure.

---

10 http://www.gao.gov/new.items/d04858.pdf

If research in the civilian sector is allowed to stagnate – the likely scenario if current trends are allowed to continue – the security of the IT infrastructure upon which our Nation depends will erode further. Because any interconnected system is open to attack via its weakest link, even the Nation's military systems, which are expected to continue to be linked to civilian systems, will continue to be vulnerable. Yet of the agencies providing major support for cyber security R&D, only NSF, NIST, and to some extent DHS operate primarily in the civilian sector. Of these, only NSF provides significant support for fundamental research in civilian cyber security.

These trends should concern policymakers because they threaten to constrict the pipeline of fundamental research that is vital to securing the Nation's IT infrastructure.

Just as alarming is the increased emphasis in all agencies on funding short-term R&D to address immediate mission requirements. The Committee's analysis shows that funding for long-term fundamental research – a necessary precursor to developing leading edge solutions to more complex problems – has significantly fallen behind. In total, the Federal investment in fundamental research in civilian cyber security is a small fraction[11] of the overall Federal investment in cyber security R&D.

The PITAC believes that the Federal budget for fundamental research in civilian cyber security must be dramatically increased or the Nation's security and technological edge will be seriously jeopardized. The next chapter provides PITAC's recommendations for addressing this and related issues.

[11] After substantial and lengthy efforts to determine specific budget numbers, the PITAC estimates that this fraction is between 10 percent and 25 percent.

4 Findings and Recommendations

A Crisis of Prioritization

The information technology (IT) infrastructure of the United States, which is now vital for communication, commerce, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices. The PITAC finds that the Federal government needs to fundamentally improve its approach to cyber security to fulfill its responsibilities in this regard.

The PITAC finds that the Federal government needs to fundamentally improve its approach to cyber security.

Finding 1

The Federal R&D budget provides inadequate funding for fundamental research in civilian cyber security.

Recommendation 1

The NSF budget for fundamental research in civilian cyber security should be increased by $90 million annually. Funding for fundamental research in civilian cyber security should also be substantially increased at other agencies, most notably DHS and DARPA. Funding should be allocated so that at least the ten specific areas listed in the "Cyber Security Research Priorities" section of this chapter are appropriately addressed. Further increases in funding may be necessary depending on the Nation's future cyber security posture.

Discussion

The Snare of Short-term Fixes

Most private-sector cyber security funding today addresses immediate needs, such as augmenting existing defenses and installing patches in poorly designed or defective systems. Such needs have a legitimate and important claim on budget resources. However, addressing these needs is akin to plugging holes in a dike.

Federal cyber security R&D also has a short-term focus. As discussed in Chapter 3, many agencies expect to benefit within several years from their recent cyber security R&D investments. Insufficient long-term cyber security fundamental research today means that we will not be prepared for tomorrow's vulnerabilities and that we are not designing intrinsically more secure systems for the future.

The October 2001 Congressional testimony of Wm. A. Wulf, President of the National Academy of Engineering and a computer systems researcher, is as true today as it was then:

> We have virtually no research base on which to build truly secure systems… When funds are scarce, researchers become very conservative and bold challenges to the conventional wisdom are not likely to pass peer review. As a result, incrementalism has become the norm.[12]

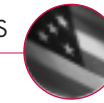
Today's urgent problems require that we continue to address immediate needs and conduct short-term research. However, significant progress in cyber security cannot be achieved as long as the focus is only reactive. Longer-range fundamental research in cyber security needs to be substantially strengthened to make future cyber security efforts proactive instead.

The Importance of Civilian Cyber Security Research

"Civilian" cyber security R&D refers to unclassified R&D associated with computing systems, networks, and software used by civilian Federal agencies, universities, corporations, and the population at large. One beneficiary of the results of research in civilian cyber security is the vast IT marketplace, which includes the commercial Internet and networks connected to it, as well as most private computing systems. Less well known is the key role civilian research plays in homeland and national security; fundamental research in civilian cyber security lays the foundation upon which their systems are built. This includes, for example, the systems, networks, and software that control key infrastructure for utilities, that support the transportation and financial sectors, and that underlie military networks. Thus, unclassified research in civilian cyber security plays an important and fundamental role across the Nation's entire cyber security portfolio.

Civilian research is distinct from research targeted to military and intelligence applications, which is often classified. Classified research is usually undertaken when its public disclosure could damage national security (such as by disclosing U.S. intelligence about adversary capabilities or revealing our

[12] http://www.house.gov/science/hearings/full/oct10/wulf.htm



military's information warfare capabilities). Thus, there are good reasons to pursue classified research, but there are also disadvantages if it is done at the expense of unclassified research. For example, the results of classified research often cannot be used commercially, because to do so would subject their inner workings to public scrutiny. Therefore, classified cyber security research largely cannot be applied to the general-purpose cyber security marketplace, and it cannot have a direct impact on the commercial Internet and its underlying technologies or on the IT infrastructure broadly, which together underpin much of the Nation's critical infrastructure. By contrast, unclassified research in civilian cyber security often benefits classified systems, because rarely is a fundamental security problem faced only in the classified world.

Classified cyber security research largely cannot be applied to the civilian cyber security marketplace.

Moreover, funding for classified cyber security research is not as effective as funding for unclassified research in increasing the number of professionals who are knowledgeable in cyber security, a critical problem identified in Finding 2 (page 30) of this report. Finally, public policy review and oversight of classified research are difficult at best, which means that research dollars may not be as effectively spent as with unclassified research.

Research Directions

As suggested by Dr. Wulf's testimony, today there are many fundamental questions about cyber security that cannot be answered satisfactorily:

- How can we build complex software-intensive systems that are secure and reliable when first deployed?
- How can we build large, distributed systems that can continue to operate reliably during hostile or natural disturbances?
- How can we verify that software obtained from a third party correctly implements stated functionality, and only that functionality?
- How can we guarantee the privacy of an individual's identity, information, or lawful transactions when stored in distributed systems or transmitted over networks?
- How can we build systems that authenticate the identities of large numbers of users in many organizations and locations?

- How can we easily determine the origin of a message transmitted over the Internet?
- How can we automatically determine whether a message transmitted over the Internet is malicious or benign?

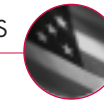
The Committee analyzed more than 30 reports on cyber security R&D (see Appendix C) to identify 10 priority areas for funding (see "Cyber Security Research Priorities," beginning on page 37). These areas are of paramount importance. Without significant advances in research in these areas, the Nation will not be able to secure its IT infrastructure. Some may view this list as overly broad in terms of setting funding priorities, while others will find omissions they consider critical. The Committee believes the list strikes a balance between these viewpoints. Cyber security is a complex and multifaceted problem. There is no silver bullet.

Federal Cyber Security R&D Funding Programs

The National Science Foundation (NSF), with its key role in supporting fundamental research across the entire scientific and engineering enterprise, is the primary funding agency for fundamental research in civilian cyber security. The Committee believes that the cyber security research investments of NSF's Computer and Information Science and Engineering (CISE) Directorate, and its Cyber Trust program in particular, which account for most of the Federal funding for fundamental research in civilian cyber security, are seriously under-funded relative to the need for cyber security research for the Nation. In FY 2004, the Cyber Trust program received 390 research proposals and made 32 awards totaling $31 million. This success rate of 8 percent of the proposals (and 6 percent of requested funds) is a factor of three lower than the NSF-wide numbers. In scientific peer review, at least 25 percent of the proposals were judged worthy of support. Further, the majority of the proposals supported were funded at levels significantly below those requested.

Cyber security is a complex and multifaceted problem. There is no silver bullet.

The Cyber Trust program's experience suggests that a quadrupling of its budget could be employed on high-quality research that would lay the foundation for critical improvements in the Nation's cyber security. In dollar



terms, this increase would add approximately $90 million in new funding to the NSF budget for fundamental research in civilian cyber security.

The PITAC estimates between 10 percent and 25 percent of FY 2004 Federal support for cyber security R&D was devoted to fundamental research in civilian cyber security. Given the central role that civilian cyber security plays across the Nation's entire critical infrastructure, the Committee believes that the funding for civilian research should be increased so that it is a much larger fraction of the overall cyber security research budget.

Funding for civilian research should be increased so that it is a much larger fraction of the overall cyber security research budget.

While NSF should continue to be the major funding agency for civilian cyber security research, the Committee suggests that NSF should not be the entire focus of increased investment in fundamental research in civilian cyber security. Different agencies provide different motivations for fundamental research, thus increasing the opportunities to apply the research to their missions and more generally.

The Committee believes that both DARPA and DHS should increase their support of fundamental research in civilian cyber security. Increased support would benefit each agency (as DARPA has experienced in the past) as well as the Nation as a whole.

PITAC recommends that the increase in the NSF CISE budget for civilian cyber security fundamental research not be funded at the expense of other parts of the CISE Directorate. The proposal success rate for CISE is 16 percent (14 percent for research grants), which is already only two-thirds of the NSF-wide average. Significant shifts of funding within CISE towards cyber security would exacerbate the strain on these other programs without addressing the existing disparity between CISE and other directorates. Moreover, much work in "other" CISE areas is beneficial to cyber security and thus reductions in those other areas would be counterproductive.[13]

[13] Some examples: Theoretical computer science underpins much encryption research, both in identifying weaknesses and in advancing the state of the art. Algorithms research helps ensure that protocols designed for security can be efficiently implemented. Programming language research can help address security at a higher level of abstraction and can add functionalities such as security assurances to software. Software engineering can help eliminate software bugs that are often exploited as security holes. And new computer architectures might enforce protection faster and at finer granularity.

Finally, Federal program managers must not be penalized for some level of "failures." Fundamental research is conducted with long time horizons and moderate to high risk for payoff. If the incentive structures within Federal grant-making agencies encourage failure avoidance, then research that favors incremental work – grants that are likely to yield definite, projected results – will become the norm. However, many expert evaluations of cyber security research challenges make the case that incremental work is unlikely to lead to solutions for some of the most difficult problems.[14]

Finding 2

The Nation's cyber security research community is too small to adequately support the cyber security research and education programs necessary to protect the United States.

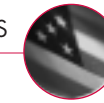
Recommendation 2

The Federal government should intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade. In particular, the Federal government should increase and stabilize the funding for fundamental research in civilian cyber security, and should support programs that enable researchers to move into cyber security research from other fields.

Discussion

Cyber security has been the focus of a small segment of the computer science and engineering research community. In the testimony cited above, Dr. Wulf noted that the Nation has "only a tiny cadre of academic, long-term, basic researchers who are thinking deeply about ... problems [in cyber security]." The Committee concurs with this assessment and estimates that U.S. academic institutions employ fewer than 250 active cyber security or cyber assurance specialists, many of whom lack either formal training or extensive professional experience in the field.

[14] For example, see the Computing Research Association's Information Security Grand Challenges at http://www.cra.org/grand.challenges.



Consequences of the existing community's small size include limitations on the amount of research that can be undertaken over all and on the number of research topics that can be investigated effectively, because productive work in a topic commonly requires a critical mass of researchers. The supporting infrastructure for research – such as technical conferences and journals – is also less developed for such small research communities. Finally, the community's small size prevents it from preparing larger numbers of bachelor's and master's candidates to work in the profession. This disconnect exists even as demand for cyber security practitioners in the United States grows.

The Federal government should intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities.

Recommendations 1 and 2 go hand-in-hand. To strengthen and enlarge the cyber security fundamental research community, the Federal government should:

- *Increase Federal funding for cyber security fundamental research.* Substantially increasing funding levels, as in Recommendation 1, is essential to building a larger cyber security fundamental research community.
- *Provide stable Federal funding for cyber security fundamental research.* Stable funding levels – an issue separate from the absolute levels of funding – are critical for achieving growth in a field, because those who are interested in entering the field know that they can have a viable future in that field.
- *Support programs that enable researchers to move into cyber security research from other fields.* Researchers attempting to change fields need funding to pursue new lines of work but face hurdles because they have no track record in the new field. Sabbaticals and similar programs would enable prospective cyber security researchers to gain knowledge and experience, thereby enabling them to contribute to the field more quickly.
- *Emphasize unclassified cyber security research.* The vast majority of the Nation's academic researchers do not hold the security clearances needed to undertake

classified work. Further, many research universities regard classified research as incompatible with their role as producers of knowledge benefiting society as a whole.[15] The trend towards increased classification of cyber security research has had a negative impact on developing the community of cyber security fundamental researchers in universities and should be reversed.

Nurturing a larger, more robust cyber security fundamental research community will help ensure that revolutionary new ideas – as opposed to incremental advances – are generated. The Committee believes that doubling the size of the cyber security fundamental research community by the end of the decade is possible and would help advance the Nation's cyber security efforts.

Finding 3

Current cyber security technology transfer efforts are not adequate to successfully transition Federal research investments into civilian sector best practices and products.

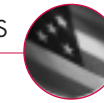
Recommendation 3

The Federal government should strengthen its cyber security technology transfer partnership with the private sector. Specifically, the Federal government should place greater emphasis on the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated; jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased; fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies; and encourage Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.

Discussion

Technology transfer enables the results of Federally supported R&D to be incorporated into products that are available for general use. There has been a long and successful history of Federally funded IT R&D being transferred into products and best practices that are widely adopted in the private sector. Figure 1 (see pages 16-17) highlights 19 examples of Federally sponsored fundamental research in IT that led to the creation of new billion-dollar

[15] Similar problems arise when the Federal government places restrictions on the work that foreign graduate students can perform or the courses they can take, because graduate students are an essential element of university research programs.



industries. This demonstrates the synergy that is possible when academia, industry, and government work together.

The diffusion of Federally supported IT R&D into products and practices benefits both consumers and developers:

- Consumers have benefited from faster hardware, faster networks, better software that is easier to use, and more frequent time- and labor-saving upgrades.
- IT research often results in new ideas and prototypes[16] that can rapidly be developed into new or improved commercial products. The developers of such innovations are free to carry their innovative ideas into the marketplace, benefiting all consumers.

Unlike other IT products, cyber security's benefits are measured by the absence of problems in IT systems. Because the market for these benefits has historically been small, interest is limited among both start-ups and large companies.

The Committee believes that, given the value and difficulty of technology transfer, the Federal government should support programs to transform existing and future cyber security research results into commercial products or operational best practices. Specifically, the Federal government should:

Unlike other IT products, cyber security's benefits are measured by the absence of system problems.

- Strengthen the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated.
- Jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results, especially those conducted or sponsored by the Federal government, are showcased.[17]

[16] See *Academic Careers for Experimental Computer Scientists and Engineers,* Computer Science and Telecommunications Board, National Research Council, 1994.

[17] Prior to 2001, the annual National Information Systems Security Conference, jointly sponsored by NIST and NSA, performed these functions. It was the one event that most security professionals attended. The conference featured invited speakers, presentation of the National Information Systems Security Award (generally considered the top award in the field) and the Vendor and Program awards, and a large vendor exhibition to showcase current technologies.

- Require grant proposals to describe the potential practical utility of their research results and have the coordinating body identified in Recommendation 4 collect and publish these descriptions. While fundamental research is usually undertaken without any direct transition path envisioned, cyber security research is often undertaken in the context of recognized problems, and documenting logical connections with real world problems is worthwhile.
- Establish a fund to support technology transfer efforts by researchers who have developed promising ideas or technologies. This fund could also help researchers cooperate with industry to bring products or enhancements rapidly to market.
- Establish and maintain a national database of results from Federally funded cyber security research, allowing vendors to identify ideas that can be incorporated into commercial products.
- Encourage Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.
- Encourage agency investment in technology transfer of cyber security R&D results through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (SBTT) programs of the Federal government.

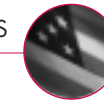
The Federal government and the private sector, by working together, can effectively and efficiently transfer Federally funded cyber security research results into commercial products and build an innovative cyber security workforce, and by doing so can help our society realize the potential benefits of this research.

Finding 4

The overall Federal cyber security R&D effort is currently unfocused and inefficient because of inadequate coordination and oversight.

Recommendation 4

The Interagency Working Group on Critical Information Infrastructure Protection should become the focal point for coordinating Federal cyber security R&D efforts. This working group should be strengthened and integrated under the Networking and Information Technology Research and Development (NITRD) Program.



Discussion

Within the Federal government, there are several coordinating bodies whose domains include various aspects of cyber security R&D. They include the:

- Interagency Working Group on Critical Information Infrastructure Protection (IWG/CIIP), which is part of the National Science and Technology Council (NSTC)
- Subcommittee on Networking and Information Technology Research and Development, which coordinates the NITRD Program and which is also part of the NSTC, and the Subcommittee's Coordinating Groups, especially the:
  - High Confidence Software and Systems Coordinating Group[18]
  - Large Scale Networking Coordinating Group[19]
- Infosec Research Council (IRC)

These coordinating bodies hold regular (often monthly) meetings, provide opportunities for agency representatives to share information, sponsor multiagency workshops, facilitate joint or coordinated funding of programs and studies, and serve as a means for academic experts and industry representatives to provide input.

Yet a key component – effective government-wide coordination of the agencies' cyber security research programs and agendas – has largely been missing. The Committee notes that the IWG/CIIP has recently begun a cross-agency effort to prioritize cyber security research areas, with the intent of developing a Federal agenda for cyber security R&D that cuts across agencies and is focused on the highest priority needs. This preliminary work is encouraging and will be critical to the efficiency and effectiveness of the Federal investment in cyber security R&D, because in the absence of such coordination, agencies understandably focus on their individual missions, rather than on the priorities of the Federal government as a whole. In addition, as the level of funding for cyber security R&D increases, greater coordination is needed to ensure that the new funding is invested wisely.

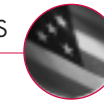
Therefore, the role of the IWG/CIIP in coordinating cyber security R&D across the Federal government should be further strengthened and integrated

[18] http://www.nitrd.gov/iwg/hcss.html
[19] http://www.nitrd.gov/iwg/lsn.html

into the NITRD Program. Objectives to be achieved by strengthened coordination include:

- Coordination of research agendas across Federal agencies, enabling the most important topics to receive priority, avoiding duplication of effort, and encouraging jointly supported work where appropriate.
- Improved communication between the Federal government and the private sector. Effective decision making about Federal cyber security R&D investments requires improved Government understanding of the activities and trends of private sector R&D and operational realities in the private sector.
- Convening forums at which participants from government, university, and industrial settings exchange information about high-level strategies and issues (for example, long-term architectural design issues) to better meet the growing cyber security challenge. Without such forums, competitive and antitrust constraints on key vendors make such dialogue difficult.
- Systematic collection of data on cyber security R&D efforts throughout the Federal government. Obtaining cyber security budget data proved a challenge for the PITAC. To track progress in cyber security R&D and give it greater visibility in budget discussions, accurate up-to-date data must be readily available.
- Tracking the intellectual progress of cyber security R&D programs and their impact on cyber security acquisition and use within the Federal government. The IWG/CIIP should issue periodic reports on the overall effectiveness of Federal cyber security R&D investments.

The cyber security R&D programs that the IWG/CIIP coordinates should be brought into the NITRD Program and the IWG/CIIP should report not only to its current parent, the NSTC's Subcommittee on Infrastructure, but also to the NITRD Subcommittee. Advances in cyber security need to be built into IT systems from the ground up, which requires cyber security R&D to be an integral part of overall IT R&D. This would be enabled by bringing IWG/CIIP under the NITRD umbrella. The IRC should continue to operate and coordinate with other Federal cyber security R&D bodies.



Cyber Security Research Priorities

The Committee analyzed more than 30 reports on cyber security R&D (listed in Appendix C) to identify 10 priority areas for increased emphasis. These areas are of paramount importance. Without significant advances in research in these areas, the Nation will not be able to secure its IT infrastructure. The ordering of the areas below does not represent a priority ranking.

1.

Authentication Technologies

Authentication schemes for networked entities such as hardware, software, data, and users are needed for a variety of purposes, including identification, authorization, and integrity checking. These schemes must be provably secure, easy to verify, supportable for use with billions of components, and rapidly executable. Methods in traditional cryptography have focused on security but may not be efficient enough for widespread use in environments where, for example, millions of data packets per second must be authenticated by a single network router. Much useful work has been done on cryptographic protocols. But the requirement that the protocols be usable in an environment such as the Internet demands the development of new protocols. Research subtopics include:

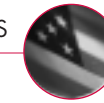
- Research on infrastructure and protocols for large-scale public key distribution and management and on other possible approaches
- Certificate and revocation management
- Integration with biometrics and physical tokens
- Decoupling authentication from identification to address privacy issues

2.

Secure Fundamental Protocols

Few of the protocols governing the Internet's operation have adequate security. For example, to misdirect traffic to an alternate site, an attacker can easily fool (or "spoof") protocols such as the Border Gateway Protocol (BGP) (which controls the paths taken by packets as they move through the Internet); and services such as the Domain Name System (DNS) (which controls the destinations of packets). Such attackers can intercept, monitor, alter, or otherwise manipulate Internet traffic, often without detection. Secure versions of the basic protocols that address threats such as denial of service, corruption, and spoofing, must be developed if the Internet is to become a reliable medium for communication. Moreover, we need to secure basic protocols against incapacitating attacks that exploit weaknesses in the protocols themselves. Research subtopics include:

- Voice over Internet Protocol (VoIP) and wireless, Web, and Virtual Private Network (VPN) security, each of whose protocols are more complex than basic Internet protocols and none of which is adequately secured
- Securing protocols even when they are shared with and executed by untrusted parties
- Tradeoffs between security and performance



3.

Secure Software Engineering and Software Assurance

Commercial software engineering today lacks the scientific underpinnings and rigorous controls needed to produce high-quality, secure products at acceptable cost. Commonly used software engineering practices permit dangerous errors, such as improper handling of buffer overflows, which enable hundreds of attack programs to compromise millions of computers every year. In the future, the Nation may face even more challenging problems as adversaries – both foreign and domestic – become increasingly sophisticated in their ability to insert malicious code into critical software. From avoiding basic programming errors to developing massive systems that remain secure even if portions of the system software are compromised, significant new research on secure software engineering is needed. Research subtopics include:

- Programming languages and systems that include fundamental security features
- Portable or reusable code that remains secure when deployed in different environments
- Technologies to capture requirement definitions and design specifications that address security issues
- Verification and validation technologies to ensure that documented requirements and specifications have been implemented
- Models for comparison and metrics to assure that required standards have been met and to enable evaluation of alternatives
- Technologies to efficiently and economically verify that computer code does not contain exploitable features that are not documented or desired

Cyber Security Research Priorities

4.

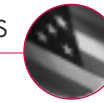
Holistic System Security

Effective security in a complex, many-layered, global infrastructure such as the Internet and its nodes requires more than the security of its component parts. Establishing sound methods for authentication, secure protocols for basic Web operations, and improved software engineering will undoubtedly become part of an evolving solution to this problem. But most importantly, researchers must recognize from the outset that an end-to-end architectural approach to the security of the whole necessarily transcends the security of the individual parts.

For example, customers assume that their online banking transactions, based on secure socket layer (SSL), are indeed secure. But by spoofing the associated underlying protocols or end-user software, a malicious party can make a user's transaction appear secured by SSL while allowing the theft of confidential data. It is also possible to compromise the security of the end computing systems, obtaining the data even though it was secure in transit.

Software usability itself is a legitimate and important research topic in cyber security. Incorrectly used software or hostile or confusing user interfaces can lead to user frustration and unauthorized workarounds that can compromise even the most robust security schemes. Research is also needed on how to make large and complex systems, where components can interact in unexpected ways, secure as a whole. Ultimately, fundamental research should address the development of entirely new, holistic security architectures including hardware, operating systems, networks, and applications. Research subtopics include:

- Building secure systems from trusted and untrusted components, and integrating new systems with legacy components
- Proactively reducing vulnerabilities
- Securing a system that is co-operated and/or co-owned by an adversary
- Comprehensively addressing the growing problem of insider threats
- Modeling and analyzing emergent failures in complex systems
- Human factors engineering, such as interfaces that promote security and user awareness of its importance
- Supporting privacy in conjunction with improved security



5.

Monitoring and Detection

Regardless of progress made in the preceding research areas, unanticipated events will still occur. When they do, tools to monitor and understand what is happening are needed to enable the proper deployment of appropriate defensive measures. The ability of current tools that monitor irregular network activity to rapidly identify the underlying cause is primitive. The current advantage that adversaries enjoy will increase as they become more knowledgeable and as the Internet becomes larger and more complex. Research subtopics include:

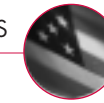
- Dynamic protection that can react when attacks are detected, possibly by increasing monitoring activities
- Global scale monitoring and intrusion detection
- Monitoring of systems to ensure that they meet declared security policies
- Better tools based on improved models that characterize "normal" behavior
- Real-time data collection, storage, mining, and analysis during a crisis
- Usable presentation interfaces that allow operators to better understand incidents in progress

6.

Mitigation and Recovery Methodologies

Secure systems must be designed to rapidly respond to unforeseen events and attacks, and recover from any resultant damage – a particularly challenging task in a system as large and complex as the Internet and its nodes. This issue has been addressed in other systems of extraordinary complexity such as the space shuttle, where a substantial investment has been made to build in maximal reliability and redundancy. No comparable effort has been invested in developing methods to make the Internet and critical computer systems reliable in the face of attacks. Research subtopics include:

- Rapid, automated discovery of outages and attacks from monitoring data
- New systems architectures that enable rapid recovery from outages and attacks
- Simplifying systems to increase the role of automated operation to reduce errors and insider attacks by human operators, especially when updating software and configurations
- Fault tolerance and graceful degradation



7.

Cyber Forensics: Catching Criminals and Deterring Criminal Activities

The rapid arrest and conviction of criminals is a primary goal of law enforcement and also serves as a deterrent. When potential criminals believe there is a strong chance that they will be caught and convicted, they are more reluctant to commit crimes.

Current capabilities to investigate cyber crime, identify perpetrators, gather and present evidence, and convict criminals are woefully inadequate. Compounding the problem, we do not really know how to deter cyber crime. Very few of the thousands of cyber criminals active today are being caught.

There is a pressing need to develop new tools and techniques to investigate cyber crimes and prosecute criminals. Robust cyber forensic methods are also needed that will prove capable of withstanding the burden of proof in court, whether employed to prosecute criminals or exonerate the innocent. Research subtopics include:

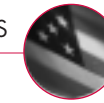
- Identifying the origin of cyber attacks, including traceback of network traffic
- Identifying attackers based on their behavior
- Collecting evidence in uncooperative network environments
- Tracing stolen information used in the growing traffic in fraud, identity theft, and intellectual property theft, including tools and protocols for recovering trace evidence from volatile and incompletely-erased computing media, disks, cell phones, PDAs, and embedded systems
- Tools and protocols to search massive data stores for specific information and indicators, possibly while the data stores are in use
- Fundamental research to develop forensic-friendly system architectures that are more amenable to investigation when incidents occur

8.

Modeling and Testbeds for New Technologies

One of the barriers to the rapid development of new cyber security products is the paucity of realistic models and testbeds available for exercising the latest technologies in a real-world environment. Some Internet modeling research has been conducted, but it has been rudimentary and has had little impact in practice. The problem is challenging because of the Internet's scale and complexity. Additionally, existing data on the Internet's workings are limited and typically confidential. Some Federal programs have been established recently, but a significantly larger and more sophisticated effort is needed if useful models and testbeds are ever to become a reality. Research subtopics include:

- System simulation environments
- Validating simulations involving millions of nodes
- Gathering and synthesizing very large amounts of data
- Designing a testbed that preserves the confidentiality of data



9.

Metrics, Benchmarks, and Best Practices

Some scientific fields have established universally acknowledged metrics and benchmarks to help evaluate new technologies or products. However, there has been relatively little research focused on developing metrics, benchmarks, and best practices for cyber security. Where benchmarks or certification criteria exist, they are typically antiquated, expensive, and even counter-productive to improving security. Without universally accepted cyber security metrics, separating promising developments from dead-end approaches will prove difficult. This, in turn, will significantly increase costs and delay time to market when transferring such technologies into the product cycle. Research subtopics include:

- Developing security metrics and benchmarks
- Economic impact assessment and risk analysis, including objective measures of risk, risk reduction, and cost of defense
- Automated tools to assess compliance and/or risk
- Tools to assess vulnerability, including source code scanning
- Discovering and documenting best practices, including auditing procedures and configuration and patch management

10.

Non-Technology Issues That Can Compromise Cyber Security

A number of non-technological factors – psychological, societal, institutional, legal, and economic – can compromise cyber security in ways that network and software engineering alone cannot address. Technology deployments that fail to address these factors can aggravate problems they are intended to solve. Cyber security research that reaches beyond technology and into these other realms is needed. Research on human and organizational aspects of IT infrastructures can be used to explore solutions that factor in human behavior. Research subtopics include:

- Strategies to change the widely held perception that greater networked security is not worth the cost to individuals and corporations – a perception that actively discourages needed software development in this area
- Ways to enhance the perceived value of privacy protection and trust in the IT infrastructure, with implications for risk management and risk analysis
- An examination of how people interact with the IT infrastructure, with a focus on ethics, culture, behavior, and other factors that can lead to non-technology security lapses
- Studies of sociological and behavioral phenomena that may lead people to commit acts of cyber crime
- Consideration of international laws and standards and the impact of both on cyber security technologies, policies, and implementation
- The implications of network-enabled commerce including jurisdictional disputes in the related areas of taxation and payment resolution, including ways to address these issues in cyber security and networking software
- National and business security issues that arise in the creation or transfer of cyber security technologies outside of the United States

Appendix A: Charge to PITAC

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

March 2, 2004

Edward D. Lazowska, Ph.D.
Bill and Melinda Gates Chair
in Computer Science
University of Washington
Department of Computer Science
and Engineering
Box 252350
Seattle, WA 98195

Dear Dr. Lazowska:

I would like to take this opportunity both to thank you for your service as co-chair of the President's Information Technology Advisory Committee (PITAC) and to outline my expectations regarding PITAC's work on cyber security. I look forward to PITAC's engagement in this important issue.

As per Executive Order 13035, as amended, PITAC exists "to provide the National Science and Technology Council (NSTC), through the Director of the Office of Science and Technology Policy, with advice and information on high-performance computing and communications, information technology, and the Next Generation Internet." With this role in mind, I would like PITAC to address the following questions with regard to the Networking and Information Technology Research and Development (NITRD) Program, as well as other relevant Federally funded research and development programs:

1. How well is the Federal government targeting the right cyber security research areas, and how well has it balanced its priorities among cyber security research areas? In particular, how well balanced is Federally funded cyber security research between shorter-term, lower-risk research and longer-term, higher-risk research?

2. How effective have the Federal government's cyber security research programs been in terms of the successful outcomes of the research and the value of the research results?

3. How useful have the research results proven as measured by implementation to improve the security of our computing and networking environments? What modifications to research areas, development efforts, or technology transfer would improve utility and encourage broader implementation of cyber security technologies?

4 How well are current Federal research efforts and supporting institutions able to anticipate or respond to paradigm shifts or fundamental shifts in technology that can create unexpected cyber security challenges?

Based on the findings of the PITAC with regard to these questions, I request that PITAC present any recommendations you deem appropriate that would assist us in strengthening the NITRD Program or other cyber security research programs of the Federal government.

In addressing this charge, I ask that you consider what the roles of the Federal government in cyber security research should be, given that other entities are also involved in this field. I also ask that you specifically consider the balance between Federal research aimed at improving security within the current computing and network environment and Federal research aimed at fundamental advances in computing and network architectures that would improve the intrinsic security of the environment.

I request that PITAC deliver its response to this charge by December 31, 2004.

Sincerely,

John H. Marburger, III
Director

Letter also sent to: Marc R. Benioff

Appendix B: Cyber Security Subcommittee Fact-Finding Process

In addition to drawing upon its own expertise and experience, the Cyber Security Subcommittee conducted an intensive review of relevant scholarly literature and trade publications. The Subcommittee also held a series of meetings during which government leaders and private-sector experts were invited to provide input. These meetings included the following:

- April 13, 2004 PITAC meeting
- June 17, 2004 PITAC meeting
- July 29, 2004 Cyber Security Research and Development Town Hall meeting at The Government Security Expo and Conference (GOVSEC) and Cyber Security Subcommittee meeting
- November 19, 2004 PITAC meeting
- January 12, 2005 PITAC meeting

April 13, 2004 PITAC Meeting

On April 13, 2004, formal presentations by the following invited experts were given:

- Amit Yoran, Director, National Cyber Security Division, Department of Homeland Security
- Carl Landwehr, Ph.D., Program Director, National Science Foundation
- David D. Clark, Ph.D., Senior Research Scientist, Massachusetts Institute of Technology
- Anthony Tether, Ph.D., Director, Defense Advanced Research Projects Agency
- Simon Szykman, Ph.D., Director, Cyber Security R&D, Department of Homeland Security

PITAC members then discussed the issues addressed in the presentations. The public was then invited to make comments and ask questions. To view or hear these presentations or to read meeting minutes, please visit: http://www.itrd.gov/pitac/meetings/2004/20040413/agenda.html

June 17, 2004 PITAC Meeting

On June 17, 2004, a PITAC meeting was held in Arlington, Virginia, at which F. Thomson Leighton, Subcommittee Chair, provided an update on the Cyber Security Subcommittee's activities and solicited comment from PITAC members and the public.

July 29, 2004 Town Hall Meeting

On June 29, 2004, the PITAC Cyber Security Subcommittee held a Town Hall meeting at the Government Security Expo and Conference (GOVSEC) in Washington, D.C. The purpose of the Town Hall meeting was to solicit perspectives from the public on the current state of cyber security and the future measures needed to help ensure U.S. leadership in this area. Subcommittee Chair Leighton provided an introduction to PITAC and its Subcommittee on Cyber Security. This presentation can be found at: http://www.itrd.gov/pitac/meetings/2004/20040729/agenda.html

The Subcommittee presented a list of questions to focus on particular areas of interest. These questions can be found at: http://www.itrd.gov/pitac/meetings/2004/20040729/questions.pdf

The initial framing discussions were presented by the following individuals:

- Harris Miller, President, Information Technology Association of America
- Joel Birnbaum, Chairman, National Research Council/Computer Science and Telecommunications Board Committee on Improving Cybersecurity Research in the United States

July 29, 2004 Cyber Security Subcommittee Meeting

On July 29, 2004, members of the PITAC Cyber Security Subcommittee met in Arlington, Virginia. Formal presentations were given by the following experts:

- Brian Witten, Director for Strategic Technologies, The Sytex Group
- John Pescatore, Vice President of Intelligence and Distinguished Analyst, Gartner Research
- André van Tilborg, Ph.D., Director, Information Systems, Office of the Director of Defense Research and Engineering
- Douglas Maughan, Ph.D., Program Manager, Homeland Security Advanced Research Projects Agency
- Robert Meushaw, Technical Director, National Security Agency

- Richard Brackney, Thrust Manager, Advanced Research and Development Activity
- Edward Roback, Chief, Computer Security Division, National Institute of Standards and Technology
- Martin Novak, Program Manager, National Institute of Justice
- John Morgan, Ph.D., Assistant Director, National Institute of Justice

November 19, 2004 PITAC Meeting

On November 19, 2004, Subcommittee Chair Leighton presented the draft findings and recommendations at a PITAC meeting in Washington, D.C. PITAC members provided guidance and specific inputs to the Subcommittee for use in drafting the report. Members of the public also provided comments. The Leighton presentation can be found at:
http://www.itrd.gov/pitac/meetings/2004/20041119/agenda.html

January 12, 2005 PITAC Meeting

On January 12, 2005, Subcommittee Chair Leighton presented the draft report at a PITAC meeting in Arlington, Virginia. After receiving public comments, the PITAC discussed the draft report and approved it for publication. The Leighton presentation can be found on the PITAC Web site:
http://www.itrd.gov/pitac/meetings/2005/20050112/agenda.html

Agency Information

A number of agencies provided written information about their cyber security R&D investments in response to a formal request from PITAC. Senior officials from several agencies participated in teleconferences with PITAC and Subcommittee leadership to provide further insight into agency policies and practices. The Committee also conducted a detailed review of some 1,500 Federally funded projects related to cyber security R&D in an effort to inform the development of its findings and recommendations.

Additional Comments

In addition, the PITAC studied written input and comments contributed by concerned individuals and organizations. The PITAC took this input under consideration in the process of drafting and revising this report.

Appendix C: Selected Major Reports on Cyber Security Research and Development

Internet Architecture Board (IAB) Concerns and Recommendations Regarding Internet Research and Evolution. Request for Comments (RFC) 3869. ftp://ftp.rfc-editor.org/in-notes/rfc3869.txt August 2004.

NIAP Certification: Proposals by CSIA for Strengthening Security Certification. https://www.csialliance.org/news/press/pr080504.pdf July 2004.

Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Research and Development Agenda. Institute for Security Technology Studies, Dartmouth College. http://www.ists.dartmouth.edu/TAG/randd.htm June 2004.

Cybersecurity for Critical Infrastructure Protection. Technology Assessment, GAO-04-321. http://www.gao.gov/cgi-bin/getrpt?GAO-04-321 and http://www.gao.gov/highlights/d04321high.pdf May 2004.

Accelerating Trustworthy Internetworking Workshop – Conference Report. Atlanta, Georgia. http://gtisc.gatech.edu/ati2004/ATI_Report_FINAL_4-25-04.pdf April 2004.

Best Practices for Government to Enhance the Security of National Critical Infrastructures. National Infrastructure Advisory Council. http://www.dhs.gov/interweb/assetlibrary/NIAC_BestPracticesSecurityInfrastructures_0404.pdf April 2004.

Information Security Governance: A Call to Action. Corporate Governance Task Force. http://www.cyberpartnership.org/InfoSecGov4_04.pdf April 2004.

Department of Defense Software Assurance Initiative. Appendix G: Software Assurance Research and Development. 2004.

Grand Research Challenges in Information Security and Assurance. Computing Research Association. http://www.cra.org/Activities/grand.challenges/security/grayslides.pdf November 2003.

Security at Line Speed: Report of a Workshop. Chicago, Illinois. http://apps.internet2.edu/sals/files/20031108-wr-sals-v1.1.pdf November 2003.

Biometric Research Agenda: Report of the NSF Workshop. Morgantown, West Virginia. http://www.wvu.edu/~bknc/BiometricResearchAgenda.pdf April/May 2003.

National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop. Atlanta, Georgia. http://www.ncs.gov/nstac/rd/nstac_03_bos.html March 2003.

Workshop on Scalable Cyber-Security Challenges in Large-Scale Networks: Deployment Obstacles. Large Scale Networking Coordinating Group, NITRD. Landsdowne, Virginia. http://www.cs.yale.edu/homes/jf/LSN-report.pdf March 2003.

National Strategy to Secure Cyberspace. The White House. http://www.whitehouse.gov/pcipb/ February 2003.

Cyber Security Research and Development Agenda. I3P, Dartmouth College. http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf January 2003.

Critical Information Infrastructure Protection and the Law: An Overview of Key Issues. Computer Science and Telecommunications Board, National Research Council. http://www.cstb.org/pub_ciip.html 2003.

Information Technology for Counterterrorism. Computer Science and Telecommunications Board, National Research Council. http://www7.nationalacademies.org/cstb/pub_counterterrorism.html 2003.

The Internet Under Crisis Conditions: Learning from September 11. Computer Science and Telecommunications Board, National Research Council. http://www7.nationalacademies.org/cstb/pub_internet911.html 2003

Who Goes There? Authentication Through the Lens of Privacy. Computer Science and Telecommunications Board, National Research Council. http://www7.nationalacademies.org/cstb/pub_authentication.html 2003.

IDs-Not That Easy. Questions About Nationwide Identity Systems. Computer Science and Telecommunications Board, National Research Council. http://www7.nationalacademies.org/cstb/pub_nationwideidentity.html 2002.

Robust Cyber Defense. Study commissioned for DARPA ITO. Slides available at: http://www.cs.cornell.edu/fbs/darpa.RobustCyberDefense.ppt Fall 2001.

Electronic Crime Needs Assessment for State and Local Law Enforcement. National Institute of Justice Research Report. http://www.ncjrs.org/pdffiles1/nij/186276.pdf March 2001.

High Confidence Software and Systems Research Needs. High Confidence Software and Systems Coordinating Group, Interagency Working Group on Information Technology Research and Development. http://www.nitrd.gov/pubs/hcss-research.pdf January 2001.

Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers. Computer Science and Telecommunications Board, National Research Council. http://www7.nationalacademies.org/cstb/pub_embedded.html 2001.

National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop. Tulsa, Oklahoma. http://www.ncs.gov/nstac/reports/2001/ R&D_Exchange2000Proceedings.htm September 2000.

National Security Telecommunications Advisory Committee, Protecting Systems Task Force Report on Enhancing the Nation's Security Efforts. http://www.ncs.gov/nstac/reports/2001/R&D_Exchange2000Proceedings.htm May 2000.

National Security Telecommunications Advisory Committee, Information Sharing/Critical Infrastructure Protection Task Force Report. http://www.ncs.gov/nstac/reports/2001/R&D_Exchange2000Proceedings.htm May 2000.

Hard Problems List. Infosec Research Council. September 1999 (and draft revision as of September 2004)

Information Technology Research for Crisis Management. Computer Science and Telecommunications Board, National Research Council. http://www7.nationalacademies.org/cstb/pub_crisismanagement.html 1999.

Trust in Cyberspace. Computer Science and Telecommunications Board, National Research Council. http://www7.nationalacademies.org/cstb/pub trust.html 1999.

National Security Telecommunications Advisory Committee, Research and Development Exchange Workshop. West Lafayette, Indiana. http://www.ncs.gov/nstac/reports/1998/R&DExchange.pdf October 1998

Critical Foundations: Protecting America's Infrastructures. President's Commission on Critical Infrastructure Protection. http://www.timeusa.com/CIAO/resource/pccip/PCCIP_Report.pdf October 1997.

Appendix D: Acronyms

ARDA
Advanced Research and Development Activity

ARPANET
Advanced Research Projects Agency Network

ATM
Automated teller machine

BGP
Border Gateway Protocol

BSD
Berkeley Software Distribution

CDMA
Code Division Multiple Access

CERN
European Organization for Nuclear Research

CERT/CC
Computer Emergency Response Team Coordination Center

CIIP
Critical Information Infrastructure Protection

CISE
NSF's Computer and Information Science and Engineering Directorate

CM
Connection Machine

CMU
Carnegie Mellon University

COTS
Commercial off-the-shelf

CTSS
Compatible Time Sharing System

DARPA
Defense Advanced Research Projects Agency

DDoS
Distributed denial of service

DEC
Digital Equipment Corporation

DECnet
Digital Equipment Corporation network

DHS
Department of Homeland Security

DNS
Domain Name System

DOE
Department of Energy

DOJ
Department of Justice

DoS
Denial of service

E&S
Evans and Sutherland

FY
Fiscal year

GAO
Government Accountability Office

GIG
Global Information Grid

GM
General Motors

HP
Hewlett-Packard

HPC
High Performance Computing

IBM
International Business Machines

ICL
ICL High Performance Systems, U.K.

IRC
Infosec Research Council

IRI
Information Resources Incorporated, U.K.

IT
Information technology

IT R&D
Information Technology Research and Development

IWG
Interagency Working Group

LAN
Local area network

MIT
Massachusetts Institute of Technology

MOSIS
Metal oxide semiconductor implementation service

NIJ
National Institute of Justice

NIPRNet
Non-secure Internet Protocol Router Network

NIST
National Institute of Standards and Technology

NITRD
Networking and Information Technology Research and Development

NSA
National Security Agency

NSF
National Science Foundation

NSFNET
National Science Foundation Network

NSTC
National Science and Technology Council

PARC
Palo Alto Research Center

PDA
Personal digital assistant

PITAC
President's Information Technology Advisory Committee

R&D
Research and development

RAID
Redundant array of independent disks

RISC
Reduced instruction set computer

SBIR
Small Business Innovation Research

SBTT
Small Business Technology Transfer

SCADA
Supervisory control and data acquisition

SDS
Scientific Data Systems

SGI
Silicon Graphics Incorporated

SRI
Stanford Research Institute

SSL
Secure Socket Layer

TCP/IP
Transmission Control Protocol/Internet Protocol

UCLA
University of California at Los Angeles

VLSI
Very-large-scale integration

VMS
Virtual Memory System

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

Acknowledgements

The PITAC co-chairs would like to acknowledge the members of the Committee's Subcommittee on Cyber Security for their contributions. In particular, Subcommittee Chair F. Thomson Leighton deserves special recognition for his strong leadership and tireless efforts in bringing this report to completion.

The PITAC thanks the staff of the National Coordination Office for Information Technology Research and Development for their contributions in supporting and documenting meetings; drafting sections of this report; critiquing, editing, and proofreading the numerous drafts; and contributing to the substantive dialogue that led to this final report. Staff members Alan S. Inouye, Martha Matzke, and Terry L. Ponick provided primary support in the development of this report, under the guidance and oversight of David B. Nelson and Sally E. Howe. Staff members Nekeia Bell, Elizabeth Kirk, Grant Miller, Virginia Moore, Karen Skeete, and Diane Theiss provided technical and administrative support for the Subcommittee's work.

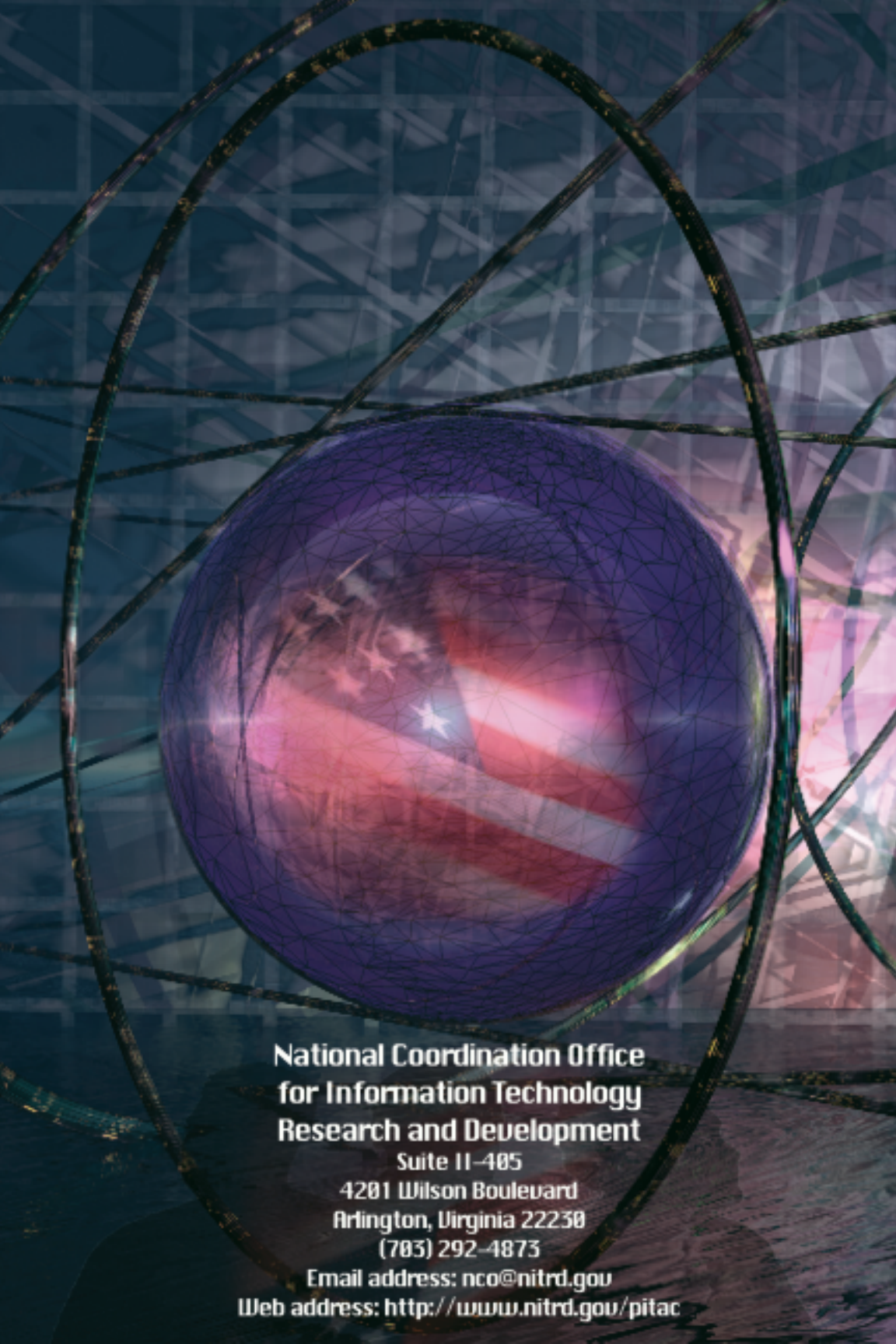
NCO interns Nils Janson and Stephanie Showell contributed to the Subcommittee's research effort as part of their NSF-supported undergraduate internships in the Federal Cyber Corps. The Corps is part of the Federal Cyber Service: Scholarship for Service program, which seeks to increase the number of qualified students entering the fields of information assurance and computer security.

The PITAC appreciates the technical information and thoughtful advice provided by Sharon L. Hays and Charles H. Romine of the Office of Science and Technology Policy. Their inputs stimulated Subcommittee discussions and led to improvements in the text.

Finally, the PITAC acknowledges Wade H. Baker, James Caras, Paul Robertson, and John Voeller for their specialized technical support of the Subcommittee's work.

Copyright

This is a work of the U.S. government and is in the public domain. It may be freely distributed and copied, but it is requested that the National Coordination Office for Information Technology Research and Development (NCO/IT R&D) be acknowledged.



National Coordination Office
for Information Technology
Research and Development
Suite II-405
4201 Wilson Boulevard
Arlington, Virginia 22230
(703) 292-4873
Email address: nco@nitrd.gov
Web address: http://www.nitrd.gov/pitac