

SECURITY IN CYBERSPACE

Y 4. G 74/9: S. HRG. 104-701

Security in Cyberspace, S. Hrg. 104...

HEARINGS

BEFORE THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS OF THE COMMITTEE ON

GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FOURTH CONGRESS

SECOND SESSION

MAY 22, JUNE 5, 25, AND JULY 16, 1996

Printed for the use of the Committee on Governmental Affairs



SECURITY IN CYBERSPACE

HEARINGS

BEFORE THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE ONE HUNDRED FOURTH CONGRESS SECOND SESSION

MAY 22, JUNE 5, 25, AND JULY 16, 1996

Printed for the use of the Committee on Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE WASHINGTON : 1996

For sale by the U.S. Government Printing Office Superintendent of Documents, Congressional Sales Office, Washington, DC 20402 ISBN 0-16-053913-7

24--541 cc

COMMITTEE ON GOVERNMENTAL AFFAIRS

TED STEVENS, Alaska, Chairman

WILLIAM V. ROTH, JR., Delaware WILLIAM S. COHEN, Maine FRED THOMPSON, Tennessee THAD COCHRAN, Mississippi JOHN McCAIN, Arizona BOB SMITH, New Hampshire HANK BROWN, Colorado JOHN GLENN, Ohio SAM NUNN, Georgia CARL LEVIN, Michigan DAVID PRYOR, Arkansas JOSEPH I. LIEBERMAN, Connecticut DANIEL K. AKAKA, Hawaii BYRON L. DORGAN, North Dakota

Albert L. McDermott, Staff Director Leonard Weiss, Minority Staff Director Michal Sue Prosser, Chief Clerk

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

WILLIAM V. ROTH, JR., Delaware, Chairman

TED STEVENS, Alaska WILLIAM S. COHEN, Maine FRED THOMPSON, Tennessee THAD COCHRAN, Mississippi JOHN McCAIN, Arizona BOB SMITH, New Hampshire HANK BROWN, Colorado SAM NUNN, Georgia JOHN GLENN, Ohio CARL LEVIN, Michigan DAVID PRYOR, Arkansas JOSEPH I. LIEBERMAN, Connecticut DANIEL K. AKAKA, Hawaii BYRON L. DORGAN, North Dakota

Harold Damelin, Chief Counsel Daniel S. Gelber, Chief Counsel to the Minority Carla J. Martin, Chief Clerk Alan Edelman, Minority Counsel R. Mark Webster, Chief Investigator to the Minority

(II)

$\rm C \ O \ N \ T \ E \ N \ T \ S$

Opening statements:	Page
Senator Nunn	1, 25, 85, 139
Senator Glenn	5, 28
Senator Levin	
Senator Lieberman	
Senator Cohen	
Prepared statements:	
Senator Roth	

WITNESSES

WEDNESDAY, MAY 22 1996

Keith A. Rhodes, Technical Assistant Director, Office of the Chief Scientist, Accounting and Information Management Division, U.S. General Account-	
ing Office	7
Jack L. Brock, Jr., Director, Defense Information and Financial Management	
Systems, Accounting and Information Management Division, U.S. General	
Accounting Office	14
Jim Christy, Investigator, Permanent Subcommittee on Investigations, Com-	
mittee on Governmental Affairs, U.S. Senate	16

WEDNESDAY, JUNE 5, 1996

Daniel S. Gelber, Chief Counsel (Minority), and Jim Christy, Investigator	
(Minority), Permanent Subcommittee on Investigations, Committee on Gov-	
ernmental Affairs, U.S. Senate	32
Jack L. Brock, Jr., Director, Defense Information and Financial Management	
Systems, and Keith A. Rhodes, Technical Assistant Director, Office of the	
Chief Scientist, U.S. General Accounting Office	39
Richard Pethia, Manager, Trustworthy Systems Program and Computer	
Emergency Response Team Coordination Center, Software Engineering In-	
stitute, Carnegie Mellon University, Pittsburgh, Pennsylvania	64
Richard G. Power, Editor, Computer Security Institute, San Francisco, Cali-	
fornia	75

TUESDAY, JUNE 25, 1996

Hon. John M. Deutch, Director, Central Intelligence Agency	- 88
Roger C. Molander, National Security Research Division, RAND Corporation,	
Santa Monica, California, accompanied by Peter Wilson and Andrew	
Riddile	104
Peter G. Neumann, Author and Principal Scientist, SRI International, San	
Francisco, California	106
Robert Anderson, RAND Corporation, Santa Monica, California	111

TUESDAY, JULY 16, 1996

Hon. John Kyl, a U.S. Senator from the State of Arizona	142
Hon. Patrick J. Leahy, a U.S. Senator from the State of Vermont	144
Hon. Jamie S. Gorelick, Deputy Attorney General, U.S. Department of Jus-	
tice	150
Hon. John P. White, Deputy Secretary, U.S. Department of Defense	159

ALPHABETICAL LIST OF WITNESSES

Anderson, Robert:	
Testimony	111
Prepared statement	364

¥.	5			
		e	э.	

Page

Brock, Jack L. Jr.: Testimony	4 39
Prepared statement	
Christy, Jim:	
Testimony 1	
Prepared statement	225
Deutch, Hon. John M.:	
Testimony	88
Prepared statement	329
Gelber, Daniel S.:	
Testimony	32
Prepared statement	225
Gorelick, Jamie S.:	150
Testimony	150
Prepared statement	390
Kyl, Hon. John:	
Testimony	142
Prepared statement	380
Leahy, Hon. Patrick J.:	1.4.4
Testimony	144
Prepared statement	385
Molander, Roger C.: Testimony	104
Testimony	$104 \\ 337$
Prepared statement	331
Neumann, Peter G.:	106
Testimony	
Prepared statement	350
Pethia, Richard:	64
Testimony	306
Prepared statement	300
Power, Richard G.:	75
Testimony Prepared statement	
	024
Rhodes, Keith A.:	7
Testimony Prepared statements	
White, John P.:	1, 210
Testimony	159
Prepared statement	
I repared statement	100

APPENDIX

Prepared statements of witnesses in order of appearance	1	17'	7
---	---	-----	---

EXHIBIT LIST

* May Be Found In The Files of the Subcommittee

1. GAO Report, Information Security: Computer Attacks at Department	
of Defense Pose Increasing Risks, May 1996, GAO/AIMD-96-84	422
2. a. Statement of Richard G. Power, Editor, Computer Security Institute	
(CSI), before the Senate Permanent Subcommittee on Investigations,	
June 5, 1996 (See also http://www.gocsi.com/csi/)	*
b. Press Release of Computer Security Institute regarding results of	
1996 Computer Crime and Security Survey, May 6, 1996	*
c. Computer Security Issues & Trends, "1996 CSI/FBI Computer Crime	
and Security Survey," Spring 1996	465
d. CSI/FBI Computer Crime & Security Survey	*
e. Current and Future Danger: A CSI Primer on Computer Crime &	
Information Warfare, Richard Power, 1995	*
f. Information Warfare: A CSI Special Report, Richard Power, Fall 1995	
g. Electronic Commerce: Treasure of Sierra Madre?: A CSI Special Re-	
port, Richard Power, Spring 1996	*
h. Computer Security Issues & Trends, "CSI's 1995 Crypto Security	
Study," Fall 1995	*
i. Computer Security Issues & Trends, "CSI's 1995 Internet Security	
Survey," Fall 1995	*
3. a. Carnegie Mellon University, Computer Emergency Response Team	
(CERT) Coordination Center Statistics (See also http://www.cert.org/)	477

		rage
	b. CERT Guidelines for the Secure Operation of the Internet, November	*
	1991	*
Δ	c. CERT Site Security Handbook, July 1991 a. Statement of Peter G. Neumann, Computer Science Laboratory, SRI	
·**•	International, before the Senate Permanent Subcommittee on Inves-	
	tigations, June 25, 1996 (See also http://csi.sri.com/neumann)	*
	b. Illustrative risks to the public in the use of computer systems and	
	related technology compiled by Peter G. Neumann, SRI International	
	Computer Science Laboratory	*
	Computer Science Laboratory c. Securing the Information Infrastructure, Teresa Lunt, June 1996,	
	Communications of the ACM	*
	d. Cryptography's Role in Securing the Information Society: Overview	
	and Recommendations, Committee to Study National Cryptography	
	Policy [Peter G. Neumann, a Committee member], National Research	
	Council, May 30, 1996 prepublication copy e. Computer Related Risks, Peter G. Neumann (New York: The ACM	*
	e. Computer Related Risks, Peter G. Neumann (New York: The ACM	ىك
-	Press, 1995)	不
5.	a. Strategic Information Warfare: A New Face of War, Roger C.	*
	Molander, Andrew S. Riddile, Peter A. Wilson, RAND, 1996	-1-
	b. Outline of RAND Presentation to Senate Permanent Subcommittee on Investigations, June 25, 1996, regarding Strategic Information	
	Warfare	*
	c. Emerging Challenge: Security and Safety in Cyberspace, Richard O.	
	Hundley and Robert H. Anderson, RAND, 1996	479
	d. Outline of presentation of Richard O. Hundley and Robert H. Ander-	
	son before RAND-Ditchley Foundation Conference, April 26, 1996,	
	regarding Cyberspace Security Challenges	*
6.	Redefining Security: A Report to the Secretary of Defense and the Direc-	
	tor of Central Intelligence, Joint Security Commission, February 28,	
	1994	*
7.	a. SEALED EXHIBIT: Security Oversight Report: Audit of Unclassified	
	Mainframe Systems Security, U.S. Department of State, Office of	*
	Inspector General, January 1996	4
	b. Executive Summary, Security Oversight Report: Audit of Unclassified Mainframe Systems Security, U.S. Department of State, Office of	
	Inspector General, January 1996	490
8.	Material received from New Scotland Yard, Computer Crime Unit	*
9.	Press Release, U.S. Attorney's Office, Southern District of New York,	
	January 1, 1996, regarding U.S. v. Alexei Lachmanov	*
10.	Press Release, Department of Justice, March 29, 1996, regarding Har-	
	vard University computer wiretap case	*
11.	NASA 1995 Incident Summary Reports	494
12.	NASA, Mars Observer Loss of Signal: Special Review Board Final Re-	
10	port, November 1993 Issue Update On Information Security and Privacy in Network Environ-	*
13.	Issue Opaale On Information Security and Privacy in Network Environ-	*
14	ments, Office of Technology Assessment, U.S. Congress, June 1995 An Introduction to Computer Security: The NIST Handbook, The Na-	
1.1.	tional Institute of Standards and Technology, U.S. Department of Com-	
	merce, October 1995 (See also http://cs-www.ncsl.nist.gov/)	*
15.	Central Intelligence Agency reply to Permanent Subcommittee on Inves-	
	tigations' questions regarding computer security at CIA	*
16.	Information Week/Ernst & Young Security Survey, November 1995	*
17.	Private Sector Leadership: Policy Foundations For a National Informa-	
	tion Infrastructure (NII), U.S. Business Views on Telecommunications,	
	Information Security, Privacy and Intellectual Property United States	
10	Council For International Business, July 1994	*
18.	SEALED EXHIBIT: Interim Report of The Critical Infrastructure Work-	*
10	ing Group Letter to Senator Sam Nunn, dated June 27, 1996, from Director of	Ť
19.	Central Intelligence John Deutch, regarding the meaning of "cyber"	511
20	U.S. Department of State briefing slides, March 28, 1996, regarding	511
	information security	512
21.	Press Release, OMB, June 14, 1996, regarding attached June 5, 1996.	012
	Information Infrastructure Task Force's (IIFT) National Information	
	Infrastructure Security Issues Forum's draft report, NII Security. The	
	Federal Role	*
22.	Thesis of Matthew J. Littleton, Information Age Terrorism: Toward	
	<i>Cyberterror</i> , Naval Postgraduate School, Monterey, California, December	.1.
	1995	*

Page

23.	Press Release, Department of Justice, July 15, 1996, regarding attached Executive Order on formation of the President's Commission on Critical	
24.	Infrastructure Protection Letter to Senator Sam Nunn, dated July 16, 1996, from General Ronald	*
	R. Fogleman, regarding information infrastructure Supplemental Questions for the Record, Honorable John P. White, Dep-	515
	uty Secretary, Department of Defense	517
26.	Letter to Senator Sam Nunn, dated September 18, 1996, from D. Diane Fountaine, Chair, Industry Executive Subcommittee, NSTAC, regarding	
27	President's National Security Telecommunications Advisory Committee . GAO Report, Information Security: Opportunities for Improved OMB	520
	Oversight of Agency Practices, September 1996, GAO/AIMD-96-110 a. Crime and Crypto on the Information Superhighway, by Dr. Dorothy	*
20.	E. Denning, Georgetown University, December 13, 1994	543
	b. Protection and Defense Intrusion, by Dr. Dorothy E. Denning, Georgetown University, March 5, 1996	555
	c. Letter to Senator Patrick Leahy, dated March 14, 1996, from Dr. Dorothy E. Denning, Georgetown University, regarding encryption	
~~	legislation	*
	Statements for the Record of Barry C. Collin and Marc Steven Colen, The Institute for Security and Intelligence	*
30.	a. Statement for the Record of Dr. Ulrich Sieber, University of Würzburg, Germany, Computer Crime and Criminal Information	
	Law b. Criminal Liability for the Transfer of Data in International Computer	565
	Networks: New Challenges of the Internet, by Dr. Ulrich Sieber, Draft	
	Translation of a law review article to be published in German in Juristenzeitug 1996	*
	c. Outline of presentation of Dr. Ulrich Sieber before Rand and Ditchley Foundation Conference on Security in Cyberspace, April 26-28, 1996	*
31.	Information Warfare: Legal, Regulatory, Policy and Organizational Con- sideration for Assurance, 2nd Edition, July 4, 1996, Joint Chiefs of	
0.0	State, National Defense University	*
32.	Preparing for the 21st Century: An Appraisal of U.S. Intelligence, Report of the Commission for the Roles and Capabilities of the United States	
33.	Intelligence Community, March 1, 1996 Letter to the Honorable Sam Nunn, Ranking Minority Member, Perma-	sk:
	nent Subcommittee on Investigations, dated November 13, 1996, from Andrew Fois, Assistant Attorney General, U.S. Department of Justice,	
	regarding statistics on computer intrusion investigations and prosecu-	594
34.	tions from 1993 to present 1996 Information Systems Security Survey conducted by WarRoom Re-	
35.	search, LLC Letter to the Honorable Sam Nunn, dated October 23, 1996, from Ro-	596
	berta L. Gross, Inspector General, NASA, regarding NASA Inspector General's review of computer intrusion incidents	*
36.	Correspondence between the Permanent Subcommittee on Investiga-	
	tions and Science Applications International Corporation (SAIC), dated May 30 and June 4, 1996, regarding SAIC testimony before the Sub-	0.0-
37.	committee	605
	national Conference (April 1996), Jointly Sponsored by RAND and The Ditchley Foundations	*

Page

SECURITY IN CYBERSPACE

WEDNESDAY, MAY 22, 1996

U.S. SENATE,

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS, Washington, DC.

The Subcommittee met, pursuant to notice, at 8:32 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Sam Nunn presiding.

Present: Senators Nunn, Glenn, and Levin.

Staff Present: Daniel S. Gelber, Chief Counsel to the Minority; R. Mark Webster, Investigator to the Minority; Mary D. Robertson, Assistant Chief Clerk to the Minority; Alan Edelman, Minority Counsel; Jim Christy (AFOSI Detailee); Harold Damelin, Chief Counsel and Staff Director; Carla J. Martin, Chief Clerk; Mary A. Ailes, Staff Assistant; Ariaden Allan, Investigator; Mark Forman (Senator Roth); John Bennett (Governmental Affairs); Debbie Cohen (Senator Glenn); and Elise Bean (Senator Levin).

OPENING STATEMENT OF SENATOR NUNN

Senator NUNN. Senator Roth is not able to be here this morning. He has a conflict and he has asked me to go ahead and proceed, so we will begin our hearing this morning.

Unfortunately—and I will make this clear to all—we have had to change around our schedule today. We will have the witnesses who were going to be here this morning, some of the witnesses, come to a hearing we have in June. We have about 40 votes on the floor of the Senate today. They are going to take approximately 10 minutes each, so it would be absolutely impossible, once the votes start, to have Senators here to pay any attention to what was going on.

This is, I think, one of the most important series of hearings that we will have this year in the national security field, so we want to postpone part of this hearing this morning until we can get the full attention of the Senators. We are going to proceed for about an hour and make sure we get in the General Accounting Office report, which is enormously important.

Technology has long been an instrument of power and change. From the invention of the printing press to the advent of the Industrial Revolution to the development of nuclear weapons, technological advances have profoundly altered our society and indeed changed the course of our history.

Today, we find ourselves in the midst of one of the most farreaching technological developments of all; that is, the computer age. Virtually every aspect of our society is becoming linked to computer systems and networks, from civilian, government, and the military, to public utilities, communications, transportation, and financial systems. These links are creating vast efficiencies in the delivery of goods and services and giving people throughout the world greater access to information, ideas, and indeed to each other.

Consider that just 5 years ago the number of users on the Internet totaled 2 to 3 million. Today, that number is over 55 million worldwide and growing at a rate of 183 percent or more a year. Computer links that stretch around the world transcend national and regional boundaries. Beijing and Baltimore are within a keystroke of each other.

This morning, we were to begin a series of hearings examining the vulnerability of various aspects of the information infrastructure. Unfortunately, as I mentioned, due to an unexpected schedule of stacked votes, at least 40 of them today on the budget resolution, we are unable to convene a full hearing. The distinguished witnesses that were scheduled today, including authors and scientists Cliff Stoll, Peter Neumann and Bob Anderson, were very, very important witnesses and they will be invited to appear at our hearings in June on this subject. I did not think it was fair to them or to the Subcommittee and those interested to try to have that kind of disjointed hearing, running back and forth every 4 or 5 minutes.

Today, we will focus on the vulnerabilities of the Defense Department's computer system. Although advanced computer technology has greatly enhanced the efficiency of our armed forces, it has also brought about new vulnerabilities and challenges we are just beginning to learn about.

There are over 2 million computers that comprise the unclassified, but nevertheless sensitive information database that is absolutely critical to our national security. Over 90 percent of all Department of Defense voice and data traffic transits these networks, and the data includes sensitive research data and valuable intelligence information. Furthermore, these systems support critical defense missions related to troop movements, operational plans, procurement and weapons system maintenance, and also all the financial information.

The purpose of these hearings is to examine whether this information infrastructure is secure; if not, to the extent possible, what can be done about it. To what extent can the vital services that are supported here be disrupted? How can we be sure that the information stored on the Internet, especially data related to our national security, remains confidential, and also available?

This morning, the General Accounting Office will release its report on the vulnerabilities of the Department of Defense computer system. Its findings should get our attention and the attention of everyone in the Pentagon and all who are concerned about our national security in the country. The GAO reports statistics that the Department of Defense likely experienced as many as 250,000 attacks on their computers last year, most of which very little is known about. Not only do we have a problem with knowing about the attacks, but we have a very serious problem, as the GAO will point out, in having reports made when attacks are known about. So a large percentage of the attacks are unknown and undetected, and even those that are detected, a very large percentage of those are not properly reported.

The GAO explains how easy it is to attack Defense computer systems with hacker tools that are available to millions of Internet users worldwide. Significantly, GAO's findings show that attacks were successful 65 percent of the time and that the number of attacks is doubling each year.

Finally, the report acknowledges that the Defense Department is attempting to react to this growing threat, but points out that it lacks uniform policies for protecting computer networks, responding to incidents, and assessing risk of damage from computer attacks.

Not all the problems have to do with the ease with which computer networks are penetrated. We will learn today, and in our hearings next month, the difficulty this issue poses for government in terms of organization. Our government's traditional national security threats have been defined geographically—in large part, a foreign threat versus domestic—and the type of threat would inspire different response from the appropriate agency, whether enforcement, military, or intelligence, domestic matters almost always being handled by domestic law enforcement, foreign threats being handled with our national security apparatus.

When we move from the physical world into cyberspace, traditional divisions of responsibility and assignment of roles and missions become confusing, if not completely outdated. Is the bad actor a 16-year-old, a foreign agent, an anarchist, or a combination of all? Furthermore, the Internet exists in a borderless world. How do you ascertain the nature of a threat if you don't know the motive of your adversary? What agency is used if you can't tell until the investigation is concluded the origin of the attack, whether it is domestic or foreign? How do you decide whether you use the intelligence community or whether you use the FBI? These are very large and unanswered questions.

We will also examine a case recently investigated by the Air Force's Office of Special Investigations. The case, which occurred at Griffiss Air Force Base in New York, demonstrates the difficult challenge of investigating one of these incidents.

In our hearings next month, not only will we hear from the witnesses that were scheduled today, but we will continue to examine the vulnerabilities of our information infrastructure not just from a defense perspective, but government-wide and in the financial and public sector as well. I fear that the problems we have in defense may be only the beginning and that will find that huge portions of our commercial networks are even more vulnerable than our defense network.

Are the trillions of dollars that are electronically transferred each day secure? What about our airplanes, electrical grids, and ground transportation networks? What is private industry doing about this new challenge? What are other nations doing? What is the international cooperation in this area, particularly in terms of law enforcement? These are just a few of the questions we will be addressing. Although the information age offers great promise, and we all know that and we all know that we are not going to roll back the clock, our rush to connect must be tempered with a desire to protect. Clearly, the time to think about the security of our information infrastructure is now. Security must be embedded into not only the technology of the computer age, but the culture as well. So I hope this Subcommittee hearing will provide a forum in which to meaningfully examine these issues so we can better understand, and therefore confront these new and great challenges.

Senator Roth is not here this morning, but he has been very cooperative, he and his entire staff, in aiding us in this overall investigation.

[The prepared statement of Senator Roth follows:]

PREPARED STATEMENT OF SENATOR ROTH, CHAIRMAN

This morning, the Subcommittee will begin the first of a series of hearings on security in cyberspace. This Subcommittee has had a long tradition of investigating emerging threats to our Nation's security. Today we turn to a topic which is perhaps less tangible, but just as serious—the security of our computers.

This has been an area of concern to me and this Subcommittee for quite some time. At my direction in the early 1980's, the Subcommittee first examined computer security vulnerabilities. A few years later, I was pleased to have been involved in the effort to pass the Computer Security Act of 1987. This legislation developed guidelines and standards to promote protection of the Federal Government's unclas sified, but sensitive data. More recently, a government report on information security and privacy in computer network environments was done at my request. Over the years, we have seen a dramatic evolution in computer technology, but the basic challenge has remained the same: How do we safeguard our valuable information resources and systems.

Today, computers have become essential to the transacting of our Nation's daily business. Everything from telephones to transportation, power networks, our financial system, emergency services, and our national defense depends upon computers Together, these components, networks, and systems make up the national information infrastructure. Now, more than ever, our military and other critical government personnel rely upon these networks and systems to maintain our national security.

Computer technology has enabled the United States to become the most advanced nation in cyberspace. However, this very strength also makes us uniquely vulnerable. Someone once said, "To err is human, but to really foul things up requires a computer." Anyone of us who has ever experienced a computer problem which caused a disruption in service, whether at the automatic teller machine or at the office, has shared this frustration. Usually the disruption is only a minor inconvenience and service is restored without significant loss or damage.

But, imagine for a moment what would happen if any of the systems we depend upon every day for our communications, commerce, transportation, and our national security were compromised or attacked. This morning you will hear that this is not some futuristic doomsday scenario. Incidents involving break-ins to computer systems causing disruption of service, destruction, and alteration of data have happened and appear to be rising at a disturbing rate. And those are just the cases which have been reported to computer emergency response teams and law enforcement officials. Many other incidents go undetected and even worse, unreported, either due to fear of embarrassment on behalf of an employee, or to prevent loss of public confidence.

We have come a long way in cyberspace in a relatively short time. Only a decade ago, few people had even heard of the Internet. In 1981, there were only 215 Internet sites. Since then, this former military computer network has gone global. Today, there are millions of Internet sites which enable private citizens, corporate employees, university communities, and government users to communicate with each other. People around the world can exchange ideas and information as though they were right next door. Currently, tens of millions use the Internet and that number is said to be doubling every year. It is a system whose security is based on mutual trust and cooperation.

Unfortunately, mutual trust and cooperation are not enough to ensure that, in this increasingly interconnected world, our computer networks remain safe from unauthorized intruders. With the ever rising number of people connecting to, and "surfing" the Internet, we may soon find ourselves in perilous waters if we do not take precautions to protect our computer networks and the sensitive information they hold.

We have already witnessed an increase in intrusions. According to the Computer Emergency Response Team at Carnegie Mellon University, also known as CERT, there were fewer than 500 incidents reported in 1991. Last year, there were nearly five times as many reported incidents. Even in my home State, the University of Delaware has had its computer accounts attacked. While it was not clear whether any data was stolen, over 2,000 student and professors' passwords were compromised and had to be changed. This matter was reported to CERT and was dis covered to be part of a larger attack involving other computers around the country.

In order to stop intruders, we need to understand the nature of the threat. Information and intelligence collected from victims of computer intrusions can help both government and private industry understand who these perpetrators are; how they are breaking in; what damage they are causing; and what their motives might be. Whether a hacker is a curious teenager or a foreign spy, cyber trespassing, thievery, and tampering puts the integrity of our data and systems at risk.

As the saying goes: An ounce of prevention is worth a pound of cure. Our information infrastructure is too important to neglect. Defending our computer systems against infiltration is perhaps the most cost-effective way to deal with this problem. By identifying our vulnerabilities now in a controlled environment, we can take precautions to protect this fundamental asset before we suffer a catastrophic and expensive loss. The protection of our computer networks and the information contained in those systems should be of vital concern to all Americans.

I would like to commend my distinguished colleague Senator Nunn for his leadership in focusing on this critical security issue, and the minority staff for their investigative work on this important hearing.

Senator NUNN. I think it is one of the most important investigations that I have been involved with. We are going to have a long way to go. Senator Glenn, as Chairman and now ranking Democrat on the full Committee, has also been interested in this overall subject and has requested the GAO report along with myself and a number of other people. So we will be working closely both with Senator Glenn and Senator Roth, as well as with others.

Senator Glenn, would you like to make any opening statement?

OPENING STATEMENT OF SENATOR GLENN

Senator GLENN. Just briefly, Mr. Chairman, and thank you very much. I am glad to join Senator Nunn in today's hearing on information security. I, too, want to apologize to our witnesses and everybody else for the truncated nature of things today around here. Sometimes, they say the Senate is the only institution we know of that is run by the inmates, and today we are evidencing that somewhat over on the floor. They have been having debates and backed up 40 votes, if you can imagine that—40, count them. So we will be over there on 10-minute votes. They estimate we will finish somewhere around 6:30 this evening; 40 votes all day today. Sam has been here a little longer than I have, a couple of years, but I don't think either one of us has ever seen anything quite like this.

Anyway, back to the subject. In this new electronic information age, we rely more and more on computers, of course, and telecommunications to make government work better and faster. Making government work better is not something I take as an oxymoron statement. I think that we can have government working better, and that has been what this Committee's efforts have been focused on through the years.

In this computer age, the benefits are many, but the costs can be high, too. Reliance on computers can make us vulnerable in ways never envisioned in the age of paper documents and filing cabinets, and the stakes are very, very high. The government deals every day with information that helps secure our national defense or involves the personal privacy of our citizens.

Over the years, this Committee has examined threats to security and privacy as diverse as teenagers hacking into DOD computers, which was mentioned, and IRS employees browsing through taxpayer records, whether just prurient interests or whether they were really trying to do something. We have some people in jail, as a matter of fact, who browsed through, changed some accounts, got a kickback, and they are now in prison. So this is not something that is just a theoretical exercise.

I wanted to add one thing, too. We are concerned today about DOD, as Senator Nunn mentioned, but the civilian counterpart is also a huge danger to this country. I mean, really, this is big stuff You think of a Russian hacker over there who transferred a couple of million dollars, part of it to an account in Geneva, or Zurich, I guess it was, and some to an account on the West Coast. This was just one Russian hacker. Multiply that with faster computers coming online, greater-capacity computers coming online, and a bunch of well-organized hackers working for a foreign government, working all these things down to where they have done everything but take the last step on transferring billions of dollars to Merrill Lynch, to somebody else, to your account, to the Fed, to a government account, to a Federal Reserve bank. If you want to let your mind run a little rampant here, you literally have a new means of warfare, and I don't think I exaggerate that too much. You could literally foul up the economy of a whole country.

I have been concerned about this for some time. I have worked with one of our agencies that deals with this, in particular. I won't go into the details of that now, but if you think on that scale, you begin to pick up the danger of it. To me, it goes even beyond some of the dangers of the hackers getting into DOD, and so on. It really is a whole different level of concern than I think we have ever really been forced to deal with before.

When we get into this, our investigation suggests serious weaknesses in government computer systems. I requested the GAO study back in September 1994. It took them a while to put it together because it is a big job, but today the report that will be released reports that our worries were well-founded. In fact, to quote their words, "The potential for catastrophic damage is great."

Now, GAO reports that Defense computers face over 250,000 hacker attacks each year. That is just in DOD, and you can bet we have real cause for concern. The question now is what are hackers actually getting their hands on and what is the department doing as a result.

I talked to a couple of our biggest bank people and had them meet with some of the government officials on what they can do, and they are very concerned about this. Some of our leading banks are extremely concerned about what can happen to their accounts and what could happen to the economic system of this country if we don't find ways of controlling this.

So I congratulate Chairman Nunn today for having this hearing. We need to learn more about our system weaknesses. We need to know what the costs are. We need to know how to invest wisely now to prevent future attacks that may compromise not only important government or personal information, but literally, I think, our economic system. I think it is vulnerable now and I think as we get into this new computer age more and more, we have to watch out and we have to take every precaution we can take.

Thank you, Mr. Chairman.

Senator NUNN. Thank you, Senator Glenn. I look forward to continuing working together with you and Senator Roth and others on this important and indeed very crucial area.

Before we receive the General Accounting Office report, I would ask GAO scientist Keith Rhodes to make a brief introductory presentation on computer basics, networking, and exploitation techniques. Given our time frame, we are going to probably have until about 9:30 this morning. My guess is we have another 45 minutes before we have to run and make the very end of the first vote. So I hope that you can summarize, but don't assume we understand all this business. Take it step by step and summarize at the same time, if you can carry that out.

Senator GLENN. Mr. Chairman, if I might add just one thing, I have to run to another meeting. I will be right back, if I can get back from it. We have too many things going on this morning here, so I have to leave right now and then I will try and be back in a few minutes.

Senator NUNN. Good.

I am going to ask all of our witnesses who are going to be testifying to please take the oath. We swear in all the witnesses before our Subcommittee.

[Witnesses sworn.]

Senator NUNN. Mr. Rhodes, why don't you proceed?

TESTIMONY OF KEITH A. RHODES, TECHNICAL ASSISTANT DI-RECTOR, OFFICE OF THE CHIEF SCIENTIST, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. RHODES. Thank you, Senator Nunn. I will be very brief in my introduction.

My name is Keith Rhodes and I am Technical Assistant Director in GAO's Office of the Chief Scientist.

Senator NUNN. If you could talk right into that mike, these pick up only if you talk right into them.¹ (*Slide 1*)

Mr. RHODES. All right. I would like to give a very brief introduction to computer and Internet security, the purpose of which is to familiarize the audience with what the panels will be discussing today, or what the other speakers will be talking about, computer and Internet risks and security. (*Slide 2*)

First, I would like to give just a brief background on the initial concept people have when they think of a computer. (*Slide 3*) They think about some input from either a keyboard or an onboard storage or a modem. There is a central processing unit. There is an output to either a modem or a printer. (*Slide 4*) In the discussions today, we are going to have to think about it in terms of one computer being the input to another computer and the output being to

¹Slides 1 thru 29 appear on pages 177-191 in the Appendix.

yet another computer because the computers do form the network and that is the key issue to remember today, sir.

To give you a little perspective, I am going to talk about transmission speeds and storage speeds. (*Slide 5*) Senator Glenn gave a good point, saying that the processing power is becoming greater and the speed of processing is becoming greater, and the speed of transmission.

This will be my baseline. If we assume that the typical novel is approximately 60 characters per line, approximately 30 lines per page, and 200 pages, that means there are 360,000 characters in a book. (*Slide 6*) Why is this important? It is important because as computers think in bits and they store things in bytes, one byte is approximately one character, depending on how the character is structured. So the average novel equals approximately 360,000 bytes, or 350 kilobytes. (*Slide 7*) That gives you an idea of the typical storage capacities in memory. You can store about four books on a high-density diskette. On a 1.1-billion-byte hard drive, a gigabyte hard drive, which is not uncommon now, you can store about 3,000 books, and on a CD-ROM with 600 million characters on it, that is about 1,500 books.

There are two pictures up here, one I have superimposed on another. (*Slide 8*) The back picture is the ENIAC, one of the original programming computers that was used in the development of the first thermonuclear bomb. The inlay there in the corner which I tried to scale to the picture is actually my home computer. To give you relative ideas, the ENIAC weighed 30 tons. My computer weighs less than 20 pounds. The ENIAC took 200 kilowatts of power. My computer at home takes less power than a hair dryer.

The ENIAC could store approximately the equivalent of four sentences out of the novel and my home computer can store about 5,000 books. So these are relative computational powers. The original ENIAC could do approximately 330 calculations per second. My home computer can do approximately 133 million calculations per second.

Why is this important? This is important because now the computational power in the hands of the average person wanting to attack a network or attack a system is tremendous. If I can bring to bear the power of my home computer to try and break your password file just even through brute force, it would have taken a long time on the ENIAC; it would have taken an infinite amount of time, supposedly, on the ENIAC. But on my home computer, I can do it with a standard dictionary in probably less than an hour.

Senator NUNN. Now, we are going to be using this term "brute force" often during the course of these hearings. Would you define brute force? I believe what you mean is overwhelming with computer power the number of probabilities so you simply cover everything and reduce it down to—

Mr. RHODES. Absolutely.

Senator NUNN. But can you give your definition of brute force? Mr. RHODES. There are two views you can take. One is that I have the computing power to exploit weaknesses in your passwords. For example, if you are using common terms in a dictionary, I can load the dictionary in and do a brute force compare; that is, I can take the overwhelming power and apply it just to give as many combinations of dictionary words as possible. Or, as in your example, which is correct, I can just take as many combinations as possible of the characters on a keyboard and try to come up with the answer to your password. So as the cryptographic developers work harder and harder to make their algorithms stronger and stronger, of course, the computational power in the hands of those who are trying to break in become stronger as well.

In terms of transmission speeds, I have given the speed of the modem or the speed of the circuit, the approximate time in decades of when the speeds were available. (*Slide 9*) At the bottom—this is very important—that is how long it would take for you to pass our typical novel of 360,000 bytes across a circuit at that speed. If we go back to 300 bits per second, it will take me 160 minutes. If we go out to what is called T-3 speeds, 45 million bits per second, it takes 0.06 seconds.

The point here is that the attack can be extraordinarily fast now. Whereas you might be able to load data on the system to keep me on the wire or keep me on the circuit a long time so that you can catch me and get better evidence, if my attack only takes 0.06 seconds, it is very hard to see that I have even been there.

Senator NUNN. Are we all the way out to the end of that scale now?

Mr. RHODES. You are actually beyond the scale now. You can procure circuits that are 155 million bits per second now. You can get that from standard carriers for companies, and up to 1.544 million bits per second for individuals. I was at the INTEROP conference in Nevada in April and there was a long-haul carrier—one of the major carriers is offering that (1.544 million bits per second) speed to your home, down to your desktop in your house, if you want to pay for it. So it is not unreasonable to think that people are going to be, from their home, moving at greater than a million bits per second.

Senator NUNN. So when you talk about 0.06 seconds to carry out an attack, would you carry that one step further and tell us sort of what kind of attack so we can grasp what you can do in less than a second? Give us a hypothetical.

Mr. RHODES. Well, if I can capture your password file, if I can exploit a problem in—

Senator NUNN. The password is the entry gate into the computer?

Mr. RHODES. Right.

Senator NUNN. It is the security system? It is your lock on the door?

Mr. RHODES. Right. It is your first level of access control.

Senator NUNN. All right.

Mr. RHODES. If I can exploit a file transfer, an existing piece of software that is on your system, and plant either a Trojan horse, which is a piece of software that does something other than what it is supposed to do that allows me to steal your password file, which is what I really want to do—I want to get the password file and bring it back to my home computer so, at my leisure while I am watching television, my computer can be crunching away trying to break your password file. If I can get that file at this speed, you don't even know I have been there and therefore I am able to get the entire file in less than a second. That is the real point we are talking about. As the computational power rises and as the speed of the circuit rises, I am able to automate the attack more and I am able to have the attack take less time.

Here is the original view of computing, isolated computers around the world. (*Slide 10*) With the Internet, they are now all interconnected. (*Slide 11*) The key to the Internet—it was originally an idea for keeping command and control alive in a post-nuclear attack. The strength of the network in being uninterruptable and being so-called self-healing, because it can re-route messages to make certain they get to their destination, is also one of the great challenges for security because that means that, as you have pointed out, you don't necessarily know where the attack is coming from, because the attack can be coming from a site several computers away from the one that you actually see the attack being launched from.

Senator NUNN. Let me ask you a basic question, but I think it is one that occurs to a lot of people. The Internet started basically as a military security program?

Mr. RHODES. Right.

Senator NUNN. So the U.S. Government basically funded up front a lot of the Internet?

Mr. RHODES. Correct.

Senator NUNN. Now, you have this massive network of computers all over the world, of which the Defense Department parts of the net are just part of it, but they are hooked into all of it.

Mr. RHODES. Right.

Senator NUNN. Who pays for all this? What are the economics of the Internet? I keep asking people that question, but nobody ever has an answer.

Mr. RHODES. That is actually a very good question, Senator. Who does pay for it? I pay for my Internet connection. There are a lot of people on the Internet who argue that it should be free, but since phone service isn't free, the Internet shouldn't be free. So the individual companies or entities that are hooked into the Internet are usually handling it as part of their own telecommunications bill.

However, the Internet is a cooperative network. Every node on the Internet, every computer on the Internet, every Internet site is part of a structure that allows it to store and forward the messages as they get moved from site to site. So it is a collective cost, in a sense. The Internet service provider that I go to is part of the Internet and therefore has a software obligation to the Internet to handle packets that get sent to it for routing.

Senator NUNN. So really everybody pays for it?

Mr. RHODES. Absolutely.

Senator NUNN. Everybody that uses it?

Mr. RHODES. Everybody that uses it ends up paying for it, of course, unless you have broken into it and then it is free.

Another point about this is that the sites that are on the system are U.S. and foreign, government, military, commercial, private individuals and individual organizations, and educational sites. So even though there are different kinds of sites that are hooked onto the Internet, they are all interrelated. Senator NUNN. This is another hypothetical but basic question.

Senator NUNN. This is another hypothetical but basic question. If the U.S. Government pulled its part of the Internet off and said, we are not going to play anymore, we don't want to be part of this net, what would it do to this overall system and how long would it take the system out there to make up for it?

Mr. RHODES. The only thing that other sites might notice is a drop in speed because that is one of the—every one of the sites out there is assumed by the network to be unreliable. Therefore, if it goes to a normal destination and can't pass its data on, it will just re-route it.

Senator NUNN. It will just be re-routed?

Mr. RHODES. Right.

Senator NUNN. The U.S. Government, although a part of this with Defense, and so forth, could pull out of it and there would still be a net?

Mr. RHODES. There is no central authority, there is no central control.

Senator NUNN. Nobody could jerk it down by themselves, or no country or no single entity?

Mr. RHODES. No single country can bring the entire net down. I was just passed a note by Dr. Neumann, I believe, that says make the point that every node is a potential spy, and that is true. That is a very clear and very direct point.

Senator NUNN. And how many nodes are there altogether?

Mr. RHODES. Right now, they are going to a new version of the protocol because they are running out of address space. In our report, we quote 40 million because that is the number of addresses that are currently registered, 40 million.

Senator NUNN. So we are really in a whole new world of information, and also a whole new world of espionage and sabotage and disruption and interference?

Mr. RHODES. Absolutely. As I stated, the strength of the network is its weakness. I mean, the fact that it is disparate makes it strong, but the fact that it is disparate makes it weak as well.

Senator NUNN. Right.

Senator LEVIN. Can I just ask one question on that just to follow up your question, Mr. Chairman?

Senator NUNN. Sure, Senator Levin.

Senator LEVIN. The Internet would exist without us?

Mr. RHODES. Oh, absolutely.

Senator LEVIN. So we don't have to play.

Mr. RHODES. That is true.

Senator LEVIN. We don't have to have any web sites if we didn't want to have web sites. The implications would be huge.

Mr. RHODES. Yes.

Senator LEVIN. But nonetheless we have chosen to participate. It would exist if we didn't participate, but if we didn't participate, our web sites would not be available and that would deny us huge benefits.

Mr. RHODES. Absolutely.

Senator LEVIN. But it also would take away the access to our web sites. Could you describe what would happen if we decided not

to have any web sites, if the DOD said we are pulling all of our web sites from the Internet?

Mr. RHODES. Well, for example, on another job that I am doing I am looking at the nature of cryo-cooling on focal plane arrays for long-wave infrared sensors. I would have to visit a lot of places to get the basic information on that to understand the state of the technology. As it is now, I can go to the web site at Phillips Lab out in Albuquerque, New Mexico. I don't have to make a phone call. I don't have to fax anything. I can go there, not bother anybody, download the current test plans that they have, look at them and know what is going on. Well, multiply me by everybody who works at DOD and everybody who wants to talk to DOD.

There are portions of the Department of Defense that have their own private networks, and they have to because they are classified. But as Mr. Brock will talk about, there is a lot of information out there that is unclassified and necessary to the commerce and the business of the Department of Defense.

Senator NUNN. OK. We had better run on through this. I will try not to interrupt again. Just go ahead.

Mr. RHODES. Just a quick view here. (*Slide 12*) If you are hooked up to the Internet, it is as though you have this infinite disk drive or storage device on your own computer that everyone can support and collaborate with. The problem is, of course, you can get the light bulb of the great idea, but you can also put your foot in a bear trap. You are connected to the world and the world is not necessarily "Mr. Rogers' Neighborhood." There are good people out there, there are bad people out there.

If you look at how the Internet works in a client server environment where the client is making a request of the server and the server actually sends a file back or has some connection, a request is sent over and a response comes back. (*Slide 13*) In this scenario, it is a file transfer. (*Slide 14*) Mr. Gelber was kind enough to give me his E-mail address. If this were a mail server, Mr. Gelber's address would be on the server and if I were the client, I would be sending him mail and I would get some response back. But that is it. It is this collaborative, cooperative environment where one node makes a request of another computer and the computer gives some kind of reply.

This is an out-of-date, very busy slide, but it represents the highspeed linkages inside the United States. (*Slide 15*) This does not include the foreign networks. This does not include the external networks around the world, but these are all very high-speed links that handle the majority of the traffic.

The point of the slide is that there are many points of entry and it is not uncommon for a message going from the East Coast to another site on the East Coast to have to navigate to the West Coast to get back to the East Coast. That presumed unreliability of the network—it sort of takes a path of least resistance.

In this example, I will talk about a real path of least resistance going from Andrews Air Force Base to Ramstein Air Force Base. (*Slide 16*) These are two DOD sites, but if I am using the Internet, they may not necessarily go from DOD site to DOD site. I go from one DOD site to another, from that DOD site to the University of Chicago, from the University of Chicago to British Telecom, from there to Oxford University, from there to the University of Hamburg, and from there finally to Ramstein. Now, that is a DOD site to a DOD site and this is an actual scenario.

Senator NUNN. You bypassed the Washington Post on that route, I see.

Mr. RHODES. Yes, I did.

Senator NUNN. That is not necessarily so, though?

Mr. RHODES. Not necessarily so.

The point behind that is that the hackers will use a technique called looping and weaving in order to hide their tracks and avoid identification and detection. (*Slide 17*) I am a subject in New York City. I go to a computer in Latvia. From Latvia, I go to U.S. News and World Report. From U.S. News and World Report, I go to George Washington University, and from there I finally get to the Pentagon.

Why is this important? This is important because if the comm group, the communications group, at the Pentagon is trying to find out where the attack originated, they may only be able to see back to George Washington University, and they call the people working at George Washington University and say, you are breaking in, and they say, no, we are not breaking in, somebody at U.S. News and World Report is breaking in. Then you go there and they say, no. it is from Latvia.

Senator NUNN. Yes, I read Cliff Stoll's *The Cuckoo's Egg*, and that was a very clear presentation of all the different routes. It was amazing.

Mr. RHODES. Exactly. One of the dangers involved is that you can place a sniffer—a sniffer actually steals data off the network (*Slide 18*) The idea is that if user A sends mail to user B, the system name, the user I.D. and password are stolen by the sniffer (*Slide 19*) It gets over to user B. (*Slide 20*) When user B replies, (*Slide 21*) the system name, password and I.D. are stolen again and now the sniffer has it. (*Slide 22*)

An example is going from Naval Research Lab to Rome Labs to Wright-Patterson and down to a DOD contractor. (*Slide 23*) If I take an alternative route, I actually go from NRL to a government site, then to a commercial site, and then to Wright-Patterson. (*Slide 24*) If, in this case, the sniffer is at the commercial site, the password, I.D. and node name are stolen and that compromises the ability of the fire walls that are set up around Wright-Patterson to actually protect their site.

Here is just a very small subset of protocols of the Internet. (*Slide 25*) The point behind this slide is that these all have known attack scenarios and they all have known counter-measures. The bad news is they can be attacked. The good news is there are counter-measures for them. Two very common break-ins are on the simple mail transfer protocol and the file transfer protocol, which do exactly as their names say, transfer mail and transfer files.

The point (*Slide 26*) to this whole discussion is that in the old world I knew how to protect a computer because I protected it as an asset. (*Slide 27*) I hired guards, I gave them guns, and I put up gates. In the new world, that is all broken because now the guard can't stand over the wire and shoot at the rogue messages coming across the wire. (*Slide 28*) The final point I would like to make is Gene Spafford runs a computer security program at Purdue University and he has made this quote tongue-in-cheek, saying that the only secure computer is one that is unplugged and turned off, and that is still not actually true. (*Slide 29*) Dr. Neumann says that you can still pick it up and steal it. Turn it back on again and now you have everything you need.

The point is that we are not going to turn them off and we aren't going to unplug them and we aren't going to put them all in vaults so nobody can use them. So we have to understand the risks and we have to understand the threat.

I know I have taken up more time than I should have.

Senator NUNN. Well, it is fascinating. Thank you very much. I understand you can put your whole presentation on a disk so it can be distributed. Is that right?

Mr. RHODES. Yes, sir.

Senator NUNN. That would be good. I think members that are not here would like to see that.

Mr. Brock is the Director of Defense Information and Financial Management Systems for the General Accounting Office. Jim Christy is an investigator detailed to the Subcommittee staff from the Air Force Office of Special Investigations.

Mr. Brock will present the findings of a GAO report, which I consider of enormous importance, which is being released today concerning attacks on the computer systems of the Department of Defense. This report, which was requested by Senator Glenn and myself and others, presents a rather disturbing picture of computer security within the Department of Defense.

TESTIMONY OF JACK L. BROCK, JR.,¹ DIRECTOR, DEFENSE IN-FORMATION AND FINANCIAL MANAGEMENT SYSTEMS, AC-COUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. BROCK. Thank you, Mr. Chairman. We have our report available today in traditional format, which is the blue cover which many of you recognize.² We also have it on a disk, and it is also available at the GAO web site. One of the points I want to make is by putting this report up on a web site now, we save an enormous amount of money on printing and publishing costs and distribution. It makes our life easier and it makes the life easier of people that need GAO reports.

I want to just make a very quick demonstration. I have right here my GAO badge and my Pentagon badge. It was hard for me to get this badge to get into the Pentagon. It is difficult to get in. If I go around and ask for information, they challenge me. They have guards at some of the doors, they have locked file cabinets. More importantly, the information is geographically dispersed. It would be very difficult for me to assimilate all the information I might want to put together on any particular program.

I can be relatively unskilled, far less than the skill that Keith Rhodes has, and get access to this information, many times with

¹The prepared statement of Mr. Brock appears on page 192.

²See Exhibit No. 1 which appears on page 422.

good reason and without being challenged. But if I am a hacker and break in, I have access to information that I shouldn't be having. We are talking today about sensitive but unclassified systems. I don't want people to make the mistake that we are talking about super-classified systems that have the deepest secrets of the Nation, but we are talking about the systems where the majority of the Department of Defense's business runs.

Just yesterday, I asked people in my group to take a look at systems that we are reviewing right now to determine what kind of sensitive information is on these unclassified systems. For example, we are looking at DOD's stock control system. It orders and tracks supplies for the Air Force and Marine Corps. It provides information on what supplies are available and who ordered and received the supplies. Illicit modification or denial of service could have profound consequences on the delivery of supplies during a time of national emergency.

We are also looking at the Army's Military Traffic Command Management System in Falls Church, Virginia. This system is a water port documentation and cargo accountability system which is used by Defense at all worldwide strategic seaports to manage port traffic and cargo transport. Any adversary with access to this system could learn when ships arrive and depart, at what ports, and what kind of cargo they are carrying.

We are also looking at the Defense Transportation Tracking System which uses satellites to track Defense and commercial carriers with sensitive cargo. This includes explosive, ammunition and classified arms. We are looking at Defense's Activity Address Code, which is a department-wide logistics system that contains shipping and billing address information on everything.

What I am talking about is a whole series of systems, not just these four or five systems, but literally thousands of systems that contain important, sensitive information, not classified, but which looked at individually and collectively can provide an adversary or a hacker with a lot of information about what the Department of Defense is doing.

When you think about computer security, it is pretty complex. A good computer security programs says, OK, how vulnerable am I, how vulnerable is my system to attack, what is the threat out there, who are the people or the entities that might want to attack, what is the value of the information, and then how much does it cost me to provide an adequate level of protection?

If you don't make these tradeoffs and assessments, by default, you have an inadequate computer security program. Very, very few systems begin to make these kinds of tradeoffs. I want to compliment the Department of Defense. We think they are further ahead than the other Federal agencies we have looked at. We haven't done a government-wide survey, but—

Senator NUNN. So this is an important point today. The problems you are pointing out in DOD are, in all likelihood, worse in other government agencies?

Mr. BROCK. We believe so. The difference in DOD, though, is they have information that is very attractive to people. People want to go after systems that have vital information, systems that control money, as Senator Glenn was talking about. I think DOD is probably, because of the size, the uniqueness of the information that is carried in the systems, more attractive to hackers and organized attacks than other systems. DOD is better prepared to deal with some of these hacken threats, but I don't think the level of preparedness is adequate.

The point I wanted to make with just this little interlude here is that 10, 15, or 20 years ago you could protect a lot of this information with lock and key and physical separation. That is not possible today, and yet the level of protection that is available today is probably less than it was 10 or 15 years ago. That is particularly challenging at DOD.

I think you mentioned some of the statistics. The computing environment at the Department of Defense—they have over 2 million personal computers. They have over 10,000 local networks. They have over 100 long-distance carriers. They have 200 command centers. They have 16 mega centers. They have a lot of computers, they have a lot of systems, they have a lot of opportunities for exposure, but yet they can't manage without this information.

Senator Levin was asking, well, what would happen if you took this away. If you took it away right now, the Department's business would stop. If you took it away from any agency, the business would be curtailed. As we mentioned, they have very attractive information, and as a result of that they are experiencing a lot of attacks. The Department itself estimates there are over 250,000 probes yearly. And many of these are successful. They are not sure how many successful intrusions take place, but the Department is unable to react but just to a very, very few of these attacks.

The attacks cause damage, and the cases that have been documented—we were able to really examine the damage that has taken place. The case that we are going to discuss this morning briefly, along with Mr. Christy, is the Rome Laboratory. The Rome Laboratory in New York is the Air Force's premier command and control research facility. For example, they do the basic R and D on air tasking order systems. Two hackers broke into this and other systems. They literally took control of the lab's primary network and 33 sub-networks for a period of 2 or 3 days. They used relatively common techniques. They were not particularly sophisticated, and yet they controlled the network.

Jim is going to provide some details on exactly what happened during that break-in.

TESTIMONY OF JIM CHRISTY, INVESTIGATOR, PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

Mr. CHRISTY. Thanks, Jack. Good morning, Senator Nunn, Senator Levin. (Slide 1)¹

I would like to make a couple of comments before we start walking you through this. The Rome Labs case was fully investigated and has left critical questions unanswered. Who was ultimately responsible for the intrusions, what was the motive of the intruders, and what was accessed and what was taken? As will be evident from this case study, we would never have discovered what we had absent human intelligence. Technology can assist law enforcement

¹Slides 1 thru 49 appear on pages 200-224 in the Appendix.

in the collection of evidence, but technology alone cannot solve these kinds of offenses. These cases will be solved the old-fashioned way, with human intelligence.

Now, I would like to take the opportunity to walk you through the Rome Labs intrusion. (*Slide 2*) It occurred in the spring of 1994. There was a sniffer, as Keith described. (*Slide 3*) A sniffer was discovered at Rome Labs by one of the system administrators. They went through all the notification process, through DISA and through the Air Force. OSI was notified.

The Air Force Emergency Response Team deployed a team from Kelly Air Force Base in San Antonio, Texas, (*Slide 4*) to Rome Labs, and OSI deployed a team of computer crime investigators from Andrews Air Force Base. (*Slide 5*) They assessed the situation at Rome, briefed the commander, (*Slide 6*) and what they found was that over 30 systems at Rome Labs had been compromised by a total of 7 different sniffers. The commander was briefed on the problem and was asked whether he wanted to leave the systems open so we could trace the hackers back or whether he wanted the systems secured. He made a decision to secure the majority of the systems and leave a couple of them open for the investigation.

We traced the hackers back using normal standard techniques to two Internet providers. (*Slide* 7) The attacks were either coming from an Internet provider in New York City or one from Seattle, (*Slide* 8) but that is basically where the path ended because they were entering these Internet providers via telephone lines. (*Slide* 9) So what we had to do as investigators is go to those local jurisdictions and get court orders for trap and traces. With the realtime nature of these cases, that really wasn't feasible.

We set up keystroke monitoring, which is the equivalent of a wiretap, at Rome Labs (*Slide 10*) and set up context monitoring, limited surveillance at the two Internet providers in New York (*Slide 11*) and Seattle. (*Slide 12*) We were able to get the hackers' names from the monitoring. (*Slide 13*) We had two hackers, one named Datastream, one named Kuji. (*Slide 14*) We then went to our human sources, our informants, and asked all of them who surf the network on a regular basis for the true identity and the whereabouts of Kuji and Datastream.

One of the informants came forward and said that they had had an E-mail conversation with a hacker named Datastream 3 months prior to that. (*Slide 15*) Datastream said that he was a 16-year-old kid from the United Kingdom (*Slide 16*) and that he hacked .MIL addresses—and .MIL is just the suffix for all military computers in DOD—he hacked them because they were so easy.

In addition, he has a hacker bulletin board that he runs out of his house, and that is how hackers share information, and he provided that phone number to our informant. Well, that is a clue, so we immediately called Scotland Yard's computer crime unit. (*Slide* 17) They set up a surveillance. They had pen registers established on the subscribers' phone numbers and within about 2 hours they had the individual's, Datastream, phone phreaking out of the United Kingdom. (*Slide 18*) Phone phreaking is the hacking of phone systems to make free long-distance phone calls.

They would hack British Telecom, which is against the law in the United Kingdom. They would then attack phone systems in Colombia, Chile or Brazil, hack their phone system, gain the 1–800 number and then enter the United States at the Internet provider in New York City. (*Slide 19*) He would pay for that subscription with a fraudulent credit card (*Slide 20*) with a credit card generator which was generated with a hacker program that is available out on the Internet. Once he defrauds the Internet provider, he now is on the Internet and can go worldwide free. He attacked Rome Labs from there. (*Slide 21*) Some of the other attacks were from Columbia, Chile and Brazil into the Internet provider in Seattle (*Slide 22*) and then into Rome Labs. (*Slide 23*)

He actually followed contracts. (*Slide 24*) Lockheed was a major contractor and had contractors on-site at Rome. Their user I.D.s and passwords were sniffed at Rome Labs. (*Slide 25*) So when the hacker got to Rome through Seattle and South America, (*Slide 26*) he then was able to pick up the user I.D. and passwords of the contractors when they dialed into their home system. He followed those contractors home, compromising four Lockheed systems in Southern California (*Slide 27*) and an additional fifth in Texas. (*Slide 28*)

The attacks went through another attack scenario through South America, (*Slide 29*) through Seattle, (*Slide 30*) and launched an attack back in Europe on Headquarters NATO. (*Slide 31*) Another attack we saw was data being downloaded from Wright-Patterson Air Force Base in Ohio (*Slide 32*) to Seattle (*Slide 33*) and it was going to Latvia. (*Slide 34*) Now, we don't know if Latvia was downloading that data from Wright-Patterson Air Force Base or whether the kid was from the UK. (*Slide 35*) But in any event, if it was the 16-yearold hacking through Latvia, if Latvia had been monitoring their system, they would have been able to collect all that information that was transiting their nodes. NASA was a major target through South America, (*Slide 36*) Seattle (*Slide 37*) to Rome Labs, (*Slide 38*) and then to Goddard Space Flight Center here in Greenbelt, Maryland, (*Slide 39*) and also the Jet Propulsion Lab in Southern California. (*Slide 40*)

Scotland Yard developed enough probable and was issued a search warrant. (*Slide 41*) They were actually circling the house (*Slide 42*) and the plan was once he got to Rome, (*Slide 43*) they would execute their search warrant so we would be able to have that complete connection. (*Slide 44*) Where he went after he went to Rome Labs, he went to the Korean atomic research institute and basically logically picked up all the disk space (*Slide 45*) and moved it to Rome Labs.

We asked Scotland Yard not to execute the search warrant at that point. We wanted to determine whether we were dealing with North Korea or South Korea because it wasn't clear at that point. It was determined that it actually was South Korea's atomic research institute, but if it had been North Korea's atomic research institute and they had detected the intrusion, it would have looked like the U.S. Air Force had been attacking them. If you remember, in that time frame we were in sensitive negotiations with the North Koreans over their atomic weapons program.

Senator NUNN. Was he downloading information from Korea to the Rome Lab?

Mr. CHRISTY. He didn't download the data, but he could have. He had total control over that data. He just kind of made all the disk space at Korea part of his computer and he had complete access to it. He didn't access it while we were monitoring. He had access prior to our monitoring and we don't know what he did at that point.

Senator NUNN. So if that had been North Korea instead of South Korea, or even if it was South Korea, it would have looked like to the South Koreans or North Koreans, whichever the case may be, that instead of a 16-year-old kid in the United Kingdom that it was a U.S. Air Force effort to get their information?

Mr. CHRISTY. Exactly. This is the total picture that we saw. We actually had two hackers, one named Kuji who was never, ever identified, and Datastream that was. (*Slide 46*) But after Rome Labs, our monitoring detected that over 100 victims downstream were attacked by these two people, (*Slide 47*) so you can see the scope of the nature and all the investigative jurisdictions that were transited here.

Senator NUNN. Did the 16-year-old not know the other hacker? Mr. CHRISTY. He only met the hacker electronically. He met him on the phone and in electronic chat sessions, but he had never physically met him.

Senator NUNN. So he didn't know who he was dealing with?

Mr. CHRISTY. No, sir, and all the information that he got he gave to Kuji.

Senator NUNN. Did he know where Kuji was, where he was located?

Mr. CHRISTY. No, sir. No one knows where Kuji is. That is still an open investigation.

Senator NUNN. He did not know where that information was being downloaded?

Mr. CHRISTY. No, sir. They meet virtually electronically.

You can see the number of countries that were involved in this. There were at least 8 countries that these hackers used as basically conduit to avoid detection and identification. (Slide 48) The problems that were encountered—whose jurisdiction, tracing on the Internet, tracing on public switches. The surveillance—where do you set up your monitoring and how do you recover what was stolen? These were all major problems. (Slide 49)

The last one is significant, and that was the damage assessment, and at that point I would like to turn it back over to Jack.

Mr. BROCK. Mr. Chairman, let me emphasize this is one incident. This could be duplicated in many systems. The Air Force estimated that it cost about \$500,000 to take the systems off the networks, to verify the system integrity, to put in the necessary security patches, and to restore information. What it is not taking into account is the value of the potentially corrupted information that was taken.

The data that was compromised at Rome is basic R and D on such projects as air tasking order systems. Actual air tasking orders, which are the basic intelligence information that the pilots use to carry out their missions, are classified. What Rome does is develop the automated systems that develop these air tasking orders. This information was on a sensitive but unclassified system. The fact that people had access to this R and D would give them a lot of insight into how we develop and execute air tasking orders.

Through Rome, they also breached Wright-Patterson AFB systems and also gained access to sensitive information there. I think Jim pretty well covered what they got from the South Korean atomic energy people. They also entered NASA systems of Goddard. They downloaded 19,000 encrypted passwords and transported those to Latvia as well as other locations. We are not sure what happened to those.

So two hackers, plus perhaps some other unidentified hackers, enter and download a lot of information. We are not sure what happened to all of that information and it is impossible to really assess what the potential damage was or could be.

Senator NUNN. Mr. Brock, we now have a vote up there and once we get over there, it is going to be hard to come back. So I would guess we have about 12 more minutes, so I just wanted to give you that so you could apportion your time on that.

Mr. BROCK. Well, rather than go through other examples, I would like to immediately go to what we see the problems are at DOD.

Senator NUNN. We are going to come back in other hearings and have other examples and we will be calling you back. We just really wanted to get this process started because of its importance, and we will have at least 4 more days of hearings on this overall subject.

Mr. BROCK. All right, sir. At DOD—and this is really highlighted in our report—they do a better job than most in terms of reacting to identified attacks. They also do a much better job than others in probing and identifying where weaknesses are. But we found that they have a lack of a consistent policy that is enforced. There is a lack of accountability among system administrators and owners as to protecting those systems and assuming responsibility for that. There is a very big lack of training.

One of my favorite stories is from a previous job we did a couple of years ago on hackers. We visited one installation where there was a clerk who was a part-time system administrator. She had never had a day of training. When we asked her what she would do if she noticed an intrusion, she broke down in tears and said she would call her sister. It turns out her sister is a telephone operator who had a PC at home or something like that and knew something more about computers than she did.

I don't want to say that is typical of the DOD environment, but there is a lack of training, a lack of skills, and a lack of knowledge. Without that, you can't make those assessments and tradeoffs that I was talking about earlier in my statement.

We have a series of recommendations that we have made to DOD which address each of these issues in terms of developing a policy, in terms of developing a mechanism for enforcing accountability, a mechanism for providing adequate training, and a developing a method for doing assessments of their individual systems.

In our exit conference with DOD, they acknowledged the problems and issues they faced and agreed, I think, in large part with our recommendations. Hopefully they will begin to take action on them. Senator NUNN. Good.

Mr. BROCK. That concludes the summary of my statement and Keith or I would be happy to respond to any additional questions you might have and also, of course, be happy to return to your follow-up hearings.

Senator NUNN. Well, thank you very much. My first question would be could you summarize the recommendations you made to DOD?

Mr. BROCK. Even though DOD is developing-----

Senator NUNN. Summarize your findings first. Why don't you tell us, one, two, three, four, what your findings were, the top three or four, and then the three or four recommendations?

Mr. BROCK. We found that DOD's policies were not consistent, or did not effectively lay out what should be done in terms of developing security policies, a security program, and protection. We found that individuals that were responsible for systems administration generally lacked training, and we found that there was a lack of accountability or an acknowledgement of a problem of security risk by people who operated, managed, or, and I will put this in quotes, "owned" systems.

As a result of those, they didn't put into place the various, I think, relatively simple precautions that would do a lot to protect their systems. We are talking about things such as effective password management, effective system administration, effective monitoring, calling in when you see a problem. These things are not occurring as a general rule.

Senator NUNN. Could you capsule for us how many intrusions there were, how successful they were, how many of those intrusions were, first of all, detected, and then finally how many of the detected intrusions were reported with the official reporting system?

Mr. BROCK. OK. We are using DOD estimates here. We relied on their estimates. DISA estimates they experienced about 250,000 attacks last year.

Senator NUNN. That is the whole Department of Defense?

Mr. BROCK. That is the whole Department. I don't think anyone has a good idea if that is a good estimate or a bad estimate. It is an estimate and it is probably better than anyone else's estimate. Based on the Department's own internal controls where they were attacking their systems to assess vulnerability, they have conducted 38,000 attacks and they successfully gained access—and this is again according to their figures—

Senator NUNN. This is the internal security, testing their own system?

Mr. BROCK. Yes, sir. They gained access 65 percent of the time. Of the successful attacks, 988, or about 4 percent, were detected by the target organizations. Of those detected, only 267 attacks, or 27 percent, were reported to the Department. So you can see a consistent trail through there. Most attacks were successful. Most attacks that were in were not detected. Those that were detected, most were not reported.

Senator NUNN. So something has got to be done on that whole chain?

Mr. BROCK. Yes, sir.

Senator NUNN. OK, go ahead. I interrupted you before you got to your recommendations.

Mr. BROCK. Our recommendations are that the Department has a defined policy on what to do with computer security, and I think it is relatively easy to develop a defined policy. The difficult part is implementing it. We would like a greater degree of accountability expressed and shown within the Department for implementing the program.

We would like to see much more rigorous training and development of a career for systems administrator security personnel. We would like to see more rigorous follow-up. We would like to see, even though they are doing a pretty good job on this, a better capability for reacting to known break-ins.

Senator NUNN. You said that the Department of Defense officials and information systems experts believe that over 120 foreign countries are developing computer attack capabilities, is that right? Mr. BROCK. Yes, sir. We were informed of that by NSA.

Senator NUNN. Is there any kind of listing of countries which

pose the greatest threat which are the furthest along in this? Would it be mainly your industrial countries?

Mr. BROCK. The NSA knows that information, but it is classified. Senator NUNN. OK. We will get into that at another forum.

Senator Levin, let me turn to you for final questions here because we have the 5-minute bell, as you see, up there. Before doing that, though, let me just briefly introduce Mr. Christy a little more because he has been a key part of our staff here.

Mr. Christy, who testified this morning, is the program manager for computer crime investigations and information warfare for the Air Force's Office of Special Investigations. He is currently detailed to the Subcommittee as a congressional fellow. For the past 5 years, Mr. Christy has been the vice chairman of the Federal Computer Investigations Committee, which is composed of computer crime investigators and prosecutors representing almost every Federal agency in the government.

Also, Dr. Stoll, I believe, came in, and I believe he came in after we had said that we have 40 votes today. This is our version of *The Cuckoo's Egg* over here in the Senate. Dr. Stoll wrote that fascinating book, and we look forward to your testimony at a point of time in June. We appreciate very much your cooperation. A fascinating book.

Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. First, Mr. Chairman, thank you for your tremendous leadership here. These are very, very significant hearings. They are going to lead to some major changes, hopefully, to protect the material which we now rely on computers to store and to access. I want to commend the Chairman of our hearing today, our ranking member, Senator Nunn, for the extraordinary effort that he and his staff have put in.

Second, I want to have my statement be made part of the record, my opening statement.

Senator NUNN. Without objection.

[The prepared opening statement of Senator Levin follows:]

PREPARED OPENING STATEMENT OF SENATOR LEVIN

"Information warfare" is a phrase that sounds like science fiction or a threat from some distant future. But the persons testifying here today know information warfare is not fiction, and it is not a future threat. Information warfare is a reality. It goes on today all across this country, and it poses a current threat to our national security. And we're not paying enough attention to it.

The problem is simple but profound. Today, our national security depends upon computers. Today, we can't move a battleship, communicate battlefield information, develop weapons, deliver supplies, assign personnel, aim missiles, or perform a thousand other military missions without computer systems.

These computer systems use communication pathways and software tools that frequently are not under the control of the Department of Defense. We're told that maybe 10 percent of DOD's computer traffic is classified and moves on very secure systems. The other 90 percent of DOD data is unclassified and moves along poorly secured pathways, the majority of which are not government-owned or operated.

These pathways include telephone lines, cable, satellite feeds, even microwaves. Each is susceptible to monitoring, infiltration and manipulation.

Information warfare is based on that fact. Its battlefields are the pathways over which computer data is transmitted. The weapons are software programs that can read, intercept and even alter the data moving from one military computer to another.

The names of these new weapons are colorful. They include sniffers, phone phreaking, worms, Trojan horses, logic bombs and more. The stereotype of someone who breaks into computer systems is the teenage hacker playing games. But this stereotype and the colorful terminology are distractions from the real national security threat.

We will hear today about instances in which computer hackers have sold military information to foreign agents. How hackers attacked military computers to get information during Desert Storm. How hackers have used U.S. computers to lift nuclear information from another country's database, risking international crisis. What happens when hackers learn how to alter battlefield instructions or, during a military confrontation, simply paralyze the computers that move our military supplies and personnel? What if hackers impair our military systems with such subtle software that we don't even know the systems have been hit?

That's not all. An information warfare exercise conducted by the Rand Corporation for DOD looked at attacks on computer systems within the United States and its allies to sabotage domestic infrastructure such as transportation, utilities and finance. These attacks could result in train wrecks, city-wide power outages, banking disruptions, and worse—together generating a domestic chaos that could undermine our national security from within.

DOD is only now establishing the infrastructure needed to detect, assess and counter the threats posed by information warfare. Established 3 years ago, the Defense Information Systems Agency conducts simulated attacks on individual military computer systems to identify vulnerabilities—succeeding, by the way, in 88 percent of those simulated attacks. Over the last 3 years, the military services have each established an information warfare center to detect and counter attacks on their respective computer systems. It is only now that the first DOD-wide vulnerability assessments are being made, with results that show we have a long way to go. For example, we will hear today that there are an estimated 250,000 attacks on military computers each year, of which only 4 percent are detected by the systems under attack and of which only 1 in 500 is reported.

The Defense Department has over 2 million computers, 100 long-distance networks and 10,000 local networks. It has 550 installations that operate thousands of active computer systems. Few of these installations have a computer security expert charged with defending the integrity of the installation's computers and data. Filling that gap may be one important step to greater computer security. These hearings will hopefully identify other steps as well, and advance us from describing the problem to designing the solution.

We have years of experience defending our borders and our global interests. Now we have to learn to defend against attacks through cyberspace. I commend Senator Nunn and my colleagues for holding this hearing and look forward to the testimony.

Senator LEVIN. One quick question would be this: You made the point that classified material is not what we are talking about here today?

Mr. BROCK. That is correct.

Senator LEVIN. One of your solutions, however, did not seem to suggest that perhaps we should classify more material; that there is a lot of sensitive material which has not been classified in our computers. Should not one of the possible solutions be that we want to classify possibly some sensitive material which is now not classified?

Mr. BROCK. That could be a solution. When you evaluate the value of the information and how you want to protect it, if you deem the information so valuable that it needs to be protected at a higher level, then classification might be an option. One of the tradeoffs on that is more limited access to people that might need the information on a day-to-day basis. So there are always those tradeoffs.

Senator LEVIN. And whatever measures we take to protect our system, there will always be hackers out there who will have counter-measures, is that not correct?

Mr. BROCK. It is growing exponentially. There will always be counter-measures.

Senator LEVIN. So this is an ongoing problem to which there is no perfect solution which is a permanent solution?

Mr. BROCK. There is no perfect solution. That is why in our recommendations we advocate that this has to be an ongoing, continuous process in terms of looking at security.

Senator LEVIN. Thanks.

Senator NUNN. Dr. Neumann and Mr. Anderson, we appreciate you being here and we look forward to your testimony. You both have credentials and we are going to be fascinated to hear from you.

Mr. Brock, Mr. Christy, Mr. Rhodes, thank you very much, and we will be talking to you as we go along. We have to run and vote. Thank you.

[Whereupon, at 9:36 a.m, the Subcommittee was adjourned.]

SECURITY IN CYBERSPACE

WEDNESDAY, JUNE 5, 1996

U.S. SENATE,

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS, Washington, DC.

The Subcommittee met, pursuant to notice, at 9:34 a.m., in room 342, Dirksen Senate Office Building, Hon. Sam Nunn, presiding. Present: Senators Nunn, Glenn, Levin, and Lieberman.

Staff Present: Daniel S. Gelber, Chief Counsel to the Minority; Alan Edelman, Counsel to the Minority; R. Mark Webster, Investigator to the Minority; Jim Christy, (AFOSI Detailee); Mary Robertson, Assistant Chief Clerk to the Minority; Harold Damelin, Chief Counsel to the Majority; Carla Martin, Chief Clerk; Mary Ailes, Staff Assistant; Deborah McMahon, Investigator; Mark Foreman (Senator Stevens); Leonard Weiss (Senator Glenn); David Plocher (Senator Glenn); Shannon Stuart (Senator Cohen); Claudia McMurray (Senator Thompson); Sandra Bruce (Senator Levin); Elise Bean (Senator Levin); Jeff Barlon (Senator Levin); Nina Bang Jensen (Senator Lieberman); Max Della Pia (Senator Levin); and Jeremy Bates (Senator Dorgan).

OPENING STATEMENT OF SENATOR NUNN

Senator NUNN. Senator Roth is in the Finance Committee this morning and has asked me to go ahead and begin. He has submitted a prepared statement for the record.

[The prepared statement of Senator Roth follows:]

PREPARED STATEMENT OF SENATOR ROTH, CHAIRMAN

This morning the Subcommittee will continue its hearings on security in cyberspace. While computer security has been a matter of concern both to me and to this Subcommittee for some time, our society's increasing reliance on computers and widespread use of the Internet makes this issue now more important than ever.

Today, just about everything from telephones to transportation, utilities, and even our financial system, depends upon computers. Families, academics, governments, and companies rely on computer networks to help them carry out their daily business. With millions of Internet sites now available, people around the world can exchange ideas and information as through they were right next door.

Unfortunately, in this interconnected information web we have woven, we have seen an increase in the number of unauthorized intruders into our computer networks. Who are these intruders; how do they break in; and how can they be stopped? These are just some of the questions we hope to get answers to over the course of these hearings.

Computer system attacks involving "spoofing," "hacking," or "cracking," are not figments of fiction writers' imagination. This morning, we will hear from information security experts that computer break-ins pose a very real and serious problem to government and businesses alike. In fact, a recent study conducted by the Computer Security Institute reflects that concern. Of the public and private organizations who responded, 42 percent had experienced some kind of intrusion within the past 12 months. The good news, the experts say, is that by reporting computer intrusions, implementing solid security practices, identifying, and patching security holes, we can help cut down on these kinds of potentially damaging incidents in the future.

Since the trend is to put more and more important data, such as medical and financial records, on-line, we must ensure that we are prepared to protect this valuable information. By assessing our risk today, we can take steps to prevent a major and expensive loss tomorrow.

I would like to thank my distinguished colleague Senator Nunn for examining this important issue and the Minority staff for their work on this hearing.

Senator NUNN. Today, the Permanent Subcommittee on Investigations continues our examination of the security of our national information infrastructure. As advances in computer technology continue with blinding speed, this information infrastructure has come to form the foundation upon which many of the critical aspects of our society increasingly depend.

In our first hearing, we focused on the Department of Defense's information systems. The Defense Department runs a vast network of unclassified computer systems which support such critical Defense missions as troop movement, operational plans, procurement, and weapons systems maintenance.

In a report prepared for the Subcommittee, the General Accounting Office found that the Department's unclassified network is increasingly vulnerable to attack. As many as 250,000 attacks are carried out against the Department's system every year using tools and techniques available to millions of Internet users worldwide and as many as 65 percent of these attacks are likely successful.

Of even more concern, we learned the Defense Department lacks uniform policies for protecting its network, responding to incidents and assessing the risk of and damage from such computer attacks.

This morning, we will focus on our non-defense governmental systems and key components of our private sector. In the broad sense, our national security depends as much on these components as it does on our Defense sector. How would our society function without energy, communications, transportation, and financial computer systems?

As we will hear from today's witnesses, these systems rely heavily on information networks in their day-to-day operations. How vulnerable are these network information systems? Could a computer-based attack cripple them or erode consumer confidence in their services? These are some of the issues we will explore with our witnesses this morning.

Unfortunately, the statistics in this area are not encouraging. A survey of corporations, financial institutions, governmental agencies, universities, and health care institutions conducted jointly by the Computer Security Institute and the FBI reveal that 42 percent of those responding stated they had experienced some form of intrusion or other unauthorized use of computer systems within the previous 12 months. Over 15 percent of these attacks involved the unauthorized altering of data. Again, perhaps of most concern, over 50 percent of those responding stated they did not have a written policy on how to deal with these kinds of network intrusions.

Just how important are these statistics in terms of actual impact and potential impact? While the total picture is unclear, we will hear today that a group of computer security companies estimated the losses among their clients alone—this is just a small sampling—was over \$800 million worldwide as a result of computer intrusions, primarily in the financial industry. Of that number, however, only a small fraction was ever reported to Federal law enforcement authorities.

Indeed, what is most disturbing about this issue is what we do not know. We will hear from the Subcommittee staff today that when it comes to computer security, the intelligence community has few analysts dedicated to data analysis and inadequate resources devoted to collection and processing of intelligence information.

The law enforcement community has been similarly unable to provide reliable threat assessment in this area, probably because so little is ever reported by the private sector to the law enforcement community. According to the CSI/FBI survey, only 17 percent of those responding to this survey indicated that they would advise law enforcement if they were, indeed, attacked.

The reluctance of private industry to share information regarding system vulnerabilities and threats is perhaps epitomized by the fact that two witnesses who were scheduled to appear here this morning and who we had already served notice that would appear have cancelled at the last moment. Mark Rasch and Henry Kluepfel, senior representatives from SAIC, and they had been talking to our staff and had been cooperating—this is a private company which, among other things, provides information systems security services—they were scheduled to testify this morning about threats to the financial and telecommunications industry.

On the eve of this hearing, that is, yesterday, SAIC representatives informed the Subcommittee that these witnesses would not testify because SAIC's clients demanded the company not discuss these issues, even generally, in a public forum, this despite the fact the Subcommittee had advised SAIC that it would not ask company representatives to reveal client identities or any proprietary information.

I understand the position SAIC is vis-a-vis its clients, but I regret that members of the corporate community have taken the position that information regarding the vulnerability of critical parts of our Nation's infrastructure cannot be shared with the Congress. This is a short-sighted approach by the private sector which I think may cause them more severe problems in the future. Without reliable threat assessment data, we can neither conduct meaningful risk management nor structure a coherent national response to this issue.

This is one area we cannot afford to continue to be in the dark on. Too many parts of our society have come to rely on information infrastructure for us to remain ignorant of the extent of our vulnerabilities and the nature of the threats that are facing us.

In this regard, I am pleased to note the efforts of the Critical Information Working Group headed by the Attorney General and chaired by the Deputy Attorney General Jamie Gorelick. In future hearings, we will be hearing from some of the principals of this working group as to their efforts to formulate both a short-term and long-term response to the cyber threat. I hope that today's hearings and those which follow will help to raise the level of awareness not only among the members of the Senate but among the public at large as to the crucial implications of this new information age. It is only then that we can begin to confront the challenges we face.

Senator Glenn?

OPENING STATEMENT OF SENATOR GLENN

Senator GLENN. Thank you, Mr. Chairman.

I have a couple of remarks. I concur completely with Senator Nunn's remarks. I am very happy to join with him in continuing these hearings on information security. I am going to be in and out during the hearing this morning, but I did want to be here to help open this, anyway.

The stakes are very high, as Senator Nunn said, extremely high, and it is not just in DOD, it is not just about someone getting into missile controls and command systems and things like that. Our government and the economy depend more and more on computers and telecommunications.

We all talk a lot about the information superhighway and how great it is and how our kids are getting this stuff in the first, second, third, and fourth grade and can run rings around most of the rest of us on computers, as I know from personal experience with two grandsons, 13 and 11. I cannot even keep up with them on the computer, not by a longshot.

So it is a problem that is going to be greater, and it is not just theoretical. About a year ago, we had a Russian hacker who, with his computer, as I recall the press reports, transferred \$1.5 million or something like that out of accounts here. Part of the accounts were transferred to his account in Switzerland and others to an account in California by this one hacker.

So this is not something that is just a minor concern. As has been indicated by what Senator Nunn said a moment ago, most of our banks and some of our security people do not want to talk about this because it means a reduced level of confidence in the bank itself. I know that from having talked to some of our leading bankers about this personally and about what they were doing in this area, because I have been concerned about this, along with Senator Nunn, Senator Lieberman, and others, for some time, and so I think these hearings are extremely important.

I look at this hearing as an extension of the DOD hearing for this reason: We are rapidly getting to the point where we could conduct warfare by computer by dumping the economy of a nation. I do not think that overstates it. If you had a bunch of professional hackers out there who got in the Merrill Lynch accounts, Federal Reserve accounts, your accounts, and all at once you get a notice from your bank your account is now zero and somebody just transferred everything you had to somebody else in San Francisco or in Europe or someplace, you can see what a mess this would be.

You multiply that by the fact that we are having computers with increased capacity and increased speed and you can see how you could set up several hundred thousand transfers like that except for the last step or two and just have them sitting there and when you decide you are going to bring down a country's economy, you hit the right buttons and all these accounts go screwy all at one time. You have just wrecked the economy of a country.

So there is a bright side to the computer age and there is a dark side to the computer age, also, as we become more dependent on computers. That is the reason I think these hearings are so important. These hearings will form the basis of whatever actions are needed to make sure we have some means of information security for the future. There is no more important issue than this.

Thank you, Mr. Chairman.

Senator NUNN. Thank you, Senator Glenn.

I am going to ask this question to the staff a little later on and see if they can respond to it, as to the accuracy of whether they have come across any of this, but just this Sunday in the London Times, and I know nothing about this except it has been reported publicly in the London Times, the first paragraph of a story says, "City of London financial institutions have paid huge sums to international gangs of sophisticated cyber terrorists who have amassed up to 400 million pounds worldwide by threatening to wipe out computer systems."

It goes on, and I will get into it a little more in the hearing, but that is just right on point, Senator Glenn, of what you are talking about. To have this at least being widely reported and to have computer hackers all over the world who know how to do this and get into these systems and then to have the private sector basically be afraid to come up and explain it to the government, it seems to me, borders on being incredible. How are we going to deal with it if we cannot even get a grasp on it, if we do not have the data, if we do not have reports?

The private sector will not even let people who understand this area and are experts and who want to cooperate, like SAIC—they wanted to cooperate—they will not even let them come to testify. You talk about putting your head in the sand. It seems to me it is absurd.

Senator Lieberman?

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. Thank you, Mr. Chairman.

That is exactly the metaphor I was going to use, which was the "head in the sand," in the sense that everybody can see the rest of you but you think you are deceiving people by putting your head in the sand and that is exactly what is going on here.

I came here to learn this morning. I thank you very much for convening these hearings. Obviously, we are into a new world. The computer chip has defined and is defining so many extraordinary opportunities that we did not have before, but it is also opening up new possibilities for danger by the misuse of this capacity.

I was just thinking as we were talking about this, the pressure on these two witnesses not to come up, your reference to the news story. Somebody just sent me a novel, and I regret I cannot remember the name of it, but looking at the book jacket, the central theme of it—it is a spy adventure novel—

Senator NUNN. It was not written by Senator Cohen, was it?

Senator LIEBERMAN. It was not written by Senator Cohen unless it is a pseudonym. I do not know. [Laughter.] But the focus of it is that an act of terrorism occurs against the United States which is addressed directly to the financial computer network nerve center in New York. The book jacket says that though the site described is not the actual site, there is such a place in New York, etc.

So I do not know what the folks who pressed these two witnesses not to come think they are concealing, but it is in the newspapers, it is being written about in novels, and I know that our hope here is to make sure that fact does not follow fiction. Thank you.

Senator NUNN. I think this news article, if it indeed is fact, and I will read it in a few minutes, is pretty close to what you just laid out in that "novel", reporting this as fact.

Senator Levin, do you have any opening remarks?

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Mr. Chairman, I will put my opening statement in the record.

Yesterday, we had a demonstration in my office, and you were represented, and others, of just how easy it is to break into the DOD computer systems and how difficult it is to close all the windows that hackers manage to open in those systems. I want to thank you and your staff for making that demonstration possible. We will be going out to Virginia to watch an actual hands-on demonstration.

[The prepared statement of Senator Levin follows:]

PREPARED STATEMENT OF SENATOR LEVIN

The prior hearing on computer security examined the vulnerability of DOD computer systems to information warfare. Today's hearing examines the vulnerabilities of non-defense computer systems in both the public and private sectors. It is clear that the problems and the threat are significant and that we are not doing enough about them. I commend Sen. Nunn for raising awareness and pushing all of us to understand the issues.

Yesterday, I had a demonstration in my office of just how easy it is to break into DOD computer systems and how difficult it is to close all the windows that hackers manage to open in those systems. Since our computers can never be totally secure, the question becomes one of identifying and managing the risks.

One issue I hope is addressed today is the role that encryption plays in computer security. The National Research Council has called for lifting current export controls on encryption technology. I would like to hear how the experts here today analyze this issue from the perspective of computer security—whether such exports would enhance or harm our computer security overall, whether law enforcement and other government officials should be given special keys to unlock encrypted information, and what implications this issue has for the future of world-wide telecommunications.

Senator LEVIN. I will have some questions for these witnesses for the record, and I assume you will be keeping the record open for that, as well.

I am wondering if we are going to be asking questions of the witnesses who did not show up here today, whether they would be willing to answer questions for the record. Do we know whether that is possible or not?

Senator NUNN. They have already, interestingly enough, talked to staff, and so I think you are going to get some flavor from the staff this morning. We can discuss at what stage we go further with these potential witnesses. I am sure there are other witnesses out there. Perhaps the hearings will stimulate others to come forward that have similar expertise. We can always decide to issue subpoenas. We have not made that decision yet, mainly because we had been getting splendid cooperation from this particular group, and it is not the company itself, it is the clients.

Senator Glenn?

Senator GLENN. Just very briefly. It is not all doom and gloom. We have had some government people that are really working on some of these things. They have been concerned about this for some time, DOD and NSA, in particular. I was out there not too long ago and spent a day looking into some of the things they have been doing. They are doing a lot of work in this area and are very concerned about it, and doing a lot of very, very good work by my naive observation.

So there are things going on. It is not all doom and gloom, but it is a tough, tough problem and nobody has come up with one real good answer to it yet. I just wanted to add that comment.

Senator NUNN. This is a very tough problem and the offense is well ahead of the defense and it looks like that curve is going to remain for some time to come.

I spent the morning over there with the experts that were brought in, both offense and defense and so forth. Similarly, Senator Glenn, it is impressive what we have going on in DOD. We have a lot going on. As I mentioned, Jamie Gorelick and others are working, but one of the big missing dimensions now is whether we are going to get private sector cooperation or whether we are going to have a disaster first and then the private sector comes running up saying, as usual, why did the government not solve it? If we are going to get in front of this situation before the disasters start occurring, timing is crucial.

Senator LEVIN. Mr. Chairman, could I, on the question of the government role, just ask you a question, whether or not the issue of the export controls on encryption capability is going to be a subject for this hearing or a later hearing?

Senator NUNN. We are on the borders of that. We have gotten into it. Since that is in itself a whole controversial area, we wanted to kind of block that off and treat it as part of this but separately. We have not gotten into it to the extent of having a hearing per se on that. But the answer is, does it apply to this area? Yes, definitely. It is going to apply even more in the future.

Our witnesses this morning will be Dan Gelber, the Subcommittee's Chief Counsel and Staff Director to the minority, and Jim Christy.

Senator GLENN. Jim Christy is one of our experts out there. He is in the Air Force and he is detailed to the Subcommittee staff from the Air Force's Office of Special Investigations and has probably been as involved in this area for a period of time as anybody in our U.S. Government, so we are glad to have him.

Senator NUNN. Additionally, we welcome back Jack Brock, Director of the General Accounting Office Defense Information and Financial Management Systems, and Keith Rhodes, GAO's Technical Assistant Director at the Office of the Chief Scientist. We appreciate both of them being here. They did an excellent job when they testified before and they are going to be giving us some real live examples, I think, of how this situation works this morning, so we appreciate you being here.

Mr. Gelber and Mr. Christy are here to discuss the results of the Subcommittee's 8-month investigation into the vulnerabilities of our national information infrastructure. Mr. Brock and Mr. Rhodes are here to discuss the hacker threat and their expertise on information security. Of course, they have already testified.

I will ask all of you if you will stand and take the oath. We give the oath to all witnesses before the Subcommittee.

Do you swear the evidence you give before the Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. GELBER. I do.

Mr. CHRISTY. I do.

Mr. BROCK. I do.

Mr. RHODES. I do.

Senator NUNN. Thank you.

Mr. Gelber, I think you are going to lead off and kind of direct the traffic here this morning.

Mr. GELBER. Yes, I am, Senator.

Senator NUNN. I believe this is your first time under oath in front of the Subcommittee as a witness, but you are very familiar with that, having come through all of the hearings before and led the way for a while, so we are glad to have you formally testify in a position where you will tell the truth, the whole truth, and nothing but the truth. [Laughter.]

TESTIMONY OF DANIEL S. GELBER,¹ CHIEF COUNSEL (MINOR-ITY), AND JIM CHRISTY,¹ INVESTIGATOR (MINORITY), PER-MANENT SUBCOMMITTEE ON INVESTIGATIONS, COMMITTEE ON GOVERNMENTAL AFFAIRS, U.S. SENATE

Mr. GELBER. Thank you, Senator.

Senators first, if I could clarify as to the change in our schedule here today from Mr. Rasch and Mr. Kluepfel. Mr. Rash was an expert in the financial community. Mr. Kluepfel was an expert in the telecommunications community. They are with Science Applications International Corporation. We had asked them to testify and they at all times were very able and willing to testify and we met with them on a few occasions to talk generally about what is going on in the financial and the telecommunications world insofar as computer hacking goes.

They did ask, and we did provide, an assurance that we would not go into anything that would reveal client confidentialities and we sent them a letter. I received, as Senator Nunn said a moment ago, a letter from their Corporate Counsel yesterday indicating that they had received great pressures from clients. The Corporate Counsel indicated to me that it was a visceral reaction and that even though we offered additional assurances that we would not go into client identities, they said that that would not do any good.

¹The prepared staff statement of Mr. Gelber and Mr. Christy appears on page 225.

I would ask at this time, Senator Nunn, if the two letters,¹ both from the Corporate Counsel to myself and mine a week earlier, be made part of the record.

Senator NUNN. Without objection.

Mr. GELBER. Senators, the computer age has arrived with great promise and expectation. Just 4 years ago, the Internet hosted one million users. Today, that number exceeds 58 million and it is increasing at a rate of 183 percent per year. Advances in computing and networking have affected virtually every aspect of our society, including civilian, government, the military, communications, transportation, and commerce. But, as Senator Glenn mentioned a moment ago, the age has brought with it great vulnerabilities and weaknesses.

Our hearing and our statement here today focuses on the most critical pieces of our national information infrastructure and how and whether they are secure and reliable. Approximately 8 months ago, Senator Nunn directed the Subcommittee staff to begin this investigation, at which point we began to interview experts in the government, experts in the private industry, international experts to discuss this issue and get their thoughts. Our conclusions, which are set forth throughout this report, can be summarized in brief as follows.

First, our Nation has created a critical information infrastructure that supports our most essential functions.

Second, it is increasingly vulnerable to computer attacks from a variety of bad actors, including foreign states, subnational groups, criminals, and vandals. Anecdotal evidence already documents that these adversaries are organized and already exploiting these vulnerabilities.

The technology that these people use, that these adversaries use, is becoming much more available and much more user-friendly. Vulnerabilities in hardware and software are giving hackers, no matter their motive, great opportunities.

Computer hackers, because of the nature of the crime, can take different routes, circuitous routes, that cross boundaries, that cross different computer systems, and as a result, this presents very novel and difficult legal issues and jurisdictional issues with which our government has to somehow navigate.

Our government and our private industry's inability to foster a culture that promotes computer security is perhaps one of the great problems in this area.

Furthermore scoping the threat is another great problem. Our government, because the intelligence community has failed to dedicate sufficient resources to this, has not yet been able to come up with what would be called a reliable threat assessment or threat estimate. The private sector, similarly, including the commercial and the financial world, has been unwilling to report their own vulnerabilities for fear of inspiring customer insecurity.

As a result, enormous losses occur that escape the attention of the law enforcement and intelligence communities, and, indeed, our whole Nation in putting together a national plan. The government has only recently even recognized the potential severity of this

¹See Exhibit No. 36 which appears on page 605.

problem and is now beginning to address its very serious ramifications to our national security.

Our Nation, the Subcommittee believes, is in need of a comprehensive strategy that addresses this vulnerability from a variety of different directions and we believe our failure to recognize this threat and respond with sufficient resources will have very severe consequences for our Nation's security as we become more connected and more dependent on our information infrastructure.

At this time, I am going to turn it over to my colleague, Mr. Christy, who will talk to you about what the National Information Infrastructure is and, indeed, the vulnerability of that information infrastructure.

Mr. CHRISTY. Good morning. The staff's investigation is focused on threats to the National Information Infrastructure, the NII,¹ and the potential impact of such threats on the U.S. infrastructure as a whole. In examining this issue, the staff adopted certain widely-accepted definitions.

The NII refers to the systems of advanced computer systems, databases, communications networks throughout the United States that make electronic information widely available and accessible. This includes the Internet, the public switched network, the cable, wireless, and satellite communications. The NII is merely a subset of what has become known as the Global Information Infrastructure, the GII.

References to the U.S. infrastructure includes those systems and facilities comprising identifiable institutions and industries that provide a continual flow of goods and services essential to Defense and the economy of the United States, the functioning of the government at all levels, and well-being of society as a whole. This includes telecommunications, energy, medical, transportation, financial systems, as well as the government operation and national defense.

Our society is extremely dependent on both the NII and GII at almost every level of our daily life, individual, commercial, and governmental. Consider the following: Much of the way money is accounted for, handled, and exchanged is now done on the NII. Salaries are directly deposited in bank accounts by electronic funds transfers. Automatic tellers, ATMs, deposit funds, withdraw funds, and make payments. When payment is made for merchandise with debit and credit cards, transactions are verified using the public switched network.

Much of our Nation's economy also depends on the NII. The vast majority of transactions conducted by banks and financial institutions are done via electronic funds transfer. Over \$2 trillion is sent in international wire transfers every day. In addition, most security transactions are conducted via computerized systems.

Health care is increasingly becoming dependent on electronic records as pharmacies and hospitals maintain computerized files containing their patients' medical records. Medical care is moving towards greater dependency on computer-based technologies. Hospitals are testing the viability of on-line remote diagnostics.

¹The chart of the National Information Infrastructure (NII) appears on page 275.

The civil aeronautics industry has relied upon computers to fly and land airplanes. Railway transportation is dependent upon computers to coordinate tracks and routes.

Within our national defense structure, over 95 percent of the military's communication utilize the public switched network. Many of the military's precision weapons depend on the Global Positioning Systems, GPS, for guidance. In addition, the military uses computerized systems to transmit data and information related to troop movements, procurement, maintenance, and supply.

troop movements, procurement, maintenance, and supply. In short, the U.S. infrastructure has increasingly come to rest on the pillars of the national Global Information Infrastructure. Should these pillars be weakened or shaken, many of the critical functions of our society could come crashing down or experience significant damage.

As dependent as society is today on the information infrastructure, that dependence will only grow in the years to come. For example, the electronic exchange of E-Mail messages is becoming so common that it is challenging other forms of communication, including facsimile, telex, and even the Postal Service.

In 1969, the forerunner of the Internet started with just four major systems on what was essentially a single network. Today, there are approximately 9.5 million hosts, or major computer systems networks. By the year 2000, the number of hosts is expected to reach over 100 million.

Senator NUNN. Mr. Christy, for those of us who are not as well informed as Senator Glenn's grandsons, would you please tell us what your definition of "host" is? What is the definition of host?

Mr. CHRISTY. Basically, a major network connected to the rest of the Internet. The Senate has a major network and would have a host that would connect to the rest of the Internet.

Senator NUNN. The host is a central unit. The Senate offices would not be hosts. They would be part of a network and the host would be the central control?

Mr. CHRISTY. Right.

Senator NUNN. How many of them are there now?

Mr. CHRISTY. About 9.5 million, sir.

Senator NUNN. What is the projection?

Mr. CHRISTY. One hundred million by the year 2000.

Senator NUNN. So in 4 years, we are going to go from 9 million to 100 million hosts?

Mr. CHRISTY. Exponential. As technology has given advanced means of creating, storing, and communicating information, it has also made the information more vulnerable. Consider the example of our armed forces. Our armed forces are the most technically advanced in the world. The Defense Information Infrastructure, the DII, operates in support of the military's war-fighting, intelligence, and business functions. The Department of Defense is extremely dependent upon computers to fly, fight, feed, and track our troops. The protection of these systems is, thus, essential to national security.

For example, computerized logistics systems that direct supplies to an appropriate post or base must in time of crisis or war get the right number of bullets or gas masks to the military installations that need them. If toothbrushes were to arrive instead of bullets, it would obviously have a dramatic effect on the military deployment, exercise, or action. Or, if a foreign enemy were able to track the movement of such supplies, strategic decisions would lose their confidentiality.

What is true for our armed forces is also true for other parts of our government and the private sector. Identifying and addressing vulnerabilities is critical. What, then, are the major vulnerabilities of our information infrastructure?

The staff has observed vulnerabilities in three major areas: (1) software and hardware weaknesses; (2) human weaknesses; and (3) the lack of a security culture. Each of these vulnerabilities can be exploited to allow intruders unauthorized access to our information systems, leaving information or those systems subject to threat, theft, manipulation, or other forms of attack.

Hardware and software—hardware is basically the computer equipment and software is the programs that control them—hardware and software flaws and weaknesses arise from the basic assumption of product developers that all users can be trusted. Rarely is security a major consideration in the research and development of an information system.

In addition, the pressure of competition forces companies to field applications as quickly as possible, often without the benefits of comprehensive testing for inherent flaws. The industry relies on the user to report product flaws. In turn, the industry will either fix the flaw or release a new version of the product. Of course, the new version may also have a new flaw.

Hackers exploit these inherent flaws and are able to globally disseminate these techniques. The hackers are much better organized and share information about specific vulnerabilities regularly. There are forums for hackers that include physical meetings as well as electronic meetings. Hackers publish glossy magazines where they share vulnerabilities and techniques and trade war stories about their individual attacks. Phrack Magazine, on-line since about 1985, is one of the most popular of these hacker magazines, providing information to the hacker underground on information about different computer operating systems, network, and telephone systems.

Technology has made it much easier for hackers to exploit hardware and software flaws. In the early 1980's, only very technically competent individuals had the expertise to break into a computer system. Not only were there fewer hackers in those days, there were fewer targets. This has changed dramatically in the past 2 years. The proliferation of computers has created a new universe of targets in the government, the military, and the private industry. Much more of the population has access to computers at work and at home.

The vast majority of the people that buy computers today have bundled software packages that give them Internet access. Similarly, more people today have the capability to develop hacker tools than 15 years ago. Colleges, universities, and technical schools graduate tens of thousands of computer experts yearly, many of whom are highly trained in methods to secure and exploit software programs. A small percentage, but, nevertheless, a significant number, of these people can and are developing tools and techniques to break into the computers and networks of others.

Unfortunately, while the hacker tools are becoming more and more sophisticated, they are becoming more and more user friendly, requiring little expertise to operate. Point-and-click technology called Graphical User Interface, or GUI, have given everyone with a computer, a modem, and access to the Internet the capability to break into someone else's computer anywhere in the world.

For example, point-and-click software such as SATAN, which stands for Security Administrator Tool for Analyzing Networks, which was disseminated on the Internet in April of 1995, is a series of hacking tools that can be used by individuals with very little experience. SATAN scans systems to find network-related security problems and reports them, whether those vulnerabilities exist on a tested system, without actually exploiting them. Although SATAN was intended for systems administrators and security professionals to analyze their own systems for security vulnerabilities, potential intruders use this tool to identify and attack government and private networks.

These tools and techniques can be extremely effective. The Defense Information Systems Agency, DISA, has been performing proactive electronic "red teaming" of Department of Defense systems for over 3 years. DOD commanders can request and authorize DISA's team of computer security experts to attempt to electronically penetrate their systems. DISA experts will only attack a DOD computer system using attack tools or techniques that are already widely available on the Internet.

As of May 1996, DISA was able to electronically compromise 65 percent of the systems they attacked using commonly available tools. What that means is that only 35 percent of our DOD unclassified infrastructure is secure. DISA officials have told the staff that 65 percent figure is really a conservative figure. The figure is a result of an average one-week dedicated attack against a particular network. These officials report that if they are given more time to attack a targeted network, they could probably compromise upwards of 95 to 98 percent of the systems.

Another potential vulnerability-----

Senator NUNN. And the 95 percent would still be using only those tools that are available on the Internet?

Mr. CHRISTY. Yes, sir.

Senator NUNN. Not more sophisticated tools?

Mr. CHRISTY. Yes, sir, the same tools.

Another potential vulnerability in terms of software is in the use of commercial off-the-shelf software, COTS. Ten years ago, software was developed specifically for the government and generally by the government. The government owned the programming code that ran the applications. The government also knew what was in the code. The government knew what the code was supposed to do and exactly what it did. If the government needed changes to the code, they would make the changes themselves or hire a contractor.

In today's environment, it is much different. The government no longer has very many mainframe computer systems that require specialized computer code and it is much more cost effective to buy off-the-shelf computer hardware and off-the-shelf computer software packages. The problem with commercial off-the-shelf software is that the software programming source code is proprietary and usually a trade secret that the government cannot examine. The government only purchases a license to use that commercial software.

The purchaser knows what they want to use the software for and may not know everything the software can do. Software packages can include features that are possibly undocumented and potentially unwanted. The typical user is completely dependent on what the vendor provides. As long as the software does what it is intended to do, it is not questioned. What if the software purchased off the shelf contained a bug that was to be triggered on a certain date and was programmed to change or destroy a system's database? Would government or business be able to recover from the information loss? This, unfortunately, is the great unknown that comes with commercial off-the-shelf software.

The human factor—perhaps the biggest source of information systems vulnerabilities are the people who use and manage computer systems and networks. The proliferation of computers and their ever-increasing ease of use has put incredibly sophisticated systems containing very valuable information under the control of millions of people who do not yet grasp the need to maintain security or the consequences of a breach of security.

One such example involves the case of a U.S. Air Force pilot that was shot down over Bosnia. After he was recovered, one of his fighter pilot colleagues went on line with a very detailed version of the actual recovery of the downed pilot. Much of the information provided in the open Internet forum was at least very sensitive. Literally tens of thousands of copies of this fighter pilot's E-Mail was read and forwarded to others, including the news media.

Based on interviews conducted by the staff with computer security experts from the private sector, the problem is generally the same outside of the government, as well. Computer security personnel in the private sector generally do not have a strong voice in the corporate and management decisions. In the private sector, the computer security experts are usually at odds with the business leaders of their companies. Generally, the computer security function is buried in the administrative computer support area of the business. The pressure to automate and connect systems almost always takes precedence over the need to protect.

The staff's own review of a number of Federal agencies confirm many of these vulnerabilities. For example, the staff requested from various agencies the name of the individual or the office in charge of computer security. Most agencies responded that they did not know who that individual was, or they did not know if such a position even existed, or the position was spread over numerous departments.

The lack of clear authority for computer security was particularly acute at the State Department. A recent Inspector General audit of the State Department's unclassified mainframe security systems found that the Department basically had no security plan.¹ As a result, the Inspector General found that the Department was not in

¹See Exhibit No. 7.b. which appears on page 490.

a position to even reliably know if information was compromised. The Inspector General also found that the lack of senior management's involvement in addressing authority, responsibility, and accountability and policy for computer security had resulted in incomplete and unreliable security administration.

Senator NUNN. That is the State Department Inspector General, is that right?

Mr. CHRISTY. Their own Inspector General, Senator.

In the Hollywood movie "The Net", a hacker electronically breaks into Bethesda Naval Medical Center's computer network to access the Secretary of Defense's medical records and change them to reflect that the Secretary was HIV-positive.

The staff contacted a senior Bethesda Naval officer to address the BNMC's actual vulnerability. That official indicated that although some of the management personnel did not see a great priority in securing the center's medical files because they could not imagine that anybody would want to break in, they tasked to have an assessment of their computer systems performed and found that they were extremely vulnerable to almost anybody. Since that time, Bethesda has aggressively and proactively addressed those vulnerabilities to those records.

The staff also interviewed officials with the FAA, who stated that they were quite confident that their system was relatively safe from intrusions. This is not, they explained, because they have instituted healthy security programs. Rather, they indicated it was because their aircraft control systems are so antiquated and consist of so many separate and incompatible systems, they are more resistant to modern hacking tools. Further, because the current system, especially power sources, are unreliable, air traffic controllers are prepared to work without computers.

Once the FAA upgrades systems, they will be more vulnerable, first, because the operating systems will be compatible with most other computer systems, including those that the hackers like, and second, because controllers may become unaccustomed to providing guidance without computer support.

The pressure to connect was commonly mentioned by security personnel within the government as a great concern and challenge for the future. Various of these professionals were very troubled, not by the current vulnerability but anticipated vulnerabilities that come with greater connection to the Internet and other networks.

At this time, I would like to turn it over to Jack Brock from GAO.

Senator NUNN. Mr. Brock, we are glad to have you back.

TESTIMONY OF JACK L. BROCK, JR.,¹ DIRECTOR, DEFENSE IN-FORMATION AND FINANCIAL MANAGEMENT SYSTEMS; AND KEITH A. RHODES,¹ TECHNICAL ASSISTANT DIRECTOR, OF-FICE OF THE CHIEF SCIENTIST, U.S. GENERAL ACCOUNTING OFFICE

Mr. BROCK. Thank you, Senator.

Last week, we appeared before your Subcommittee and I think the good news we told you was that the Department of Defense

¹The combined prepared statement of Mr. Brock and Mr. Rhodes appears on page 276.

probably had better computer security awareness than any other Federal agency. Then, of course, the bad news was that it was not very good.

I think we have heard from Mr. Gelber and Mr. Christy this morning that this is a threat that extends far beyond the Department of Defense. It is a serious threat and has severe ramifications not only for the security of the country but also for the integrity of much of our financial and trade data, as well. We have been discussing with the Subcommittee staff avenues for further investigation, as well, which we will be pursuing later on.

So, computer security is a big problem. As mentioned before, we have new systems, new technology that make us more vulnerable and accessible to whole groups of people that never had access to this information before.

I am going to turn the presentation over to Keith Rhodes, our Technical Assistant Director. He is going to go over some hacking techniques. These are techniques that are available over the Internet. Keith told me just a few minutes ago that he spent an hour and a half doing the research on this. Keith is an experienced user on the Internet, so once you learn how to turn on the machine, access the Internet, maybe it would take you or I 2 hours to download these techniques. We are not talking about rocket science. We are talking about things that many people can do, that many people have access to.

Without any further remarks, I would like to turn it over to Keith, who is going to go through a brief overview of hacking techniques.

Senator NUNN. Mr. Rhodes, we are glad to have you back.

Mr. RHODES. Senator Nunn, Senator Glenn, and Senator Lieberman, I appreciate being asked back.

Yes, it did take me only an hour and a half to search this, but one of the assumptions I made was that, in reality, I was, as Senator Glenn described, an 11-year-old or a 13-year-old that had no prior knowledge about hacking and just had a basic computer literacy and a knowledge of the network itself.¹ (*Slide 1*) So the point of the briefing today is to not execute an actual break-in but is to explain how easily the tools can be accessed and what level of sophistication the user needs in order to get to these sites and download the tools.

As I begin, here I am at my home in the D.C. area. (*Slide 2*) Where do I need to go and how can I find out where I need to go? Where to start? I can ask the network itself. There are many search engines on the network that know where computer sites are, know where Internet nodes are, know where web sites are. (*Slide* 3) What I did was a preliminary single word and dual-word query on the alta vista query. (*Slide 4*) I put in the word "hacking" and I got greater than 20,000 responses. I made a simple 2-word query, "password cracking", and I got 20,000 responses.

What does a response look like? For example, the two responses that I have here are alt.2600. (*Slide 5*) That is a user group, a USENET newsgroup which is on the Internet that supports the readers of 2600 Magazine, which is a hacker quarterly, one of the

¹Slides 1 thru 45 appear on pages 283-305.

glossy magazines that Jim Christy was talking about. The alt.2600 survival guide, the purpose of this guide is to help you fit into the newsgroup so that you do not get reverse-hacked by the people that you are trying to get information from.

All I would have to do is move the cursor down to this particular site, for example, click on it, and I would immediately be sent by the network to the web page that has that particular file on it. This is just a representative site. It is not necessarily the site where the file is.

But in this case, you go to a site called the Internet Underground. (*Slide 6*) On the Internet Underground, you get the standard disclaimer that says, we are making this data available for information purposes only. (*Slide 7*) We do not want you to use it. We do not think you should use it. But, of course, people do use it.

Go through another set of files that are-

Senator NUNN. Put that last one back up there. Think of this as a guide of what not to do.

Mr. RHODES. Right.

Senator NUNN. If you are not going to do something, why do you need to know how?

Mr. RHODES. That is a very good question, Senator. It is giving me a step for how not to bake a cake, but I am going to bake the cake.

I go into the Internet Underground and I see the FAQ's, the frequently asked questions. (*Slide 8*) I take a look at the survival guide itself and it says, "Welcome to alt.2600." (*Slide 9*) We discussed telephony, which is phreaking, phone cracking, computers, hacking, and related topics. This is so you are not made a fool of or flamed by your associates. The last two lines, I highlighted. "Alt.2600 readers pride themselves on being hackers. Hackers seek out information by every available means." That is what we will be going over today, is what are the means that are available to get this information.

The next part is info philes. (*Slide 10*) They spell it with a "ph" because they are mostly affecting how to break into a phone system. The first line is the boxing page. This is not about Carlos Monzon or Galindez or the great fighters. This is actually about how to build things called boxes. Boxes are devices that allow you to break into cable/video boxes or pay phones or regular telephone circuits. "Again, my intention is not to defraud or encourage people to defraud the phone company." (*Slide 11*) That is highlighted in there. We are still not baking the cake.

As you can see, there are quite a few kinds of boxes here. (*Slide* 12) We go all the way through. (*Slide* 13) I believe the count is 26. Some of them are used to, for example, send out the digital signals and tones to be dimes and quarters and nickels on pay phones and things like that.

Here is a specific description, just to give you an idea of the level of detail needed to modify a Radio Shack dialer to be a red box. (*Slide 14*) Buy part number this. Unscrew all the screws. Take out the crystal that has 3579 on it. Replace it with a specific crystal with this specific frequency on it. Replace the cover. You now have a red box. So we can definitely bake the cake from this recipe. Senator NUNN. What do you have when you have a red box? What is the bottom line of this?

Mr. RHODES. The bottom line on a red box is you can make a pay phone think that you are paying money when you are not. That is really the initial—

Senator NUNN. To beat the phone company.

Mr. RHODES. Right. That is what you are trying to do usually with the boxes.

Other publications, in this case, as Jim pointed out, Phrack is a very popular phone cracking association on the Internet. (*Slide 15*) I click on that. (*Slide 16*) I now go to Phrack. At Phrack, what do I find? I find a great many directors, the archives. (*Slide 17*) The archives here are groups on the net who post to this archive who have published documentation that tells you how to do things or where to go to find information or what conferences to go to or, again, mostly focusing on breaking the phone system, but they also point to other sites, as well. (*Slide 18*) As you see, the list goes on for quite a while. (*Slide 19*)

From that, I then can figure out how to go from my home into some public switch, not pay for it, go from that public switch to another phone switch and then out from there, in a sense, making it harder for somebody like Jim, a professional investigator, to trace me. That is the point, is to get free service and also make it harder for people to trace me back. (*Slide 20*)

Senator NUNN. Jim, at this point, do you want to comment on the difficulties from law enforcement with that rather simple chart up there right now, before you get into the 8 or 10 switches? If you are alerted and one of those is hitting an Air Force base after going through perhaps Europe or Asia or somewhere and coming back, what is the jurisdictional nightmare you run into just at that stage, between the FBI and what they can do and what our intelligence community can do and what our military can do?

Mr. CHRISTY. How much time do you have, Senator?

Senator NUNN. I just want you to give us a summary.

Mr. CHRISTY. First off, on the Internet, you are going to have to deal with each individual geographic jurisdiction, whether it is a county, a city, a State, or Federal. When dealing with multiple countries, you are going to have to deal with that country's law enforcement agency. They may have multiple carriers within that jurisdiction and you are going to have to get a court order for each and every one.

Senator NUNN. But do you not first of all decide which agency of the Federal Government can get into it, based on whether it is domestic or foreign?

Mr. CHRISTY. Yes, sir.

Senator NUNN. How do you decide that? That is the first roadblock, is it not?

Mr. CHRISTY. I would run this as a criminal investigation rather than a counterintelligence investigation, thereby not worrying about intelligence oversight because it is a criminal act that I am investigating. So I am going to deal with the criminal arms of each one of these law enforcement agencies as I follow it back, one step at a time. It is pretty time consuming, and as a prosecutor, and Dan, you may want to comment on how easy it is to get a wire tap or a pen register or a trap and trace order.

Mr. GELBER. Senators, as you all know, in order to actually get this stuff and to start surveilling it and to take it back one circuit, that is a Title III electronic intrusion that the government is doing, and therefore it has to go through all of the exact same minimization procedures and application procedures and get the approval of very high-ranking officials at the Department of Justice in order to even do that, and that is only in the last circuit.

If you think about doing that, as you would for an organized crime case, where you know where the phone is, in this kind of case, you do not even know where the next one is going to come from or whether it is even within a Federal district, which one it is in, or whether it is even in our Nation. It becomes a very vexing task to, even if you know what you are doing and where you are going, to get it done in a time that you can respond.

Mr. CHRISTY. And even when you get those orders, if the hacker changes his path, it is for naught. You lose that.

Mr. RHODES. Jim, stop me if I am getting too detailed here, but the type of switch that I go to is very important, also. If it is an automated switch, it is much easier—I retract. It is easier. It is not easy but it is easier for the law enforcement using the phone company to trace back.

But if I am going to a site in a country where the telecommunications infrastructure is more primitive, then the switch may actually be a physical switch that has rotors in it, an old-style switch, an old Western Electric 71 or something like that, where it is like a ratchet that actually turns and pots touch one another.

Now I need a human being at the switch to watch when they move, which Cliff Stoll encountered and Jim encountered in Hamburg. Because of the type of switch, they had to actually time it to have somebody there to watch the switch and see how the numbers were clicking up. It was not a remote thing that they could look at. So it does make it more difficult.

So now I have some finesse with attacking the phone system and now I go and get the SATAN package, which is a suite of, as they say, user-friendly attack tools exploiting rather common attack scenarios on Internet hosts. (*Slides 21 and 22*) This is a tool that represents the kind of standard tools that one would use to attack a net or to attack a node. This would be comparable to parts of any attack scenario.

Also, I can get a tool called rootkit, which is a series of Trojan horses. (*Slide 23*) The Trojan horse is a piece of software that looks like a standard piece of software but it actually does something else.

A couple of points that I have highlighted there, on the UNIX system. DU tells you what the disk usage is. LS lists the files. PS gives you a process table that tells you what processes are actually running on the computer. (*Slide 24*) With the Trojanized version of it, I will be invisible even to the correct system administrator who executes those commands. They will not be able to see me. Plus, I will have my own account on there that has system administrator privilege.

Senator NUNN. How did SATAN get on the Internet and when did it get on the Internet? Also, is there anything illegal about SATAN now? Does it cross any boundaries of law, as the law currently exists?

Mr. RHODES. I would have to defer to Dan and Jim about the legal issue, but how it got on the net was a programmer, Dan Farmer at Silicon Graphics, who was a security analyst there and put together a standard set of tools off of the Internet. He built some himself and put a nice user interface on it. Regardless what you may consider of your own computer literacy, if I put SATAN on your machine, I could turn you into a hacker. All you have to do is put in the computer address, move the mouse over, click on "go", and the attack begins.

Senator NUNN. Is SĂTAN being sold? Is somebody getting paid for the sale of SATAN?

Mr. RHODES. No. The copy that I have, I downloaded for free.

Senator NUNN. So what did the person that developed SATAN or the company that developed SATAN get out of it?

Mr. RHODES. Dan got fired. [Laughter.]

Senator GLENN. And you just got a bill sent to you for your downloading for free.

Mr. RHODES. Right. Exactly. The purpose behind the tool, the stated purpose behind the tool was, here is a tool that you can use to check the vulnerabilities of your own system, much in the way that a host or a site would use DISA to come in for a vulnerability assessment. Now you would be able to use SATAN and turn it on yourself and say, this is how I can exploit the vulnerabilities.

There is quite a bit of discusion continuing in the community about the value of SATAN because it now grants people with much less capability the ability to use powerful tools to go out and attack systems easily.

Senator NUNN. Two questions, Mr. Gelber, on this point. The first is, is having SATAN on the Internet in any way illegal? Then, second, is the use of SATAN by hackers illegal?

Mr. GELBER. Insofar as the first answer, 18 U.S.C. Section 1030 is the unauthorized computer intrusion statute. I do not know the answer to the first one directly, Senator, whether it being out there is illegal. I suspect the fact that it is simply out there is not, because most of our Federal statutes require some kind of criminal intent.

Now, the use of SATAN to create an unauthorized intrusion, I have no doubt, is illegal in a variety of different ways, depending upon the intent and the damage and the motive of the individual or individuals who are using it. That is a fairly new statute. If you would like more, certainly the Department of Justice has a unit dedicated just to this that helped forge this statute, but I have no doubt that the use of that tool, depending upon the intent of the user, is a crime.

Mr. CHRISTY. But only if it is trying to break into the system. If it is just gathering information on the system, that may not be illegal. Only if it tries to gain unauthorized entry, not if it is looking for vulnerabilities.

Senator NUNN. Right.

Mr. RHODES. Now that I have some of the tools involved, I now search another bulletin board and find that there are some active attack sites that I can utilize and I go to the Computer Underground Digest. (*Slide 25*) The Computer Underground Digest, again, is another site that has a great many directories. (*Slide 26– 29*) The one that I am going to pay attention to today is 40HEX. (*Slide 30*) 40HEX publishes "Spotlight on Viruses" and actually does include some of the source code for the viruses that you can then exploit and load onto somebody else's machine. (*Slides 31 and 32*)

Senator NUNN. Give us a definition of a virus now.

Mr. RHODES. A virus in the computer world is not unlike the virus in biology in that—

Senator NUNN. You put it in the system, it spreads and fouls everything up, is that right?

Mr. RHODES. Exactly. It implants itself into an active program and makes it do something.

Senator NUNN. Why would there be any legitimate use of a virus, or is there any legitimate use of a virus?

Mr. RHODES. The only legitimate use I guess you can see is that you are going to use the virus in order to figure out how to defend against the virus, but that is a circular argument if you have not actually invented the virus.

Senator NUNN. So this whole section you are dealing with right now, the 40HEX issue, basically is telling people how to foul up other people's computers?

Mr. RHODES. Exactly. To give you sort of an eclectic flavor for the Computer Underground Digest, there is a directory called "Boom" and what they talk about is making explosives. (*Slides 33 and 34*) So it is a wide range. These are very simple, a gasoline bomb and a sort of a Roman candle. But as you can see from the last line, "Dazzle your friends while burning off their eyelashes with this amazing rod." There is sort of a flippant attitude. But that just gives you an eclectic feel for what is out on the net.

The real point (Slide 35) behind all of this is that with an hour and a half and the computer literacy of Senator Glenn's grandchildren, I can now start up my home, (Slide 36) loop back on myself with the phone system, (Slide 37) go from there to some ancient switch in Northeast Africa, (Slide 37) down to Latin America, (Slide 39) up to Mexico, (Slide 40) out to perhaps Thailand, (Slide 41) then go into Europe. (Slide 42) In Europe, I launch my attack on the network. (Slide 43) Now, in black, I am on the net. From there, I launch an attack on, say, a university site in Florida, (Slide 44) go from there to the site I intend, which might be a DOD contractor in, say, Southern California, (Slide 45) and that is where I win.

If I ask Jim, how would he trace me back, I guess that would be a rather tough question.

Senator NUNN. Let us ask Jim that and let us ask Dan, at what stage in any of that—why do you not give us the final motive in terms of when you hit the final site there? What are you doing at that site?

Mr. RHODES. At that site, say it is a contractor site and I know something about that site. I know that there is a procurement involved or this is my competition. I want something on that node. The whole point is that I have gone this circuitous route and not launched my attack from the United States necessarily, or traceable to me in the United States, so that I can get to my West Coast competition and steal their proposal, or get to my West Coast competition and steal their research and development, or get to a DOD military site and then launch from the DOD sites into the rest of the DOD network.

Senator NUNN. Mr. Christy, let us say you get a call right there and something has happened. Without getting into great detail, just tell us sort of one, two, three, what your problems are, and then I am going to ask Mr. Gelber to tell us at what stage in that process there the perpetrator has done something illegal.

Mr. CHRISTY. Basically, Senator, that is an unsolvable case unless you have intelligence on who is doing it. It is a whole lot easier to set up a surveillance like we did in the Rome Labs case on the kid in the U.K. and watch him launch his attack. That is easy. To trace them back with the technology that is available and the investigative jurisdictions involved, that is an unsolvable case, because that hacker, if he is smart enough to take those kind of routes, he is only going to do that once or twice.

Even if I get the appropriate court orders, which is going to take months in all those different jurisdictions, he is going to change that route when I have my surveillance set up. So that is an unsolvable case without the intelligence community, both law enforcement and the foreign intelligence.

Senator NUNN. So we are reaching a point where if we do not get our intelligence community involved in something that may appear to be domestic, then it is not going to be solvable. Am I overreading this?

Mr. CHRISTY. No, sir. That is exactly right. We have to merge the law enforcement and intelligence communities' collections.

Senator NUNN. This is a legal and a cultural change for us in this country. I think everybody ought to understand that. That does not mean you solve it easily if you do that, but we really, if we are going to deal with this kind of world, we are either going to have to have our present intelligence community or we are going to have to form some other whole group and duplicate some of that capability in order to link law enforcement with intelligence. Is that fair to say?

Mr. GELBER. Senator, you do not even know whether the motive here is to steal something for espionage, which is a crime, or a national security motive, or to find some intelligence information. So then it is even difficult to task it.

This is a very good example. As far as your question as to what is a crime here, I suspect that because that person looks to be like he started in Washington, D.C., is here, it is probably a crime here. And all along the way, everything that he does there is probably a crime here.

The greater problem, however, is if it is somebody elsewhere. For instance, the Department of Justice just a few months ago indicted a 22-year-old Argentinean citizen for breaking into some DOD systems, launching an attack, I believe, from Harvard University. Senator NUNN. In other words, the perpetrator was physically in Argentina—

Mr. GELBER. He was in Argentina.

Senator NUNN [continuing]. But the attack came from Harvard University?

Mr. GELBER. That is right. Now, they got a court-ordered nonconsensual—the first time they got a court-ordered non-consensual Title III surveillance, at which point they now were able to determine where this person was coming from. They basically did solve that case. It was, I would consider, a very incompetent attacker. I think the experts I consulted agreed with that, and that is probably why they caught him.

But what is interesting is they indicted him and it was a very long press release from the Department of Justice. Unfortunately, at the end, it was very clear from reading it, and we have checked on it, that the day after this happened, that 22-year-old likely could have continued doing exactly what he was doing the day before, because in Argentina, it was not a crime.

So when you talk about the way in which we are assembled to deal with this problem, that is a pretty good example. We solved that one, luckily, but even the day after, other than taking his computer, that young man could have continued doing exactly what he did from a different university and was not violating the laws of a foreign country. There is a lookout for him with Interpol, so now his travel is limited, perhaps, for the rest of his life, but beyond that our government was really not able to deal with that in any meaningful way, even when it got lucky.

Mr. RHODES. That concludes the presentation.

Senator NUNN. What is the good news out of all of this?

Mr. GELBER. I am about to get actually into what I thought was going to be the bad news, sir. [Laughter.]

I was going to talk about the threat at this point, because we have a section in our staff statement where we talk about what this threat actually is. It is a very difficult thing to do because the first thing we observed was nobody has really scoped this threat out. It is just something that is very difficult, because the intelligence community has not been able to collect data from it and the business and financial communities, as we have talked slightly about, have been unable, or unwilling, actually, to come forward and send this into what would be our national data base.

Most of the documented incidents which we have seen deal with the least competent attacker. That seems to be everybody's agreement, that we are catching the bottom of the food chain and that we are really not that able to deal with what would be a sophisticated structured and funded attack which would come from an organized subnational group or a foreign nation or an organized criminal organization.

The first thing we looked at was the intelligence community, and recently, the Brown Commission report on the roles and capabilities of the U.S. intelligence community issued, I think, a top-to-bottom look at that community that came out this year. In that report, which I think is a very thorough report, there is a paragraph about collection of information security. It says in that paragraph: "While a great deal of activity is apparent, it does not appear well coordinated or responsive to an overall strategy."

I think the Brown Commission was being rather polite. One senior member of the intelligence community responsible for collection of this data compared it, I think better, to "a toddlers' soccer game, where everyone is sort of just running around trying to kick the ball somewhere but not really knowing where the ball is supposed to go."

We found that. We went to briefings from all these intelligence agencies, counterintelligence agencies and we asked them, is this a problem? What is it? What are you doing about it? There was universal agreement, "this is an emerging problem," "this is a very important problem." Everybody said it was "substantial," and there were plenty of people at our briefings, but when pushed to reveal how many people were actually collecting information, how many people were actually doing things on this subject, it was usually just a handful.

We went over to the CIA and they have an information warfare center. At the time of the briefing—I know they intend to expand it—there were only a handful of people even working on this issue in terms of collecting the kind of data that we would hope they would be collecting on defensive info war, despite a lot of the emphasis placed on this.

There is a growing awareness, however, I think, in the intelligence community, we found, that this is something that is going to have to be done. There are a lot of working groups that are coming out. There is a lot of information warfare being put into preexisting offices.

But there has not been any real retraining of intelligence officers in sort of the technical aspects of this problem, which a lot of members of the intelligence community said is something that will hurt us later, as we find we do not have a dedicated, experienced, and well-trained pool of people able to help us on this subject. One very senior intelligence officer said, "Do not wait for the intelligence community to provide a threat estimate. It will probably take the intelligence community years to break the traditional paradigms and refocus resources on this important issue."

Of course, the Kyl amendment requested that the Director of the Central Intelligence Agency actually give a threat assessment to Congress. That was due this month, but it was an ambitious schedule and they have asked for an extension. When we asked what is going on there, someone confided in us anonymously that the problem is they are trying to put their hand in the box so they can give us the information that is in there to give us a threat assessment and there is just nothing in the box to begin with.

Senator NUNN. How much of an inhibition in the intelligence community goes back to the separation between the ability to operate in this country and the ability to operate abroad, based on both law and custom and on the whole culture? They have been excoriated for the last 25 or 30 years anytime they even get anywhere close to anything domestic. So how much of this gets into their basic vision or gets in the way of that basic ability to come to grips with it? Mr. GELBER. Quite a bit. The problem is that they are dealing with it in a geographical sense and it clearly occurs in a borderless world. One problem is, now that the intelligence community has at least, quite a bit of the intelligence community cannot do a lot of collection, obviously, domestically. A computer node, a terminal in the United States, even if it took that route that we saw a moment ago, if the last circuit is in the United States, it is a U.S. person, which immediately means that our intelligence community cannot do certain things, even if it comes from a foreign national, if you do not know that, which you do not. So it is very hard to task it.

That also means that the intelligence community has to rely on other things, like the law enforcement community or the private sector to send it the kind of data that it can use to form sort of an institutional data base that can grow. So the organization and these paradigms, I think, are a great obstacle to this.

Also an obstacle is the fact that there is no mandatory reporting, even in government. In the Department of Defense, some of the services do, but if you are intruded, and Mr. Christy will tell you this since his normal job is as head of their enforcement division on computer crime at the Air Force, he will tell you they do not have to come to us and tell us. There is no mandatory reporting.

In fact, in the Department of Defense, we heard from numerous places that some people are simply afraid because they think it reflects poorly upon them. That is a very difficult paradigm to break, when your most important source of information will not come forward and it is even your own employees and your own government agents. So that is a big problem.

A common theme expressed by all the experts we spoke to was that although the principals of these communities, the intelligence and the enforcement community and even in Defense, believe this is significant but there is still no blueprint. There is no national sort of strategy that might guide a national effort and let middlelevel managers in these agencies understand the priority. There has been quite a bit of rhetoric, and a lot of it, I believe, very sincere, but the problem is it is hard to move an organization this huge—some of these institutions have paradigms that have been literally existing for 200 years—and change their view of what the next threat is going to be and how they are going to deal with it.

The lack of reporting in the government might be a huge problem, but I think when you get to the private sector, you are getting into what is the most troubling problem. There is very little anecdotal data concerning the threat posed to the private sector and I think we are very convinced, as indicated by the absence of two witnesses on our next panel, that this is primarily due to the fear of the marketplace.

The most common theme among the commercial sector, it is simply loathe to report intrusions. It does not want to affect customer/ shareholder confidence. Company insiders confirm to the staff that they have experienced intrusions on a regular basis, but they fear reporting them to the government or any other agency that might ultimately report them into a public record. It is a very unusual paradigm that now exists in these companies. One of the premiere companies that provides security services, including countermeasures to intrusions to private companies—we call them cyber posses, that is what our staff has nicknamed them—explain the extent of this problem. This company informally surveyed a handful of other companies that do the exact same thing they do, informally and anonymously, using all the techniques that they have. They are in this field, so you can be sure that their communications were encrypted.

This small group of firms was able to account among their clients alone in the financial, mostly financial and commercial world, over \$800 million of losses last year alone. That figure included only actual losses reported by clients of either money or some sort of intellectual property. Over \$400 million of that was attributed to U.S. companies. These figures do not include losses that might come from loss of data or lost access or things like that, or even the cost of the investigation.

Senator NUNN. Let me at this point read from this London Times article that I alluded to. I am going to read you about three paragraphs and just get your comments on this.

The London Times this past Sunday, "City of London financial institutions have paid huge sums to international gangs of sophisticated cyber terrorists who have amassed up to 400 million pounds worldwide by threatening to wipe out computer systems. Banks, brokering firms, and investment houses in America have also secretly paid ransoms to prevent costly computer meltdown and a collapse in confidence among their customers, according to sources in Whitehall and Washington." Again, I am quoting from this paper.

"An inside investigation has established that British and American agencies are examining more than 40 attacks on financial institutions in New York, London, and other European banking centers since 1993. Victims have paid up to 13 million pounds at a time after the blackmailers demonstrated their ability to bring trading to a halt using advanced information warfare techniques learned from the military.

"According to the American National Security Agency, NSA, they have penetrated computer systems using logic bombs, coded devices that can be remotely detonated, electromagnetic pulses and highemission radio frequency guns which blow a devastating electronic wind through a computer system. They have also left encrypted threats at the high security levels reading, 'Now do you believe we can destroy your computers?'

"The authorities have been unable to stem the attacks, which are thought to originate from the United States. In most cases, victim banks have failed to notify the police. They have given into blackmail rather than risk a collapse in confidence in their security systems, said a security director at one blue chip merchant bank in the city. A senior detective in the City of London police said, 'We are aware of the extortion methods but the banking community has ways of dealing with it and rarely reports it to the police.'"

That is all from the London Times. Have you looked into that at all? Is this the kind of thing that appears to be already happening out there?

Mr. GELBER. Obviously, we cannot confirm the entire story in the *London Times*, but it is extremely consistent with exactly what company insiders and security firms told us.

Initially, actually, we were told that this sort of cottage industry started when a hacker might break into a company or a bank or somebody and then try to get hired by that bank to help them stop the intrusions, since they were wise enough to break in. It is not unlike the old protection rackets, perhaps, that this Committee is familiar with when they did previous organized crime hearings. You are protecting you from us.

One thing I would note, though, is that, of course, what we are looking at there are people who are operating out of greed and who convince an institution that is obviously profit-motivated that it can harm it, and that is that scenario.

I think a far more dangerous scenario is going to be one where it is not greed but either anarchy or national interest of a foreign government that is going to motivate somebody and create a scenario where they do not care whether they are paid. We are a Nation of soft targets, in many ways, and I think our information infrastructure has given us many more soft targets. The fact that these banks are willing to pay tells you that they believe that they are a soft target in some ways.

Despite these huge numbers that have come around, and I would stress that these are only estimations and we have not, Senators, in any way gone out and confirmed these numbers, but they are consistent with everyone we have talked to, and we have talked to a lot of different folks.

But despite this, there really have been very few reported intrusions. The Citibank case that Senator Glenn referred to, there was a couple million dollars moved around, and actually, after they caught the group that did this and they were indicted, approximately \$400,000 was actually lost in that case.

But there is a huge delta between what is being reported, what is being investigated, what is even being indicted and what we believe is going on, and I think that is a big concern. The disincentive for an institution to not report a loss is obvious. Customer confidence is a huge staple to anybody who is running a business.

One thing that was very interesting in the Citibank case, the staff was advised that after Citibank received publicity about it, Citibank's top 20 customers were immediately targeted by six of their competitors. The competitors argued that their banks were more secure than Citibank.

This, I think, is something that we are most concerned with in the cyber posses that are out there. We heard from innumerable of these security firms that security in the marketplace—it can be described this way. It is stop the bad guy and send him to your competitor. There is no great desire to see that this person is arrested, because, indeed, an arrest, a prosecution, will likely result in a public trial, which is the last thing that a bank or a financial institution or a business wants. On the other hand, if he goes to your competitor, then perhaps he might have to suffer those tragedies. So we heard it as a win-win-win from the private industry side of not reporting it, and that was of concern. Now, there are some reporting requirements and there are some very new reporting requirements that came out in April of 1996 on financial institutions, some of which are intended to include some of these things. Nothing yet has come in. We have checked with FINCEN, who is responsible for obtaining a lot of these suspicious activity reports, and nothing has come in yet. But, of course, it just started in April, so it is possible over the next year or two we may hear about more. But there is no doubt that there is a great amount of underreporting or nonreporting going on.

As one senior account representative with one of these security firms said, there is a lot of reporting requirements but there is reporting and then there is reporting. They explained the various methods. It is almost another cottage industry, of avoiding reporting by using the general counsel's office to run the investigation or by reporting it in a large bulk of other documents that make it very difficult, relying on the fact that the government regulators may not look at everything accurately. So there is a lot of that concern.

This has created a huge problem in terms of assessing the threat and where it is coming from because we do not have a baseline at this point. We just sort of define things by the very last example, and there are very few of those, so we do not get a good shape of what it is. We cannot, therefore, devote resources to it or make people believe it is a problem.

There is a problem. As reported by GAO and the National Security Agency in our last hearing, they believe that there are 120 countries developing offensive information war capabilities. This, of course, is a great equalizer, this business, because you do not need to be a nation to do it. All you need is a modem, an off-the-shelf computer, and the desire to do either damage or make some money.

One of the concerns that the staff had was that there is this rush to connect that is going on right now. The classified networks of our government have air space between them, for the most part. They cannot be intruded into by an outsider. They could not get into those classified networks.

However, there is a rush to connect those networks to themselves and that is a big concern, because what that has done is increased the number of trusted persons at each agency into those classified networks to very large numbers. Anybody, whether they have something to do with it, whether they do not, could potentially now have access to these areas, so that is a big concern and that is something we recognize as a problem.

As far as efforts to promote security, we will have some folks on the next panel who will talk about it. I would like to go over just one or two right now.

First and foremost, we believe there needs to be a national policy on this. There has to be a top-down approach to this problem, from the White House down to the principals of the agencies so that it is understood.

Now, there is an effort going on at the Department of Justice right now led by the Attorney General and the Deputy Attorney General. It is called the Critical Information Working Group and it was a product of PDD-39, unclassified version of that is attached to the staff statement, where the Attorney General is supposed to be looking at these infrastructure issues, physical and cyber. What they have done is come up with a few recommendations after the last 6 or 7 months of work. We have looked over those recommendations. They have not been released yet. But we include them in the staff statement because we think that they are a pretty good start at looking at this issue. They have come up with two basic recommendations. I will describe them to you now.

One is to create basically a task force within the Executive Office of the President to study infrastructure assurance issues and recommend national policy. This task force, according to the Justice Department, would be led by a Presidential appointee, and their hope is that it is from the private sector. It will be comprised of full-time representatives from a lot of different agencies in and out of government. Their job would be sort of the macro, to set policy and to begin a top-down look at this issue. They believe that it would take that organization, that task force approximately a year to do their job, although they perhaps could go longer.

In the meantime, recognizing all those issues that Mr. Christy and I and Senator Nunn and the other Senators have asked us, they want to set up an interim group also in the meantime to deal with these assessment issues. Right now, they have that agency in theory chaired by the FBI. The advantage of the FBI is that they have the real domestic terrorism physical side of the problem, so they would give them the cyber side, as well. That group, for the next at least year, would have some interim operational response so that they could help all the various agencies that are dealing with this, and there are a lot of efforts, but they lack direction, to somehow be better coordinated.

We looked at those groups and we have some recommendations that are in our conclusions that, I think, would request more of a robustness to the interim group, or at least to the ultimate group that is created. I will go over those in a moment.

I think there are also other things that can be done within a lot of these other agencies, as well as the private sector. We believe, for instance, the CERT program you are going to hear about later is probably one of the best models that are out there of what can be done in this area. The CERT is the Computer Emergency Response Team, and Mr. Pethia, who runs that program at Carnegie Mellon, will talk to you about what they are seeing.

Finally, as far as our recommendations, and I'll summarize them because it's approximately a 60-page report and I think you may have some questions and there are other witnesses—

Senator NUNN. Let us go down the recommendations one by one, because we need to come out of this with some sense of where we are going and what we can do about the problem.

Mr. GELBER. Recommendation No. 1, formulate a national policy to promote the security of the infrastructure. It is simple, it is broad, but that seems to be the most important thing and it needs to sustain a White House interest because, clearly, the biggest problem right now is that there is no security culture within government and there is no understanding of the issue outside of government and its security implications. So that is our first one.

The second one is that we create a national information infrastructure threat center that absolutely is a free-standing unit, not led by any single department but free-standing, recognizing that this thing is an organic, evolving problem and you need everybody from intelligence, enforcement, foreign and domestic, all parts of it, counterintelligence, so that when something comes in, it can be sent to the right group. It may not be an enforcement issue. It may be an intelligence issue. It may be a security issue. But it needs to have an actual responsive capability.

Senator NUNN. What is the difference between that and CERT? We are going to hear from the CERT witness in a few minutes, but what is the difference between that and what we have out there now?

Mr. GELBER. The CERT, as Mr. Pethia will tell you, it is government-supported but it is just a very small group that is set up to respond to intrusions anywhere. Actually, it is not unlike the CERT except the CERT has a very small budget and they will tell you they are so overextended that they cannot do any of this.

This would be to take government and give all the agencies and even representatives from the private sector an ability to look at this threat as it comes in, to operationally task it to whoever it needs to go to, and, at the same time, to start determining a baseline of what our threat estimate ought to be. This may be what the Justice Department group ultimately comes up with or the White House group ultimately comes up with.

Senator NUNN. Is CERT an alternative for private sector complaints where they do not want to report directly to the government and do not want publicity?

Mr. GELBER. Yes. Mr. Pethia, I am sure, will tell you that he does not report them. He is not supposed to. He advises them that they can and they ought to, I think he will probably say he rarely reads about them in the paper the next day, so they are probably not being reported. He will tell you how overextended they are, and it is quite amazing, the amount of work they do. As a matter of fact, I think their budget is being cut on their operational response to something like under \$1 million. It is really almost nothing.

Senator NUNN. It is now part of the DARPA budget?

Mr. GELBER. Right. There are other CERT's out there. IBM might have a CERT. Other people may have what they call a CERT. But he is the actual CERT and I think he will talk about that in a second.

We also recommend that the Director of Central Intelligence complete an NII, a national infrastructure threat estimate, and they should also, we recommend, have an unclassified version that would be made available to private industry. It is very important to understand, we believe, that this is no longer a "Government is going to do it; we are going to provide the answers." It has to have the private sector there.

They may come kicking and screaming, but we have to do something for them, and I think that a lot of their concerns are actually true. They may suffer market—maybe going to the FBI has some problems for them, but we have to create a system where they can come forward.

Senator NUNN. You may need, for instance, antitrust waivers for possible cooperation in this area. If one bank thinks that by reporting, their competitors are going to go around and get all their clients by saying they are not secure, then that is a real problem. That is the ultimate of taking the market economy to its ultimate absurdity because everybody in the long run is going to get hit.

I do not know whether there are antitrust implications or not about having the financial community working together. That is one thing you might want to look at, because it may be one way the government can make it easier for the various financial institutions, at least, and maybe others to work together.

Mr. GELBER. The telecommunications has a model that they use, the NSTAC, and all the specifics are set forth in the staff statement, but what that is is a group of telecommunications and government folks who get together and talk about this confidentially and anonymously and talk about threat assessments. It is a very good model. We have it in here, and we have used that model as something that we would blossom into a larger macro idea.

The next recommendation, Senators, is that we create an international computer crime bureau and CERT-type apparatus internationally, not so much for having the law enforcement response but because this is an international problem. It has that dimension. Clearly, there are efforts, as our staff statement indicates, from the international community already, but much more needs to be done.

There are whole countries, whole regions of the world where coming in and doing what this young man in Argentina did is not against the law. Or if it is against the law, they do not know how to deal with it. So we think it is very important to realize that this is a problem that does not know national boundaries and that we need to deal with it in that way.

As far as the government itself, our government, we need to maintain a better pool of security professionals and generally improve the consciousness of our users. If you talk to Mr. Christy or other folks who do this, they will tell you that our government loves generalists. If you learn anything about a specific area too long, it means you usually cannot get promoted.

What we do is we do that to its worst degree in the computer field. Our security professionals who run networks are usually somebody who just happens to know a computer better than the next person and is not a computer professional, or someone who perhaps is given that as a part-time job. That is a huge problem within government, this entire security culture.

So we recommend in order to ensure the stable pool of information security managers and investigators and specialists, that there be career tracks for these people and that we recognize that this is a whole area that—this is something you cannot learn in a month or two and then do it for a year or two and then give it to the next guy. There has to be a way that people can stay in this, do not go to the private sector because they pay more, but stay in the government for at least some period of time and give us some institutional and corporate knowledge.

The next thing we recommend within government is more vulnerability assessment, sort of what DISA does over at the Defense Department. We think that has to be something that is done regularly in the non-defense government. That does a lot for increasing awareness, as you can just see what the DISA has done over at the Defense Department. Senator NUNN. Does every agency need that, or should there be some group that swings between the smaller agencies?

Mr. GELBER. Our recommendation is that a group be assigned to do that, to oversee that with all agencies. You do not really, I think, need each agency to have their own, but rather have a group—just like DISA is defense-wide, have somebody doing it over in the—in fact, DISA potentially, I guess, could do it in the nonmilitary government, but it might make more sense to have a civilian government agency doing that on the civilian government side. We thought that was very important.

Another thing we recommend is mandatory reporting in the government of intrusions. Just that simple thing will improve our baseline of knowledge. It is not done. It needs to be done, but we have to get over this fact that people are embarrassed or ashamed that their systems have been intruded. That is not something that is a secret. It is something that we need to bring out.

Finally, log-on banners, and this is simply—this is our last and it may seem like a minor recommendation, but it is a very important tool. Right now, the Department of Justice encourages, recommends log-on banners. What they do is they say, if it is a government system, this system could be monitored by the folks who are running it for certain reasons, just to let the users know that if they are on a government computer, they may be monitored for some purpose.

Right now, in some agencies, if you do not get that banner, you might have to go out and get a wiretap or a Title III order to monitor it because you just simply cannot get that—you are not allowed to do it simply because they have not made it mandatory.

So we recommend, in terms of government computers, that that log-on banner be there so that if we get an intrusion, if we are trying to discover something, and most of these are going to be innocent parties. Just about every one of these users are not going to be the perpetrators, but you still have to go get a Title II order or their consent, if they are available, and then it might go somewhere else, in which case you have to stop the investigation and get someone else's consent and it is very difficult, so we think that is important.

That is our conclusion, Senator—

Senator NUNN. Who would do the monitoring in that case, when you say that? Would this be this same group of people, DISA in Defense and that counterpart?

Mr. GELBER. Senator, what we are talking about here is if there is an actual intrusion into a system. If you are sitting at a Department of Justice terminal and somebody is trying to get a proposed indictment, let us say, and that would be probably the FBI would have jurisdiction. They heard about it through human intelligence. They might want to go and investigate this case.

Right now, even if it is a government computer and if there is no log-on banner on it, they might have to go get a Title III wiretap. It takes about a week to get, even if you are part of the Department of Justice, and going through all the approval mechanisms, and then it may go to another computer—

Senator NUNN. You mean for the Department of Justice to look at its own computers, for the FBI to look at its own computers with somebody trying to steal prelimination on possible indictments, that they would have to get a court order?

Mr. GELBER. The Department of Justice may be a little unique because they recommended and, therefore, have made it mandatory within their Department. But in a lot of the other——

Senator NUNN. If the FBI were checking in the Agriculture Department about somebody——

Mr. GELBER. I think so. I think they would have a real problem going into somebody's computer at this point. That is why they have a log-on banner. There has been some debate about that. Jim, you have—

Mr. CHRISTY. Log-on banners have been mandatory in the Air Force for, I guess, about 3 or 4 years now and we still find computers when we have an intrusion that do not have a warning banner. The first thing we do is we install a warning banner even if it scares the hacker away because it is too cumbersome to go get a Title III wiretap order.

Senator NUNN. I think you gave us a little to think about this morning.

Senator GLENN. Mr. Chairman, may I ask a question on this? This is a comment and I would appreciate your response to it.

I think we have a very basic thing we have not really addressed here this morning, too, and that is in a democratic society like ours, what risks should a democratic society be willing to live with in order to reduce or eliminate its own vulnerabilities to hacking? This gets into some pretty basic matters.

When we start restricting people's ability to communicate in our society, we get onto some very, very thin ice. People communicated by mail. Well, we made it illegal to steal mail out of your mailbox and imposed stiff Federal penalties for something like that.

Then we had a phone system. Operators used to listen in back in the old days when we had operators, and then that became illegal. Now we have improved that up to where you have to go to court and get a wiretap to let you listen in and get people's communications.

Now we are up to computers where masses of information are being sent back and forth between individuals by different means and we are trying to deal with how much you can restrict somebody else's ability to listen in on this. In Defense matters, I certainly would not have any problem with saying we set up whatever systems we have to set up with all sorts of encryption, whether it is 40-bit, 56-bit, or way on up to 126-bit or whatever.

But when it gets into all the private conversations back and forth in this country and the business communication back and forth and economic matters, it is a whole different ballgame, it seems to me. We are rapidly getting to the point where I think, in law enforcement and other Federal entities, we cannot eat our cake and have it, too.

The law enforcement and intelligence communities will ultimately have to decide whether they want to continue to have the ability to break into the systems of others, in which case they are going to be vulnerable themselves, or whether they would prefer to go along with deep encryption, whether it is the 56-bit or whatever bit we come up with, and I am sure Mr. Rhodes, if he could do all this in an hour and a half, he could probably design an invulnerable encryption system in 20 minutes or something like that.

I think what we are talking about is, are we going to get communications back to privacy by encryption or are we not? I do not know that we really have much choice. It seems to me this way, anyway, that because there are lots of smart people out there like Mr. Rhodes, and I am sure the rest of you here, too, but I will use him as the example because he is the one that went through all this a little while ago here, who are going to be providing some of these encryption codes. He could design one in a few minutes, probably.

They are going to have these encryption codes and probably give them to people or you could have your own in-house hacker within your own company design your own code for this thing, so you are going to have privacy one way or the other. Basically, encryption is going to be very difficult to break.

I think what we are going to have is the ability of law enforcement and intelligence communities to break into other people's computers coming virtually to a halt because this is going to develop anyway, as I see it.

Am I oversimplifying this? We can set up all sorts of analyses of the danger. I do not have any problem envisioning a danger. To me, it is monstrous and it is big and it can upset our whole economy, our society. It really is that kind of a danger. It is what we used to talk about when we go to war. It is that kind of a threat, literally. I do not know that we have any option but to go to some of these encryption things. It tends to put us back toward the area of privacy in this new area of communications we call computers and the information superhighway.

Am I oversimplifying this? I would appreciate your comments on it. This may be a little broader question, but it seems to me that we have a very basic question here of how far we, in a democratic, free society, go in restricting what people can do to protect their own right to communicate. That is a big and a tough area and maybe goes beyond the scope of this hearing, I do not know, but that is the bottom line when we consider what we should do and maybe require in legislation. Then that is a very, very basic, fundamental thing.

It seems to me we are going to have to address this because all of our problems are not just in DOD or even government-wide. I do not have any problem in going ahead and setting up whatever we need in DOD, and let us do it. But when you get out to all the other places, the banks and businesses communicating—even if it is a matter of a business hacking into a bid from MACDAC on the West Coast that is coming back to the Department of Defense if some other company is doing this privately, trying to find out what their bid is going to be and things like that, we are into a whole different ballgame here that scares me when we get into trying to figure out an answer.

Do you have any thoughts along these lines? That is a big question.

Senator NUNN. I think these philosophical questions really are at the heart of what we have to start deciding. I do not see how the law enforcement and intelligence communities can sort these jurisdictions out and even begin to stake out positions until there is a broader public understanding of the dilemma and the questions, because I can see now if the Director of the CIA came out and said he wanted to be able to basically start tracing anybody's Internet call in the United States in order to protect national security, I think there would be a horrible kind of reaction.

I am sure that until there is a broader understanding of the vulnerability itself, it seems to me—I mean, I grew up in a small town where you had party lines unless you could pay a lot more and had a private phone. It seems to me we are getting to the point with the Internet that, to greatly oversimplify it, that everybody is on a party line except law enforcement and they are the ones that cannot tune in. Everybody else is. So people do not have the privacy they thought. It may be privacy only against the FBI.

Senator GLENN. I did not know Sam was that old. I thought I was the only one who grew up on a party line phone system.

Senator NUNN. It is not age, it is small towns. [Laughter.]

Senator GLENN. What is your comment? Where do we go with this? Why do we not just encrypt? I gather we could make encryption systems that would be virtually unbreakable, at least by present technology. I am sure they will break down sometime, some way. But right now, we could pretty well protect things if we just say, we are going to go that route and encourage everybody to do that.

Mr. RHODES. That is one piece of the solution. To encrypt, to have a strong algorithm, to have an intelligent key exchange is very important, but you also have to protect the sites on the Internet, as well, because depending on how you store the key in the system—

Senator GLENN. My first question is, do you want a key? Do you want the government to have a key? Then the government has a way of getting into everybody. That is the basic, fundamental question right there. Or do you want to let people go ahead and provide for their own security of communication?

Senator NUNN. Then you also have the philosophical question, as I see it, Senator Glenn, about the great advantages of the information age we are in, is that you basically have a free flow of information between millions of people out there. That is the advantage. Encryption may protect certain areas, but if you use encryption and take it to its ultimate and everybody wants everything to be private, you end up destroying the value of the system itself.

So there is a balance here that has to be reached and there is going to have to be a lot more discernment, I think, in the kind of information that we have always viewed as non-classified and whether that sensitive information moves into some other category. So the type of information, it seems to me, comes very much into play here, and I do not even think we have started as citizens, let alone as a government to think about this.

Senator GLENN. Would you each comment across the board on my comment here, what you think about it? You have undoubtedly thought along these same lines, too.

Mr. GELBER. I will start, and I will preface by saying I am a former Federal prosecutor, so my perspective is very pro-law enforcement. But I will tell you that this Subcommittee, and I am familiar with its history, has documented the fact that criminals do use technologies and terrorist groups and our enemies use technologies to enhance their abilities to do damage to us.

The digital pager, the cellular phone revolutionized the drug trade in many ways by providing anonymity, and there are a lot of comparisons between those tools and what is happening now. Of course, we use digital pagers to bring doctors and emergency technicians to the scene, so obviously the same balancings occur.

On the other hand, I think that, as my colleague said a moment ago, encryption is not simply the key. It is just—it is not a pun, but it is not the key to this, it is just a part of it. We do not have a baseline right now to make that determination. When you start asking people to measure privacy interests, we are measuring in a black box, in a vacuum. We do not even know really what the threat is at this point.

I suspect there will have to be encryption at some point, somewhere, by somebody, and there are a lot of folks that are looking at this issue and I would urge anyone listening that the Committee on National Research Council chaired by Ken Dam recently came out with a report which I think actually was trying to loosen export controls on encryption. But I think that we have to realize that this is going to be there.

I will, however, say this to you, Senator Glenn. I believe that criminals, even if you have encryption out there that somebody else made, will ultimately still use a good part of the time encryption that is provided by the government, because perhaps other agencies will be using them. Criminals have to interact with banks, with other institutions. So if some of your institutions which are either victims of attacks are using some form of encryption which you have access to, criminals will probably use that. In the World Trade Center case, one of the masterminds of it was using encryption to communicate with his colleagues.

That is the kind of encryption you may never get, you may never hear about, and that is going to happen. But criminals and bad guys will always use—they will always make mistakes and they will use publicly available encryption technologies no matter what, so the question is whether you want to just, by sending it out there, give everybody the choice.

Our Subcommittee has not really endorsed anything. We have a section here on it, but I think we did not endorse anything because there is so much that has to be looked at and—

Senator NUNN. We are not ready to make a recommendation on that now. I made that judgment myself. I think we have a long way to go in that arca.

Mr. CHRISTY. I am law enforcement, Senator, so you know where I am coming from. Basically, I think all we want is status quo. There are all kinds of procedures that limit what I can do as a law enforcement official and what I can monitor, and rightfully so. When we go through all of those, we ought to be able to see the communication.

Our head lawyer in OSI said that on the networks, you should have a reasonable expectation of anonymity but not a reasonable expectation of privacy, and they are two different things. Everybody on the Internet is being monitored. It is a party line, like you said, Senator Nunn. Everybody is monitoring and the only ones who cannot monitor it is law enforcement.

So if we set up standards and there is key escrow and you go through the proper procedures, we should be able to look at maintaining what we have already and what we need. Encryption is coming and law enforcement is going to be shut out of this if we do not have key escrow.

Senator GLENN. Would your position be we should prohibit encryption?

Mr. CHRISTY. No. I believe robust encryption is important for everyone.

Senator GLENN. I think it is coming whether we-----

Mr. CHRISTY. But there needs to be an escrowed key-in. When law enforcement makes that very high threshold of probable cause and can get that court order, they ought to be able to see what is being communicated.

Senator GLENN. Mr. Brock.

Mr. BROCK. I think you are asking the very key question. Perfect security would undoubtedly restrict the privacy rights of individuals and would undoubtedly restrict the flow of communication between individuals, and that may well be appropriate for some sorts of systems and information.

I think the recommendations that Mr. Gelber was making earlier are appropriate. If you want to know how you should protect your system, you need to know the threat against the system, you need to know the content of the information which really defines the threat, you need to know the vulnerabilities of the system, and then you can make a risk assessment. How much do I need or want to protect this information and what are the tradeoffs that I want to make in order to protect that information to an appropriate level?

Unless you understand the vulnerability and unless you understand the threat, it is very difficult to make those tradeoff decisions. If you do not understand the threat and the vulnerability, you are likely to make decisions that may be out of balance one way or the other, offer too little protection or, in fact, restrict the rights of individuals going the other way.

So I would endorse any efforts to better determine threat, to better determine vulnerability, so that when you begin to examine the tradeoffs on protecting the information, you can do so with as much information as possible.

Senator GLENN. Mr. Rhodes.

Mr. RHODES. I would have to echo the points here, but I would have to take the operational view and say that it is not, again, not just the encryption. It is how you are going to store the key, how you are going to handle the key, how the key exchange works. If I store it in software, I can burp it out of memory and get your private key and then break your system. It has to be a whole solution of encryption and firewalls and packet filtering and good passwords, and, and.

Senator GLENN. Can you design a key that cannot be hacked into itself?

Mr. RHODES. I was talking, a couple of weeks ago when we testified, I was talking to Dr. Peter Neumann and we were making the point that I do not really need to worry about the algorithm because I can go after the implementation. I can go after the software——

Senator GLENN. Say that again. I am not sure I follow you.

Mr. RHODES. I do not need to worry about the algorithm itself. Yes, you can. You can make relatively unbreakable algorithms because you can make them so complex that they take so long to break that you look at them and say they are unbreakable. But how is it stored? How is it used?

Senator GLENN. You could, in effect, bypass it, then, is that what you are saying?

Mr. RHODES. Depending on how it is implemented, yes. If somebody chooses not to use it—

Senator NUNN. Somebody has to be able to read it at both ends and—

Mr. RHODES. Right. Somebody has to be able to read it at both ends, and if I am passing secured messages and it is point to point, it is directly from my computer to your computer along a closed line, the chances for compromise are less than if I am out on the Internet and I have all these intervening nodes, as we talked about at the earlier testimony. The distance between two points on the Internet is not usually a straight line.

Senator NUNN. Thank you very much, Senator Glenn.

I have one question and then we will have our next panel. You stated that a number of private computer security firms have been using what you termed offensive counter-responses. Could you explain what offensive counter-responses means and the pros and cons of private firms using this?

Mr. GELBER. I will begin, but I will ask one of my more technically able colleagues to finish, because when I learned about it— I am a lawyer so I am not expert in anything—what we had heard from some of these private security firms is that, literally, they will go to an institution—I do not want to keep saying a bank because it is so easy to say, but any financial or commercial institution who is being attacked and they will give them the alternatives.

One of the alternatives that is sometimes given, although no security firm would confirm that they actually have done it, but they talked about this, and they may have been tight-lipped with us, of great concern was actually responding to the attack with something like, I guess the term is called polymorphic response, which is a program that responds to the attack, sends another program out there that does some damage or does something, like tells you, "We found you," or destroys the system or does something, but a responsive attack to the intruder.

When I heard that, I was extremely startled, because------

Senator NUNN. Which node up there would be destroyed?

Mr. GELBER. It would be the last one, or perhaps anyone after that. I will ask my scientists over here to tell you, but-----

Senator NUNN. You could basically be destroying completely innocent systems.

Mr. GELBER. Or a foreign government, even. Jim or Keith?

Mr. RHODES. Do you want me to handle this? I have to be careful on methods here. It is possible to reverse the attack. It is possible to reverse the attack through multiple nodes. Yes, you could, in effect, be destroying interim nodes that are blind to the attack.

For example, in the example that I showed in the earlier testimony where I went from New York City to Latvia to U.S. News and World Report to George Washington University and then into the Pentagon, to get back to the source, if I were to attack the interim hosts with any kind of reverse attack, yes, I could do extreme damage to those in between and it would be an active counterattack.

Mr. GELBER. It is the wild, wild West, Senator. When I heard that, it sounded like the O.K. Corral again. That is something that we are concerned about, and it is occurring, I believe, because there just are a lot of issues out there that are not being addressed, I think, by the government or by the industry.

Senator NUNN. But if you are the final victim up here on your chart, Mr. Rhodes—put that chart back up there, if you would. Back to that, I guess, black or brown part of the chart where it points to the final destination, you are there and you are being attacked and you hire a private firm to come in and they say one of your option is to go to, what do we call it, counterattack?

Mr. RHODES. Yes.

Senator NUNN. When you start counterattacking, what are you going to be able to get to? Who are you going to hit?

Mr. RHODES. I am probably not going to get home.

Senator NUNN. You are going to have to destroy every system along the way to get home, are you not? Mr. RHODES. Right, and I genuinely am going to have to exercise

Mr. RHODES. Right, and I genuinely am going to have to exercise multiple active countermeasures, which, in this scenario, as Jim pointed out, would necessarily involve human intelligence, depending on the sophistication of the route, the phone switch that I am passing through.

Senator NUNN. You could solve your problem immediately by destroying the previous node.

Mr. RHODES. Right. If it were—

Senator NUNN. That solves your problem, but then that previous node is gone and they did not even know anything about the attack.

Mr. RHODES. Unfortunately, if that is a university in Florida where people are doing legitimate work and somebody just happens to be using——

Senator NUNN. Let us use U.S. News and World Report. I think that would get more attention. [Laughter.]

Mr. RHODES. If it is U.S. News and World Report and they are innocently actively using their computer and somebody decides that that is going to be the jump-off point, yes, that is correct. They would have to go through and might necessarily bring down some part of U.S. News and World Report and have nothing to show for it, in effect, other than, "I brought U.S. News and World Report down and found out that it is some node in the Netherlands."

Mr. CHRISTY. Real-world scenario, Senator, we had an investigation. A DOD site was attacked. We set up our surveillance and our monitoring and we watched the good guys that did not know we were surveilling launch an attack on a foreign country and steal their password file in retaliation. They could justify that in their own minds. "They stole ours. We are going to steal theirs." It is the wild West. It may be not just to damage. If it is a bank, they may just be trying to go through all this looping and weaving to get their money back. It is an offensive info war.

Senator NUNN. We thank all of you very much. GAO has done excellent work. We really appreciate not only your excellent work but your excellent representation, both appearances. We thank you very much.

Mr. BROCK. Thank you, sir.

Senator NUNN. Dan and Jim, we thank you very much.

We have two other very important witnesses this morning, Richard Pethia, who manages the Trustworthy Systems Program and the CERT Coordination Center at the Software Engineering Institute, known as SEI, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. The CERT Coordination Center is a Computer Emergency Response Team whose focus is to conduct computer security system incident response activities.

We will have our witness discuss how the center fosters the development of incident response infrastructures to correct vulnerabilities and resolve computer-related incidences. He will also give us some examples of computer security incidents.

Richard Power is the editor of the Computer Security Alert, the Computer Security Journal, and the publication Frontline and an analyst for the Computer Security Institute at San Francisco, California. He is the author of a number of computer security articles, including "A CSI Primer on Computer Crime and Information Warfare". Mr. Power will discuss the results of the 1996 computer crime and security survey conducted by the Computer Security Institute, composed of questions submitted by the Federal Bureau of Investigation International Computer Crimes Squad, San Francisco office.

We are glad to have both of you here. We will ask that both of you, who have not been sworn, if you will stand and take the oath.

Do you swear the testimony you give before the Subcommittee be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. PETHIA. I do.

Mr. POWER. I do.

Senator NUNN. Thank you.

Senator GLENN [Presiding]. Please proceed.

TESTIMONY OF RICHARD PETHIA,¹ MANAGER, TRUSTWORTHY SYSTEMS PROGRAM AND COMPUTER EMERGENCY RE-SPONSE TEAM COORDINATION CENTER, SOFTWARE ENGI-NEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PENNSYLVANIA

Mr. PETHIA. Mr. Chairman and Members of the Subcommittee, I want to thank you for the opportunity to be here. My name is Richard Pethia. I manage the Trustworthy Systems Program and the Computer Emergency Response Team at the Software Engineering Institute. The SEI, the Software Engineering Institute, is

¹ The prepared statement of Mr. Pethia appears on page 306.

a federally-funded research and development center based at Carnegie Mellon University.

Back in November of 1988, for those of you who have been involved with computers for a while, you may remember that the Internet was called the Arpanet and we had an event on the Arpanet called the Internet worm. At the time, the Arpanet consisted of about 80,000 computers, nowhere close to what the Internet is today. That security event was the first harbinger of possible problems on network security.

At that time, DARPA decided to establish at the SEI something called the CERT, Computer Emergency Response Team, Coordination Center. Our primary mission, defined then, is to respond to computer security emergencies on the Internet, to work with the people who were suffering problems, to identify difficulties, flaws in the technology, to help them understand the problems that they had in their network security policy and their network security administration practices that led them to being vulnerable to attack, and then to work with those victims and others, to warn other downstream victims of potential attacks.

We are also charged to serve as a central point for identifying and correcting vulnerabilities in computer systems. We routinely receive vulnerability reports from people in the Internet community. Most of the reports come from research universities, people who are actively working with the technology, trying to use it for new purposes, or in some cases, actually probing it to find weaknesses. When we do find problems in the technology, we work with the technology producers and the vendors to resolve the problems and then issue advisories to the broad Internet community.

Our direct mailing list for advisories has about 13,000 entries. Many of those are mail exploders, so our direct mailings probably reach over a million people on the Internet. Indirect distribution reaches millions of others.

We continue to maintain close ties with the research community and to conduct our own research into tools, techniques, and methods that people can use to protect themselves when they connect to wide-area networks. In fact, the research and development activities are a growing emphasis for us and the direction in which DARPA would like to see their funding move in future years.

Finally, we are very active in trying to take proactive steps to raise understanding of information and computer security issues. I think you have heard today that one of the big problems we all face is that many people simply do not understand the risks. They do not understand the threats, and therefore they do not understand what level of investment they need to make to protect themselves when they connect to wide-area networks, such as the Internet.

Finally, we were chartered by DARPA to serve as a model for other incident response teams. It was their belief and ours, back in 1988, that a single national team would not be sufficient to meet the needs of the country. The vision at the time was that the networks would grow and expand very rapidly, but more importantly, the vision included the idea and the understanding that different parts of the community are going to need to respond in different ways to security problems when they occur. The policies, rules, and regulations that govern the activity of Federal agencies are very different from the policies, rules, and regulations that govern the activity of private industry, are very different from the rules and regulations that govern the activity of university communities. Each of those separate cultures are going to respond to incidents in their own way, and trying to jam all that into one uniform model did not seem to us to be an approach that was going to scale-up long term.

So, the next slide, we developed a distributed model, and we have helped start a number of other incident response teams. You find response teams now in the Department of Defense, in civil agencies, in universities, in commercial firms. There are a number of international teams. So, for example, the Australian team covers all of Australia. There are two teams in Germany. There are teams in Italy and the Netherlands and all of us work together as best we can.

Each team focuses on their own constituents. So, for example, the Westinghouse team focuses on Westinghouse Corporation sites. The Penn State team focuses on the campuses of Penn State, which happen to be about 22 scattered across the State of Pennsylvania. The Stanford team focuses on Stanford University. Motorola conducts incident response services for its own Motorola facilities. We at the CERT in Pittsburgh basically take care of the Internet and everybody else who does not have a team to call.

So if you put it all together, while there is coverage for many organizations, we certainly have a long way to go before everybody who needs to have this kind of service has it available to them.

The next slide, please. I think some of the testimony you have already heard this morning helped you understand the kinds of attacks that we are seeing. Over the years, in 1988 and 1989 when we started, we saw an awful lot of what I think people would today consider to be minor pranks or overly zealous, curious teenagers looking around the network for information that they found in some way satisfied their curiosity.

Senator NUNN. Would you agree with the previous testimony that the ones we are really catching are sort of at the bottom of the food chain in terms of the least sophisticated?

Mr. PETHIA. I think that is exactly right. I think when you actually look at the numbers—when you compare the number of incidents that are being reported to the number of times we can actually successfully find and successfully prosecute someone that there is a huge gap. I also think we are catching the ones who are sloppy, the ones who are making enough mistakes that allow people to see what they are doing and actually trace them.

As you saw from some of the earlier charts, tracing back some of these people is next to impossible. Jim Christy said with his example, it is an unsolvable case, and I think he is exactly right. We are catching the people who do not understand how easy it is to be even more sophisticated than they are.

Our focus is not on understanding damage. Our focus is not on prosecution. When DARPA gave us our charter, they were very clear to tell us that we had no authority. We could not speak on behalf of the Federal Government. We could not investigate on behalf of the Federal Government. When we receive reports from people out on the Internet community, we consider the information that they send to us as their information. We believe it is proprietary to them. They send it to us because it allows us to analyze technically what is going on and give them some technical advice on what to do in terms of shoring up their systems so they are less vulnerable to attack.

Very often, we do not even know what the extent of the damage is. Typically, by the time someone gets through an incident and is at the stage of doing damage assessment and adding up all the costs, we have already gone down the road to the next 52 incidents that have come at us.

But we certainly hear anecdotes, as many of you do from time to time, that the cost to organizations is going up. There are operational losses. A large engineering firm, for example, pulled off the network for over a week. Over 1,500 engineering work stations went out of productivity while the organization rebuilt all the software, rebuilt all the systems and brought themselves back up into operation.

We have, I believe, some reports from the U.K. that I think are harbingers of the future that we need to pay attention to. Detective John Austin in New Scotland Yards has reported two cases of medical records tampering, where this was not simply an invasion of privacy. In one case, medical records, the results of cancer smears for three patients, were changed from negative to positive, and for a period of time, several women in the U.K. felt that they were at high risk for cancer because of these test results.

There is a second case involving medical data in a system that stored images from brain scans, data was to be used to help surgeons to perform an operation. They discovered right before they started surgery that the system had been penetrated, that the data no longer had integrity. They therefore had to postpone the surgery for a week while they took the system off the network, rebuilt it, reran the tests, and rescheduled surgery.

Fortunately, in both cases, there was no damage done to the patients, but I think you can begin to see how important some of the data is that we have on line and the kinds of consequences that can occur if it is simply tampered with, let alone people who try to steal it for monetary benefit.

The intruders, from our experience, are becoming increasingly technically sophisticated. It is becoming more and more difficult to understand the techniques that they are using because they are understanding more and more things about operating systems, about network software, about the idiosyncracies of much of the technology that we are using today.

I think, just as important, they are becoming increasingly stealthy. You have heard about the tool called rootkit. When we do now get calls from sites, we are often discovering that the intruders have been using the computers at the sites for months, if not, in some cases, even years. Their activity has gone undetected. When we try to work with the site system administrators to look at the files that the intruders have left behind, increasingly, they are using strong cryptography to encrypt those files, so it is very difficult to understand what they are doing. Also, they are gaining increased efficiency and leverage through tools. We have had some discussion here this morning about the tool called SATAN. From our perspective, SATAN is one of the least interesting tools in that there is nothing that SATAN does that the hackers have not been doing for years.

One of the big difficulties that we have with tools in the area of computer security is that almost all of them are double-edged swords. The legitimate system administrators do need technological support to help them do a good job of securing their systems. Unfortunately, the same tool that can help you protect your system too often is a tool that helps others break into systems, and that is something that we do not have a good technical solution for today.

I think the major thing, however, about tools that is important to consider is the fact that taking the expertise of a hacker and embodying it in a tool not only allows that individual to be more efficient with his trade craft, it also allows less sophisticated technical people to become effective at breaking into systems, and that is the trend that we see with the work that we do.

Very often, we will see an incident. We will discover that the incident has, in fact, been perpetrated by the use of some new tool. Within weeks, we will see a dramatic increase in the number of reports for that particular kind of incident. So it is obvious that these tools are effective and it is obvious that they are being shared throughout the population of intruders.

Within the last 2 years, we have seen increasing numbers of attacks on the network infrastructure itself, the various servers on the network that allow the network to operate. We are seeing attacks against network service providers. We have the beginnings of network service providers reporting that they believe they are under attack from some of their competitors, people who are trying to disrupt the service of their operations so they, in turn, can go to their customers and claim that they have a competitive advantage by offering a higher-quality service.

Two years ago we began to see the use of what are now called network sniffers, pieces of software that are planted in systems on the network to collect information as it goes past across the network. Typically, what is collected are computer addresses, account names, and passwords, which very often traverse the Internet in clear text. The intruders come back, take that information, and can then use it to break into the systems that are referred to by the data they collect.

In those cases, we often have incidents that affect not only one site, the site that was originally penetrated to install the sniffer, but very often tens, hundreds, or in a few cases, even tens of thousands of sites have been affected because the keys to their systems have been picked off the network by intruders.

And finally, the number of incidents itself is increasing. Back in 1989, our first full year of operation, I think we had less than 140 incidents reported to us. By 1995, that number had increased to over 2,400.¹ The security incident report rate is growing at the same rate that the Internet is growing, and I think you just heard

¹See Exhibit No. 3.a. which appears on page 477.

that the growth rate is exponential. We are seeing that kind of increase at our response center in spite of the fact that there are now over 50 other teams who are each taking care of their own part of the problem.

So the problem, in our estimation, is getting worse, not better. There is more activity. The intruders are becoming more sophisticated. The attacks, from the anecdotal data that we get from the sites, are becoming more serious in that they are costing these organizations more and more to recover and to get back into operation.

Senator NUNN [Presiding]. Mr. Pethia, one interruption here. What can you do about one of these intrusions once you find out about it? Your job, as I understand it, is not to stop the intrusion nor to play a law enforcement role nor to go back and trace it. Yours is more of an informational advice/consultant kind of role, is that right?

Mr. PETHIA. Yes. Let me step you through, perhaps, a typical incident. We will get a call from a site. They have discovered that someone is doing something with their systems that they do not understand. We work with their system administrators to try to help them figure out what is going on. In the process of doing that, they send us activity logs from their systems. They send us other files which we then analyze.

So, typically, for any site that calls us, we can tell them what the intruders are doing at that site—not necessarily all of their activities—but at least a list of probable ways that the intruders have gained access to their system. We then let them decide what they want to do. Typically, what they want to do is prosecute, until they begin to think about the ramifications of that. That is when people begin to clam up on us.

We offer to connected them with law enforcement organizations. In fact, we offer to make that connection for them, if that is what they choose to use. We will support investigations, and we have worked very closely with the FBI and with other investigative organizations, but we do this at the request of the people who call us. So from that perspective, we view ourselves as third parties who are there to provide a service to people on the Internet.

We look at the technical vulnerability. What was the weakness that they had in their software, in their administrative practices, or in their policy that allowed that intrusion to occur? We help them correct those vulnerabilities. To the extent that those vulnerabilities are prevalent across the systems on the Internet, we work with the technology producers and the vendors to find solutions to those problems and then to warn the community that the problem exists and that they need to take corrective steps to repair their systems.

One of the things we are seeing, certainly in the last 2 years to a larger extent than ever before, is what is now being called by many people Internet fever. The rush to the Internet, in our opinion, is leading to the exposure of sensitive data and a much greater risk to safety-critical systems. People are connecting to the network without understanding what they are doing.

At the same time that we are seeing the explosion in the use of the Internet itself, we are seeing a general explosion in the use of the technology. If you think not just of the growth of the Internet but the growth of the use of computers and other automated information systems in our day-to-day lives and in our business operations, we are seeing a fantastic explosion in the use of the technology.

We are also seeing a trend towards distributed technology. So the days of the centralized mainframe or the days of the centralized large time-sharing system with a small staff of professionals who administer and manage those computers for all of us are gone. We have distributed the technology and we have distributed the management of the technology along with that.

I believe, unfortunately, that means we now have many people in the position of system manager and system administrator who not only do not understand the security risks, they do not even understand the technology that they are trying to manage. I think that is leading to increasing vulnerabilities.

More and more often, when we talk to people on the phone and try to help them technically analyze what has happened to them, we find we are talking to someone who does not understand the technical details of the system that they are operating.

We have done a glorious job in the computer industry. We have made systems that are easy to use. We have made them so easy to use that hundreds of millions of people are using them. Unfortunately, we have not made them easy to secure, and that is a problem that we need, I think, to deal with, and we need to deal with very vigorously.

The vendors are not putting security first. Products are engineered for ease of use. I met with a senior manager of a large technology firm last week and I asked him, what are the three most important characteristics that you believe are important to your customers? His answer was, ease of use, ease of use, and ease of use. I believe we are in a situation where we do not have enough skilled system administrators to handle the technology that we have out there today.

It is possible to connect to the Internet and operate a highly-secure system. We know of many sites that do that, but those sites are blessed with skilled technical expertise, people who understand how to do all the various things that are necessary. They understand how to use encryption. They understand how to use firewalls. They understand what firewalls are good for and where they do not protect you. They understand that you need policy in place in your organization. They understand how to do good system configuration management practice. They understand how to keep track of the vulnerabilities that are being discovered. They understand how to take CERT advisories and actually do things with them. They understand how to take a source code-level patch from a vendor and install it in their systems.

But the number of people who have that breadth and range of technical expertise compared to the number of people that we need to manage the technology that we have today is decreasing.

Finally, I think it is important to remember that, from a technological standpoint, there are no silver bullets, but we are beginning to see evidence of some snake oil out in the marketplace. I do believe that awareness of computer security and the need for better security is beginning to increase.

Senator NUNN. When you say snake oil, in what respect are you talking about snake oil? Are you talking about security specialists that are selling solutions that really are not solutions?

Mr. PETHIA. People who are selling solutions that really are not solutions, and I believe sometimes that is intentional, but I believe sometimes that is because they do not know, either. I believe that is part of the situation that we are in with this dramatic explosion in technology.

I do know that there are people who are selling many devices called firewalls. Simple network routers with some filtering capability are often called firewalls, and there are many people who firmly believe that that is a solution to a problem. They are selling their product with confidence in their minds, I think there is no lack of integrity there, but the problem is they do not have the real solution. The problem is much more complex than anything they understand, and as a result, people are finding themselves in positions where they are not really as secure as they thought they were, even after they made a substantial investment in improving security.

We are seeing the same kinds of things with security audits. There are many security audit techniques that are left over from the days of the large centralized mainframe computers. The techniques focus primarily on system administration policy and system administration practice but they do not really look deeply at the technology. Unfortunately, if you go through one of these audits and you are not using a centralized mainframe, but are using one of the new client server open system architecture kinds of configurations, you are typically going to end up feeling that you are secure when, in fact, you are not. We are very concerned about that trend, as well.

Finally, some of the things that we think might be useful to do resonate well with some of the recommendations you have heard earlier this morning.

We think it would be a help to have a center to collect, analyze, and disseminate computer security incident data. I believe that center is probably not one monolithic organization. It is probably made up of several. I think, again, it is very important to be sensitive to the different cultures that are using all these various networks that we have. One thing I am very sure of is that we are not going to get out of this problem until we build market awareness for the need for improved security in the products that are there.

I think, ultimately, it is going to be the marketplace that drives this process to a successful completion. In the meantime, some rules, policies, regulations, and mechanisms might help, but I think in the end result, it is really going to require the marketplace to respond to this problem. That means the people who need security are going to have to recognize that need and be willing to invest in it.

I believe that all of the incident response teams-

Senator NUNN. It also means that the cost of the information age is going to go up very rapidly in terms of expense, is it not? Mr. PETHIA. I think we are going to perceive it as a cost increase. I think what we need to recognize is the fact that the cost is already here. We are paying it on the back end. The cost of recovering from an incident, the cost of going through an investigation, the cost of public lack of confidence when the investigation becomes public is much greater than any initial cost would be had the cost been made up front to prevent the incidents before they occurred.

Senator NUNN. Your big institutions, perhaps the ones that are most vulnerable, are probably more able to pay these front-end costs, but my experience tells me that there are an awful lot of small folks out there that cannot.

Mr. PETHIA. I think there is an awful lot that can be done with very simple techniques that do not require a major investment in technology.

Senator NUNN. Not a lot of money?

Mr. PETHIA. What we find is people, again, due to lack of understanding, do not understand that putting a firewall, for example, on the front end of a set of systems connected to the Internet does not help much if, at the same time, you allow 500 modems connected to each of the systems in the back room. So people are, unfortunately, making investments without understanding what they are investing in. I think there is an awful lot that could be done with simply good, sound, pragmatic guidance on how to configure and administer systems, and people can go an awful long way with very inexpensive technology.

Senator NUNN. One of your functions is to give that kind of advice.

Mr. PETHIA. That is correct, and increasingly, we are spending more and more of our time doing exactly that. We currently have a project underway to put together a set of what we call system administration key practices that will give very pragmatic advice to system administrators on steps they can take to secure those systems. Pieces of that work will begin to become available within the next 2 months.

Senator NUNN. How many people do you have on your staff?

Mr. PETHIA. For both the reactive and the research work, we have about 20 people. The current funding profile from DARPA has us shifting our emphasis from the reactive work to research and development. Last year, three-quarters of our funding was spent on incident response and one-quarter on research and development. Next year, it will be the exact opposite of that.

Senator NUNN. Are you able to handle the requests you get?

Mr. PETHIA. No. For the last 3 years, we have been unable to handle the requests that we get. We go through a triage process every day. We focus on the incidents that look like they are going to have the widest impact, so we look at network sniffers, we look at attacks on the network infrastructure, we look at things that threaten the integrity of the network itself, or we look at things that will potentially affect tens, hundreds, or thousands of sites.

Senator NUNN. So I am a user out there and I am being attacked and I need help and I need advice and so forth and I call up. Am I going to get one of those numbers where you stay on the line for hours and hours saying, "We love your business. We will get with you just as soon as we can"? [Laughter.] Mr. PETHIA. We will not keep you on the line for hours and hours but we will tell you pretty quickly that there is not a lot that we can do for you. We will point you to our archive of information. We will give you a set of diagnostic techniques that we think you can use to help you understand what has just happened to you. We will give you a set of suggestions on steps you can take to protect yourself. We can do that because we have all of those things prepackaged and ready to go.

But our ability to give individual response to the people who have called us has declined rapidly as the phone rate has increased exponentially over the last 4 years. So there are certainly a number of people who need help, frankly, much of the Internet community is becoming increasingly frustrated with our ability to help them.

While I am on the topic of frustration, I wanted to throw in one more point. I think we have heard a lot of discussion this morning about why people do not report incidents. I think there is something very important to consider as you begin to think about what you might establish to encourage that kind of activity to happen.

Many people call us, and we are often recognized or at least touted to be "the CERT", as I heard earlier this morning. I think one of the reasons that people call us is because they get something back. They get some kind of service. They get some kind of help. They get something to help them deal with their problem.

Very often, they say, when they call law enforcement, that is not what they see. What they see is a long process that has a low probability of success and they simply do not want to get involved. So I think lack of public confidence in their operation is one thing they worry about.

But the second thing they worry about is, what am I going to get into when I get into an investigation? What is it going to cost me and what is the probability that anything effective is going to come out of all this? I think most of them, when they go through that analysis today, conclude that they had better just go take care of their own problems and be on with life because getting involved in something bigger is not going to go anywhere.

Another thing that I think would be very important to do is to initiate, and I think Federal sponsorship might be necessary to help this happen, academic programs for the education and training of computer security professionals, including the training of system administrators and managers who are skilled and knowledgeable in the area of information system security.

One of the problems that all of us who work in the security area struggle with is finding funding to do the work that we do, and security is an up and down kind of thing. When incidents get a lot of public attention, public funding is available, and after a few months, when interest dies off, then it is less easy to get to.

Even more difficult than finding funding, however, is finding qualified technical people who can work in this area. We are simply not training them. They are not coming out of the universities, with the exception of one or two small programs. They have to learn on the job. The number of people that we need technically skilled to deal in this area, when you look at the explosion in the use of the technology and the networks, is staggering. How we are going to train enough people, let alone deploy them, to help us solve that problem?

And finally, I think we certainly need not to think about this as a short-term problem. It is going to be with us for a long time to come. The tools and techniques that are effective at dealing with the problems that we have today, the firewalls that we all like to reach out and grab and hang onto and hide behind are not going to be effective as the technology changes over time and the use of the technology changes along with it.

Senator NUNN. Is this going to be a case where the offense is going to have a continuing advantage over the defense?

Mr. PETHIA. I am not sure that it is going to have a continuing advantage, but I do believe firmly that it is going to be a continuing foot race. I think we are always going to have to pay a lot of attention to this area.

Today, we are moving to a situation where more and more government agencies and private corporations are doing more and more computer interconnections with their customers and with their suppliers. Every time you connect to some other organization, every time you allow that organization through your firewall, you are opening up another potential path for the hackers to get in.

Our prediction is the technology we are using today, while it is currently effective, will not be effective within the next 2 or 3 years, as distributed computing becomes more and more the paradigm of doing business on these wide-area networks.

I think we need to continue to support programs like the DARPA program on information survivability, work by other research organizations like the National Science Foundation, to ensure that we have the research and development staying ahead of the problem. Otherwise, we always will be in the position of trying to catch up.

Senator NUNN. You are being shifted more to research and development. Is your overall funding being cut, also?

Mr. PETHIA. No. Our funding from DARPA is at the same level, actually a slight increase this year, but they are directing more and more of that money to the research and development activity.

Senator NUNN. Which means you are going to be able to be less and less responsive to people who call in.

Mr. PETHIA. On the operational side, that is correct. We have been working with the National Institutes of Standards and Technology. We are beginning to put a program in place where we believe we will get some funding from the civil agencies, through NIST to help the civil agencies with the problem. We are working with some of the DOD organizations to allow us to continue to support some of the operational work, and in particular, our threat and vulnerability analysis work, and we are trying to find ways to keep the operational work going. That path is beginning to come together, but it is a long way from there currently.

Senator NUNN. Do you think that your organization should be kept abreast in funding to handle these kind of complaints, to keep up with the growing both complaints and threats from intrusions, or do you think that your role basically has been to get other organizations out there all over to do this? Do you believe you should be funded to meet the increased threat? Mr. PETHIA. It is a question I love to answer. The one thing I think we have done is put ourselves into a position where we are widely visible and recognized and trusted within the community. There is some reason why we get these 2,500 incident reports a year and other teams do not. I think now that we have that capability, we ought to hang onto it, because I think it is an important national resource. I think the trick is to convince more and more of these people to make their data in a sanitized way be available for the greater good, and I think we are in exactly the right position to do that.

We are not considered part of the Federal Government. We are not considered industry, so we do not threaten anyone from a competitive standpoint. We are housed in a research-based university, so people believe that we have the credibility of a large academic research organization behind us and I think we are very well positioned to do that kind of work.

Senator NUNN. Can your information, sanitized so it protects proprietary information you may get, can that be made available as part of the threat assessment?

Mr. PETHIA. I think the information certainly can be made available. We have not done it in the past for primarily the reason of funding. The information that we get does not come to us in nice, neat packages. It comes to us in bits and scraps of E-Mail and phone messages and log files and what have you. The task of going through that information to sanitize it is one that is larger than the resource we have available.

Senator NUNN. But would that not be, if we are going to get an intelligence threat assessment or national intelligence or whether it is the CIA or someone else doing it, if we are going to get a real threat assessment as a beginning tool to understand the scope of the problem, would it not be worthwhile to take the information that you already have and spend enough resources to put it together in a form that can be utilized?

Mr. PETHIA. I certainly believe it would be. It will help us understand much more about the technical problem, and to some extent, it will help us understand about the scope of the problem. I think in addition to the data that is being collected by all the various response teams, with us having the most, we also need to look at the kinds of studies that I believe we are going to hear about here very shortly because what we have is only a piece of the puzzle.

But I do believe, again, we are well positioned to collect a lot of this data and I think there is an awful lot of value in having it available to a greater audience.

Senator NUNN. Let us go on to Mr. Power and then we may have questions for both. Mr. Power, thank you for being here.

TESTIMONY OF RICHARD G. POWER,¹ EDITOR, COMPUTER SECURITY INSTITUTE, SAN FRANCISCO, CALIFORNIA

Mr. POWER. Thank you, Senator Nunn. It is an honor.

First of all, I want to say that I am really gratified to hear some of the testimony and some of the questions from the Committee that I have heard this morning. CSI represents information secu-

¹ The prepared statement of Mr. Power appears on page 324.

rity professionals in corporations, government agencies and universities; the people who, to a great extent, kind of started with a thumb in the dike and now have run out of fingers.

What you have been hearing about the Internet, as Mr. Pethia just said, is one piece of the pie. Maybe it is a pie dish itself that has brought it all together. But there have been many information security problems as long as we have had network computers and even before that.

To bring it all together, just to give you a brief glimpse before we go into the results of our survey, information security professionals in enterprises, both in the private sector and public sector, not only have to worry about outside intrusions and sophisticated or less sophisticated hacks. They also have to worry about fighting for budget, for staffing, for training, keeping up with the technological changes that are just happening incredibly fast—LANs, WANs, wireless, Internet access, intranet, electronic commerce, web servers.

It is just staggering. They are fighting for budget dollars, both inside the government and in the private sector. They are fighting to train their people, to staff the places. They are fighting for security awareness dollars, which is a really extraordinary need, as we have seen.

So let me tell you what this survey entails. The 1996 Computer Crime and Security Survey was conducted by CSI and composed of questions formulated by the FBI Computer Crime Squad office in San Francisco.¹ We sent it out to over 4,000 information security professionals in Fortune 500 corporations, government agencies, and universities. We got back an 8.6 percent response. I think it is 428 information security professionals responded. There has been very little data collected in this area, and in my written testimony, I have cited some of the other ones.

We are very happy with the results. We asked 33 detailed, touchy questions. We got some very fascinating results, and I think there are some other studies: Ernst and Young information, American Society for Industrial Security, and East Michigan State University. I want to refer you to all of them, also, I do not think any of us are claiming this is scientific data, but we are trying to get a glimpse of the facts on the ground. Maybe we will take a little tour through the survey now.

Response by industry segment, 24 percent financial, 19 percent government, 12 percent manufacturing. You can see it is a pretty broad cross-section. We have also mined down through there in some of those specific segments.

Senator NUNN. What is the big one down at the bottom, the big part of the pie?

Mr. POWER. That is financial.

Senator NUNN. That is what?

Mr. POWER. Twenty-four-point-seven percent, financial.

Senator NUNN. Financial.

Mr. POWER. The financial sector. So unauthorized use of computer systems within the last 12 months, 42 percent of respondents had experienced some form of unauthorized access of computer sys-

¹See Exhibit No. 2.c. which appears on page 465.

tems within the last 12 months, and here, we are not talking about people playing games on their computers, as we will see in a moment.

One other thing here, before we move on, 21 percent do not know. This should not be taken as a slight of the people who are doing this job. It is an indication of the situation which you have seen outlined by both the Committee staff and your witnesses.

There are a couple of interesting things here. Number of attempts made within the last 12 months. Do not know, 21.2 percent Twelve-point-two percent, more than 10 attempts within the last 12 months. Twenty-two organizations answered more than 10 incidents in the last 12 months. The individual numbers of attacks ranged from 14 to 1,000 and the total number of attacks for these 22 organizations totaled 3,201.

Types of attacks are diverse. I have included a list of definitions in the addendums to my testimony. Basically, in information security, you are not only dealing with confidentiality, which encryption solves a great deal of problems. You are also talking about availability and you are also talking about integrity. For example, when you are dealing with data diddling, you are dealing with the integrity of the information.

We found in the survey results that when we looked at the financial sector and the medical sector, when we extracted them out from the whole pool, the numbers of data diddling for medical were 36.8 percent and for financial were 21 percent, significantly higher than, for instance, on the next slide, data diddling in the government, 15.9 percent, and data diddling in utilities, 14.2 percent.

The thing to ponder there is obvious, without being alarmist, either. When you are talking about medical institutions and financial institutions, you are talking about people's money and some of the most confidential information that individuals or societies could have. So it was curious to us to see, when we looked at the data for medical and financial, separated out from the rest, that that particular form of attack was significantly higher than, say, in the other two sectors.

Senator NUNN. And by data diddling, you mean disturbing the data or altering the integrity of the data?

Mr. POWER. Yes. Mr. Pethia cited the recent incident in London, that was brought out by John Austin, of changing somebody's medical records for malicious intent, or, for that matter, changing somebody's medical records or financial records in their favor, for instance, somebody's credit history. Some of that kind of activity has been documented in the literature on the hacker underground. On the high end, data diddling can also include unauthorized financial transactions.

Networks are being probed from all access points. This is really important to emphasize. The Internet has brought this all to a boil. But LAN technology started some time ago and WAN and wireless and modem technology. These forms of connectivity have all been compromised and now, with so many companies and so many organizations signing on, the Internet has just aggravated a problem that was already there.

What you are seeing is that organizations are faced not only with a threat from the Internet but threats from remote dial-in access. You can see mobile sales forces and the exposures there, and internal systems, are still the major concern, 53.3 percent.

The next graph shows that of the number of incidents that we could document in the report, the number of incidents from the outside overtook the number of incidents from the inside. That is interesting because the conventional wisdom is that 80 percent of the computer security problem is internal, in other words, from disgruntled or dishonest employees.

These figures could indicate that the preponderance is shifting. It is certainly shifting because of the Internet connectivity, but one caveat is that the frequency of attack from the outside may be much higher because they are trying different ways to get in.

Would the information sought be of any interest to competitors? Fifty-four-point-nine percent said, yes, domestic competitors would have been interested in the information that was sought. Twentyseven-point-six percent said foreign competitors would be interested in the information that was sought. And 17.4 percent said foreign governments would be interested in the information that was sought. I thought those numbers were somewhat high, actually.

Senator NUNN. In what way high?

Mr. POWER. I was surprised that even on an anonymous survey, they would admit that, frankly. This, of course, was an anonymous survey. We knew who we were sending it to, and when we sent the questionnaires out, we said, this is a survey being conducted by CSI with questions from the FBI but it will be anonymous. We will not know who these answers are from.

Senator NUNN. But when you say high, do you mean that was higher than you expected or higher than you believe to be reality?

Mr. POWER. Higher than people acknowledge face to face.

Senator NUNN. The survey was higher than basically you had expected to get back?

Mr. POWER. Right. Yes.

Senator NUNN. But you do not think it is unrealistic?

Mr. POWER. No, I do not think it is unrealistic. I was just surprised that even in an anonymous survey, that they would admit it.

The next few graphs show likely sources of types of attack. There are about five slides here of different types of attack and you will notice that the numbers for hackers are very high and the numbers for disgruntled employees are very high. That, again, is what we read about most often in media accounts of various types of security incidents.

But the interesting thing here is that over 50 percent throughout these slides consider U.S.-owned corporate competitors a likely source—not the only source but a likely source—of each form of attack. For example, eavesdropping, 58.5 percent perceived U.S. competitors a likely source, while 76 percent perceived hackers as a likely source of eavesdropping. System penetration, spoofing and wiretapping, all pretty much consistently around 50 percent for likely source of attack from U.S.-owned corporate competitors. Foreign and domestic averaged pretty much 15 to 20 percent all the way through these various types of attack. Then we asked a wide range of questions about preparedness to get an idea of what people were doing. They had performed some risk analysis in terms of trying to quantify or qualify the threat. They had done some good things, like security awareness programs, 60 percent; ethics programs, 60 percent; written policy on E-Mail usage, 60 percent; and 68 percent reserved the right to examine employees' E-Mail.

Senator NUNN. Do you think that the people who were more likely ly to respond to this would be also those who would more likely have taken some of these steps?

Mr. POWER. Yes.

Senator NUNN. In other words, if you are sitting out there and you get the questionnaire and you never really thought about this subject very much and you have not done anything, you are not likely to respond to it in very much detail.

Mr. POWER. Absolutely.

Senator NUNN. So this would probably be your more alert-

Mr. POWER. This is a better case scenario.

Senator NUNN. Right.

Mr. POWER. I would not say best case, but yes, it is a better case scenario, because these are being mailed to information security professionals. That means the organization has one. There are many organizations where information security is, at best, a parttime job.

Senator NUNN. Right.

Mr. POWER. Over 70 percent said that few employees had a working knowledge of current laws on the misuse of computer systems. It would seem to me that would be a good place to start in terms of public education. Over 70 percent do not have a warning banner, and you heard this addressed by your staff folks. If you do not have a warning banner in place—

Senator NUNN. That is what they call a log-on?

Mr. POWER. Yes. You are hamstrung right from the beginning if you don't have one.

Senator NUNN. Do most of the private sector have those? Do a great deal of the private sector have the log-ons?

Mr. POWER. Do you want to go back?

Senator NUNN. Yes. I did not get that.

Mr. POWER. Seventy percent-

Senator NUNN. Oh, I see, do not have.

Mr. POWER. That is across the board, and I would bet you that in the private sector, the percent who didn't have a warning banner would probably be higher. The government sector probably brings that number down because of DOD, I imagine, and Justice, which do have warning banners.

Eighty percent have a written policy on the misuse of computing facilities, but 61 percent say it is loosely enforced. Often, if a company has a policy, that is fine, and good, but it becomes effective when somebody, upon hire, sits down and signs an agreement saying, "I have read these information security policies and I understand they are part of my job. They are not just something that goes and collects dust somewhere." So 60 percent, loosely enforced. That indicates something. Even more disturbing, 58 percent do not have a written policy on how to deal with network intrusions. In other words, what happens when you have a break-in? There are whole procedures there that should go on. I think it is a serious issue for almost 60 percent of organizations responding not to have a policy on network intrusion.

Of those that do have a network intrusion policy, 50 percent of them do not include a provision for notifying the appropriate law enforcement authorities. Sixty percent do not have a policy for preserving evidence for civil or criminal proceedings. In other words, even something as simple as immediately upon detecting an intrusion, you make a backup. Something as simple as that would be a place to start, but beyond that there is a whole range of things you can do to make your case stronger.

Less than 17 percent who experienced computer intrusions in 1995 who responded to this survey reported them to law enforcement. When you look at it by industry sector——

Senator NUNN. Would you agree with Mr. Pethia's statement that one of the reasons they do not is because they do not expect anything to come from it and it is a lot of frustration? Why do you think, being in this business yourself, why do you think people do not report it to law enforcement?

Mr. POWER. I think that low expectation certainly is a major factor. But I think the overriding factor is negative publicity, fear of negative publicity and competitors exploiting it. Losing your job is another one. But I think that the misperception or the perception that nothing will come of it is strong.

Senator NUNN. Do you think that this sort of intrusion when there are serious consequences is getting reported to top management? Was that anywhere on the survey?

Mr. POWER. No, that is not on here. It is an interesting question. My guess would be that in many situations, the answer would be, "We do not want to know. Just deal with it." If it is reported, it is pretty much—if we can go back—"Did your best to patch security holes." That is with or without telling management. That is almost 45 percent. There is a serious problem there, but there have to be incentives. There is another figure farther along that is kind of interesting in that regard.

Over 70 percent cited negative publicity and fear of competitors as likely reasons for not reporting, but we allowed multiple answers here because we wanted to see just that kind of thing, for instance, the feeling that nothing might happen. It was interesting to me, over 70 percent said negative publicity, but also over 50 percent cited at least some unawareness that they could report. In other words, that would be not only not knowing who to call, I mean, people know there are law enforcement agencies. But they do not necessarily know that law enforcement agencies are ready to deal with network intrusions.

Also, 60 percent saying civil remedies seemed best (although I am certain 60 percent did not take the civil course) would seem to indicate they trust litigation more than criminal investigation.

Seguing off of that unawareness that they could report, note that over 80 percent said they would find it useful to receive a general presentation on computer crime from the FBI. Senator NUNN. So there is an education and learning curve here that could really be exploited, or an eagerness to learn?

Mr. POWER. Absolutely. I think that is a very critical point, if we can overcome some of that doubt that anything will happen and also the fear that it will be your worst nightmare to report some kind of incident. We can get people to come forward and report. I did not have time to get it together for you, but I would have liked to have seen the stock quotes for certain companies before certain incidents and after to see if you could really see if there was much of a difference in some of these things. But I think awareness and education is critical. There is an opening there in some of those last figures we looked at for education to make the situation a little bit better.

Senator NUNN. We will put your entire statement in the record. For both of you, any exhibits you would like to include will be part of the record. Go ahead.

Mr. POWER. Thank you. So just in terms of what needs to be done, it is our view that the preponderance of evidence indicates the problem of computer crime is only getting worse, and although heated debate over the U.S. export restrictions on cryptography would seem to suggest otherwise, encryption is not a panacea. All organizations with a public or a private sector must develop a comprehensive security plan. Encryption is a vital component but it is not the complete solution.

There is an insufficient level of commitment to information security. A serious commitment to information security translates into budget items for building information security staffs. A serious commitment to information security also means conducting a periodic risk analysis. security awareness for users is also essential. Even physical security is often overlooked.

There is a great need for emphasis on information security in computer science curriculum and computer ethics as a critical part of good citizenship. We want computers in every school in this country, and I think that is wonderful, but I think it is about time that in terms of—and Gene Spafford at COAST and others have really brought this forward, that part of software engineering and computer science courses, inherent components in these programs, should be information security.

Senator NUNN. Do many of the computer science courses, even college level, teach a course in computer ethics?

Mr. POWER. I do not believe so-there are very few of them.

Senator NUNN. Some of them do?

Mr. POWER. Some of them do, yes, and they are leaders in the field. But it is not across the board, and it should be. Information security should be an inherent part of computer science and computer ethics should be an inherent part of any education.

Then finally, two last things. These were brought up when Mr. Pethia was talking. The high-tech vendors of operating systems, applications, and hardware must begin to pay more attention, more than lip service, to information security. Things have been moving very fast. Everybody is interested in speed, ease of use, interoperability. Every organization has spent a lot of money on computers. They do not want to hear that now they have to spend some on securing them. But a lot of the fault for this lies in the products that have been put out there. The vendors have to make a more serious commitment in terms of information security.

And also, finally, and what I have seen here today is encouraging, I think there is a real need for collaboration and cooperation between the private sector, law enforcement, and the academic world in some new ways, and I hope that your hearings will be contributing to that.

Senator NUNN. As the awareness goes up about the exposure and vulnerability of private systems—I am not talking about government systems now—is it not likely that that will become a competitive feature in the hardware and software that is being sold? It seems to me that a company buying a system and deciding whether it is from IBM or Apple or whatever, plus all the software, would ask the logical question if they have begun to start thinking about this, and it seems to me that is one of the purposes of these hearings, as to what their security capabilities are in terms of being built into the software and the hardware.

Is that what you mean, Mr. Pethia, when you say that you believe the marketplace is going to begin to address these problems more seriously?

Mr. PETHIA. Yes, that is exactly what I mean. I think, ultimately, the reason for calling for a better job of collecting threat data, damage data, and making that widely available to the community, the public, is exactly that, to build that marketplace.

In a recent conference, a major vendor surveyed his customers and the requests for COBOL compilers on UNIX machines was far higher than the request from customers for improved security in the vendor's products. Currently, the vendors are not seeing any demand from their customer base for secure products. I think their responses—when we tell them about the problems, their response is very simple. Help me build a marketplace and I will respond to the demand, but currently, there is not one.

Senator NUNN. How much of a role do you think the government is going to have in this as opposed to the marketplace? Do you think that as awareness goes up, the marketplace is going to solve most of these problems, or do you think the government is going to have to do a great deal itself?

Mr. PETHIA. In my opinion, the government can do some things to act as a catalyst to spur marketplace activities into action. I do not believe that government regulation by itself or government actions by itself will really solve the problem. But I do think the government can help through things like awareness campaigns, making data available, sponsoring educational programs that are developed in the private sector to train practitioners to do a better job of understanding problems. Those things are the catalysts that will begin to get the marketplace to become aware of the problem and begin to get it to move.

Senator NUNN. Mr. Power, the same question.

Mr. POWER. I would certainly agree with that, except that I would also add that information security is a national security issue, as you have outlined today. So there obviously is a great responsibility and role for the Federal Government to play there. As all human commerce and communications moves into cyberspace, crime follows money and there will be an awful lot of crime in cyberspace. Somebody has to deal with that, so in the sense of law enforcement as a role, if there is no consequence to the crime, there is no deterrent. So, obviously, law enforcement has a role and that is yet to be sorted out.

Senator NUNN. We have very little deterrence today, do we? Mr. POWER. No.

Senator NUNN. Do you agree with that, Mr. Pethia?

Mr. PETHIA. Yes, very little. I do not think fear—even fear of being caught, let alone prosecuted, is really in the hearts and minds of the people who are attacking systems today.

Senator NUNN. Do you have any observations about any of the recommendations made by staff? Do you disagree with any of those? Would you like to add those? We have your own very helpful recommendations, but are there any of the recommendations that you recall made by staff this morning that you would either disagree with or have comments on?

Mr. PETHIA. The only one that leaps into my mind quickly is the need for mandatory reporting of security incidents. I do not understand how to implement that effectively from my experience, again, of when do people call and when do they not. I believe there have been mandatory reporting requirements in the DOD and other parts of the Federal Government for some time, and to my knowledge, they have not been effective in helping deal with this problem.

If we need reports, then I think we have to provide some kind of a service back to the people who we are asking to report to us. I think that is help in terms of securing their systems or help in terms of investigation or prosecution. I believe there has got to be a service component connected with any reporting requirement.

Senator NUNN. More than just saying it has to be done, you have to have some positive result that flows from doing it, is that right?

Mr. PETHIA. I have seen many corporate and civil agency security offices that have report drawers that are empty because when a report comes, nothing positive comes in return.

Senator NUNN. Mr. Power, do you want to comment on that, or any other recommendations that you would like to comment on?

Mr. POWER. I would concur with that. I would imagine mandatory reporting would really be something that you would have to look at segment by segment or sector by sector, something like that, depending on the nature of the information involved, perhaps.

Senator NUNN. You need a certain threshold of either damage or seriousness, too, do you not, so that you do not just get into a paperwork drill?

Mr. POWER. I think so, so there is that. But one point that I would just reemphasize that I heard throughout the testimony is that security awareness, education, training, the human factor is critical here. The discussion about encryption, I thought was very interesting because it highlights something about technology. Technology is only a component of the solution, whatever kind of technology it is, whether it is encryption, firewalls, or anything else.

Human beings are ultimately building systems, deploying them, and breaking into them. So it is human beings that we have to reach in terms of training, awareness, and understanding their responsibility, not only to their corporations or their job security but to their country, to the world, really. It is a global issue now.

Senator NUNN. Are there any other observations about the recommendations in particular?

Mr. PETHIA. No. I think the positive thing that I see here is movement toward action, which I think is necessary. We have talked a lot about this problem in the industry and in government for a long time. Moving towards action is positive. I think as we take that action, we need to be very careful to ensure that we turn around the current situation where the stigma attached to being a victim today is much worse than the stigma attached to being a perpetrator. We have to turn that situation around.

Senator NUNN. Thank you both. I hope you stay in touch. We appreciate both of you coming. I know you are from out of town and went to considerable effort to come and we appreciate it very much and we appreciate your staying in touch with us as we try to develop a legislative response, not necessarily laws but recommendations, as well as perhaps changes in the laws.

Mr. Rhodes, thank you again, and I hope you tell Mr. Bowsher and your other superiors that this Subcommittee greatly values what you and Mr. Brock have submitted to us. You have been very, very helpful. I have seen a lot of GAO reports, and I am not saying that all are not helpful, but there are degrees and this has been one of the best.

Mr. RHODES. Thank you very much, sir.

Senator NUNN. Thank you. The Subcommittee is adjourned.

[Whereupon, at 12:36 p.m., the Subcommittee was adjourned.]

SECURITY IN CYBERSPACE

TUESDAY, JUNE 25, 1996

U.S. SENATE,

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS,

Washington, DC.

The Subcommittee met, pursuant to notice, at 10:10 a.m., in room SD-352, Dirksen Senate Office Building, Hon. Sam Nunn, presiding.

Present: Senator Nunn.

Staff Present: Harold Damelin, Chief Counsel; Carla J. Martin, Chief Clerk; Ariadne Allan, Investigator; Daniel S. Gelber, Minority Chief Counsel; John Sopko, Minority Deputy Chief Counsel: Mary D. Robertson, Assistant Chief Clerk; Alan Edelman, Minority Counsel; R. Mark Webster, Minority Investigator; Claudia McMurray (Senator Thompson); Bill Greenwalt (Senator Cohen); Sandra Bruce (Senator Levin); David Plocher (Senator Glen); Corey Henry (Senator Dorgan); Jeremy Bates (Senator Dorgan); Todd Lawson and Alexander Selby, PSI Interns.

OPENING STATEMENT OF SENATOR NUNN

Senator NUNN [Presiding]. Senator Roth is unable to be here at the opening of the hearing, so I will preside until such time as he does come.

[Prepared statement of Senator Roth follows:]

PREPARED STATEMENT OF SENATOR ROTH, CHAIRMAN

This morning, we continue our examination of our Nation's computer security During the Subcommittee's recent hearings on this subject, we learned about the explosive growth of the Internet and the increasing number of computer intrusions taking place. Some of those incidents were quite serious. We also heard experts testify how victims' unwillingness to report computer intrusions to proper authorities both in the public and private sector, contributes to the problem.

both in the public and private sector, contributes to the problem. Computer technology has positioned the United States as a world leader in the information age. But ironically, our strength in this area has also become our Achilles' heel. In the world of cyberspace, anyone with a computer, know-how, and access to a network can wage an attack. Even those with little expertise can become skilled hackers by picking up tips posted on publicly accessible hacker bulletin boards. Unlike the real world, which has defined geographic borders, cyberspace is with

Unlike the real world, which has defined geographic borders, cyberspace is without boundaries. Intruders can penetrate our computer systems, and read, even steal files without ever leaving home, whether home is down the street, or halfway around the world. Intruders can even disguise their on-line identity and pose as authorized users. It is not hard to imagine what kind of damage such a masquerading intruder could cause.

The very technology which makes our computers capable of storing extraordinary amounts of data and handling complex calculations can also be used against us, to crack passwords and codes, and infiltrate supposedly "secure" systems. In short, the information age challenges us to rethink the way we protect and defend ourselves, our computers, our data, and our entire information infrastructure.

As the Internet continues to grow, it is crucial that we continue improving the security of our information systems. Improvements should include better training for computer users to ensure that they understand their role as gatekeepers, and more secure computer hardware and software that protects systems from outside attackers.

We must also strive to understand the nature of the threat facing our information systems. If your neighborhood was being targeted by a burglar, you would certainly want to know which houses on your block had been hit. Think how difficult it would be for law enforcement to catch a thief if victims did not report the robberies. Not only would police be handicapped in their investigation, but residents would be unable to take precautions to secure their property. Similarly, reporting, investigating, and analyzing information about computer intrusions will help all of us, in the public and private sectors, to protect our systems from future attack.

This Subcommittee has a history of focusing the public's attention on emerging security issues. I want to thank my distinguished colleague Senator Nunn for his ongoing work in this area and his staff for their preparations for today's hearing.

Senator NUNN. Today the Subcommittee holds the third in a series of hearings examining the security of our national information infrastructure. In previous hearings we explored the vast and growing dependency of critical parts of our society and government on computer information systems and the increasing vulnerability of those systems to disruption, manipulation and other forms of cyber attack. We also learned how difficult it often is to identify the source of cyber attacks due to the techniques used by attackers and the limitations under which our law enforcement and intelligence authorities operate.

This morning we will focus on the possibility that cyber-based attacks on our national infrastructure could be used as part of a coordinated strategic attack on the United States. How likely is such a scenario? Who has the capacity to launch such an attack? How do we defend against such an attack? Perhaps most important, would we even recognize the fact that such an attack was being carried out and be able to determine who was behind the attack in a very timely manner?

These are among the most important questions that we will attempt to ask our witnesses today. These questions all point to the critical role of intelligence in this area. As the Subcommittee staff pointed out in our last hearing, our intelligence agencies have acknowledged that potential adversaries throughout the world are developing a body of knowledge about Defense Department and other government computer networks. According to DOD officials, these potential adversaries are developing attack methods that include sophisticated computer viruses and automated attack routines which allow them to launch untraceable attacks from anywhere in the world.

Our government understands that many countries are developing offensive information warfare capabilities. The staff's report found that the collection and analysis of data that might provide the nature and extent of the threat posed to our information infrastructure is not presently enough of a priority in our intelligence community.

The staff is not alone in this opinion. The Brown Commission Report on Roles and Capabilities of the United States Intelligence Community observed that "while a great deal of activity is apparent in the area of information warfare, it does not appear well-coordinated or responsive to an overall strategy."

We are privileged to have the Director of Central Intelligence with us this morning. I hope that the Director will provide us with a sense of what we do know, what we do not know, and what we need to be thinking about when it comes to the potential for a cyber-based strategic attack.

Intelligence, however, can only take us so far. At some point, we must consider how we would respond to an actual attack if one were to happen. What are our options, and how would such decisions be made?

We will have a unique opportunity to explore these questions today in the setting of an actual war games scenario presented by our witnesses from the RAND Corporation. This scenario will hopefully provide the Subcommittee and the public at-large with a better appreciation for the difficult issues which must be wrestled with when it comes to information warfare.

The advance of the computer age has presented the United States with a whole new range of national security challenges. Just this past weekend, British authorities announced a second arrest in the case involving cyber attacks on the Rome Air Development Center at Griffis Air Force Base, a case which has been highlighted in the Subcommittee's previous hearings. Last year, a 16-year-old London resident was charged with carrying out these attacks. According to the reports, the individual arrested this weekend, a 21year-old resident of Wales, may have been the previously unknown "Kuji" who had tutored the 16-year-old on how to carry out his attacks.

What is perhaps most interesting is the fact that the charging document accuses this individual of acting with others in a conspiracy to carry out the attacks. Of course, we do not know at this stage who the others were. Could they have been foreign intelligence operatives or agents of a hostile foreign government, or were they just youthful hackers? In the cyber world, it could be possible that the two arrested may not even know the identity of their fellow co-conspirators.

Once again, this case highlights the need for sound policy for intelligence and for response planning. Just as we need to be attuned to the possibility of strategic attacks, we also must not over-react to every probe or attack. We must begin to prepare our defenses to these possibilities in a way that does not seriously dilute the advantages which are derived from dynamic new information technology. This balance will be a real challenge.

It is my hope that this set of hearings will provide some impetus to confronting these new challenges that lie before us.

On July 16, the Subcommittee will examine how our government intends to respond to this threat as we will have testifying before us Deputy Attorney General Jamie Gorelick and Deputy Secretary of Defense John White. These witnesses will relate recent efforts by the executive branch to address this challenge and our ongoing emphasis on the importance of this serious set of challenges we face.

Director Deutch, you have testified before the Subcommittee before. We appreciate very much your cooperation and the cooperation of your agency. We swear in all witnesses before the Subcommittee, so if you would raise your right hand and take the oath, we would appreciate it.

Do you swear that the testimony you will give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. DEUTCH. I do.

Senator NUNN. We have plenty of time for whatever statement you would like to make this morning, Director Deutch, so please go ahead and give us your statement, and then we will have questions for you.

TESTIMONY OF HON. JOHN M. DEUTCH,¹ DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Mr. DEUTCH. Thank you very much, Mr. Chairman. It is a pleasure to be here before the Subcommittee once again. With your permission, I would like to submit my prepared statement for the record and make some summary comments to allow as much time as possible for discussion.

Senator NUNN. I believe this is the first time that you will have testified in the open about this overall threat, isn't it—or have you testified before?

Mr. DEUTCH. That is correct. This is the first time I have addressed this subject in open testimony.

Senator NUNN. Well, your entire statement will be made a part of the record, and you go ahead and give whatever you would like to this morning, but we are not pushed for time, so if you would like to elaborate, feel free. Mr. DEUTCH. Mr. Chairman, I am here to address the subject of

Mr. DEUTCH. Mr. Chairman, I am here to address the subject of foreign information warfare programs and capabilities. Let me begin by giving you the definition that I am using today for information warfare. By that, I mean unauthorized penetrations and/or manipulation of telecommunications and computer network systems. That is the subject I am addressing—foreign threats to those kinds of systems.

I want to begin by saluting this Subcommittee for addressing this important subject; it deserves the attention of the intelligence community, it deserves the attention of the national security community, the law enforcement community, as well as private industry and private citizens.

There are two reasons to be especially concerned about information warfare. First, there is the growing dependence on worldwide information infrastructure in telecommunications and computer networks. Second, both nations and terrorist organizations can, with relative ease, acquire the techniques to penetrate information systems. That is what is different about this category of threat to our infrastructure from other kinds of threats, the conventional explosives or nuclear, biological and chemical—the growing dependence and relative vulnerability of the information infrastructure and secondly, the relative ease with which nations or subnational organizations can gain the techniques necessary for penetration of these networks.

¹ The prepared statement of Mr. Deutch appears on page 329.

Let me tell you the kinds of targets that are threatened by information warfare. The first is the domestic infrastructure, both the government sector and the private sector—for example, air traffic control, power plans and banks. The second category of targets which are threatened by information warfare involve international commerce, international funds transfer, international transportation and, of course, international communities. And finally, information warfare threatens our military forces whether they are deployed in peacetime or during operations in wartime. In some sense, Mr. Chairman, the electron is the ultimate precision-guided weapon. With appropriate knowledge, it can be directed directly to the command and brain structure of our military systems and our military forces. The electron, in my judgment, is the ultimate precision-guided munition.

Successful attack against systems, however, requires more than computer literacy. It requires sophisticated computer programming technique, it requires detailed information about the character of the target, the computer network or the telecommunications system that you are addressing, and it does in some sense require access to the target, whether by physical or electronic means.

This means that an undefended network will be more vulnerable to attack than a defended network, although the extent to which full protection can be provided and the cost that it would take to provide such protection is very much a matter of analysis and, I might say, of dispute at the present time.

Beyond these capabilities, there has to be intent. The intelligence community has taken some measures to try to estimate both the intent and the capabilities which exist in foreign entities around the world to attack the different kinds of targets that I mentioned before.

First, there is a highly-classified intelligence estimate that focuses on foreign attacks on the public-switched telephone network system of this country and supervisory control and data acquisition systems—the control systems that operate some of the critical parts of our infrastructure.

Second, separate assessments are available or underway about efforts to limit our information dominance on the battlefield, that you know that information dominance will be an important part of our future military superiority. We have studies underway to look at the vulnerability in military situations to attacks against our military forces and systems.

Third, we are alert to the possible future use of information warfare techniques by terrorist groups.

We have a number of specific intelligence community initiatives to address these threats. First, we have new collection activities and priorities designed to develop planned or actual foreign efforts to penetrate network systems. We are working extremely closely with the FBI and the Department of Justice on these issues in the case of targets which are based in the U.S. or where there is foreign criminal involvement.

As you will hear, Mr. Chairman, there is an interagency Critical Infrastructure Security Group, of which the intelligence community is an active member, with the Department of Defense, the Department of Justice. We are working together to assess and put into place programs and policies to deal with the vulnerability of our domestic infrastructure.

Third, we are forging relationships with industries that are beginning to address this subject on a worldwide basis where they find themselves in international commerce. The CIA and the DIA the Central Intelligence Agency and the Defense Intelligence Agency—have launched new analytical initiatives directed toward threat analysis and warning of information capabilities and intentions of foreign countries.

Let me say that the National Security Agency under its new director, General Minihan, is reorganizing this agency to address directly information warfare. An important part of this effort will be to establish a community-wide information warfare technology center which will provide us with the tools to deal with this emerging threat.

Senator NUNN. Where are you talking about housing that center? Mr. DEUTCH. That center will be, in my judgment, housed at the National Security Agency, and it will report, in ways yet to be completely defined, to myself and the Deputy Secretary of Defense.

Senator NUNN. Can you plug in the domestic side of that, the domestic law enforcement end of that, or do you cross jurisdictional lines in domestic versus foreign when you do that?

Mr. DEUTCH. My hope would be that this would be the place where we could produce tools to deal with these problems whether they are going to be used by domestic agencies or agencies which are involved in national security or intelligence. So it is more of a place to build the toolbox, do threat assessment and analysis, rather than a place to get involved in actual law enforcement or operational decisions. It remains to be worked out, but I am personally committed to seeing the establishment of that center at Fort Meade.

We have a major national intelligence estimate underway which will bring together all parts of the community including the Department of Justice, the Defense Information Systems Agency, the military, the FBI, criminal units from the Department of Justice, providing a formal intelligence estimate of the character of the threats from foreign sources against the U.S. and foreign infrastructure. We plan to have this estimate complete by December 1 of this year.

Let me stop, Mr. Chairman, with the following two remarks. Much needs to be done. This is a complex and very difficult subject. We are not well-organized as a government to address these issues. Traditional government methods are not enough. What is required here is very intense and deep cooperation with industry, those who own, build and operate the civilian infrastructure, and those who are closer to the very rapid technological change which is occurring—I am speaking here about the protection of our infrastructure. It really requires a different way of addressing what is a very major problem, and it is an intellectually demanding problem and is not one where it is absolutely apparent about the best way to proceed.

We are committed to continue to work with our colleagues in the executive branch and to work with Congress on what we consider to be a vital matter and a very, very serious emerging threat to our country and to our allies.

Thank you very much for your attention, Mr. Chairman. I will be happy to address any questions you may have.

Senator NUNN. Would it be fair to say that the technology is now outrunning by a substantial amount our ability to both organize government to deal with it and our legal system's reaction to it?

Mr. DEUTCH. Yes.

Senator NUNN. Numerous witnesses have explained the great difficulty in determining the origin of a cyber attack. For instance, because hackers "loop and weave," using those terms of art, and "spoof" from system to system, often criss-crossing national borders, we often cannot tell if an attack is from a United States person or from a foreign state. How does this affect both the intelligence community and law enforcement's ability to sort cut this problem and to work together?

Mr. DEUTCH. I think it is quite right to say that hackers and those who are adept at dealing with the information networks are able to move around surreptitiously, if you like. But this is not a new problem. This is the kind of measure/countermeasures game which intelligence organizations have dealt with for a long time, and I feel confident that with effort and with the development of both expertise and techniques, it is not in my mind an insurmountable problem. We will not be able to spot everybody or spot everybody quickly, but with time and with ingenuity, we will do well in defending ourselves in that kind of measure/countermeasure game.

Senator NUNN. It is not insurmountable, but we have not surmounted it yet, have we?

Mr. DEUTCH. That is absolutely right. I did not mean to suggest we had surmounted it. I am saying to you that it is a big problem; it is a huge intelligence infrastructure out there, and the possibilities to be attacked are endless, but it is not completely futile to try to stay in front of it and know where your highest vulnerabilities are and who your most determined adversaries are.

Senator NUNN. One expert testified and described cyber war as a great equalizer for rogue states or subnational groups, the logic of this statement being that these potential enemies do not need great funds, resources or even technology to launch a very effective cyber attack on our Nation's infrastructure.

Do you agree with this assessment, or is it going to be more difficult than that for someone to mount that kind of an attack?

Mr. DEUTCH. In part, I agree with that statement. It is the kind of statement that I might make and indeed I believe I have made in front of this Committee before about chemical warfare agents as well—a determined subnational adversary can get quite a long way there.

On the other hand, we do not want to make it that easy to do. As I tried to mention, it is not only knowledge of programming that is needed in computers. You also have to have a way to access the Net, you have to make sure you have the techniques available to penetrate the Net; so it is not altogether that easy to have the detailed knowledge of a network that you are hoping to attack or a point of access to it. Defense will help in this regard, but it will not be a full defense, just as it is not in the case of a CW threat from a terrorist group against an infrastructure country. So that while I think it is, so to speak, an attractive weapon of choice for a subnational group, I do not think it is all that simple to use.

Senator NUNN. It sounds like the obstacles you just put up would be more difficult for those over the age of 30. [Laughter.]

Every one of the things you listed, I think my son would be able to master pretty easily.

Mr. DEUTCH. It is either that or be an old man at MIT; you have two choices—excuse me—an old man or woman, Mr. Chairman.

Senator NUNN. Do we presently know enough about this threat given its potential to harm critical components of our Nation's infrastructure? What needs to be done so that the intelligence community can obtain greater appreciation of this threat? You mentioned some things, and I believe you mentioned that a joint assessment is taking place now.

Mr. DEUTCH. I do not think we know enough about this threat, and there are elements of it which are going to take a lot of work. We have to work with industry to understand how they see the threats to their own control systems, we have to work with the national security communications system, and of course, we have to do a lot more in understanding what the intentions are and the activities of foreign governments are in this area. So there is a great deal more work to be done here, but it is under way, and it is recognized that this is a tremendously important subject of high priority for the intelligence community.

Senator NUNN. Does this question about not knowing where the attack is coming from basically disrupt our ability to use traditional deterrent strategies? Are we going to have to rethink the whole question of how we deter when you cannot tell the origin of the attack?

Mr. DEUTCH. I do not think of this as being a deterrence issue; that would not be the way I would characterize it. I would characterize it as being a kind of defense in-depth sort of situation where it is not going to be one silver bullet that will make a network completely inoculated from potential penetration. So I do not think of it as a deterrent; I think you have to say that there are barriers to anybody who is going to try to get in. Barriers which raise the risk to somebody to be able to get in require more determination, require more sophistication to penetrate a network, and it will take some costs to do that. But I would think of it in terms of defense in-depth as opposed to deterrence. I do not think deterrence is going to be very helpful here.

Senator NUNN. We have used deterrence for a long, long time in our defense strategy. That is, if we are attacked, then whoever attacks us will be both detected, and we will mete out very severe punishment. We have used that in the Cold War, and we have used that not only with nuclear but with chemical; we have deterred chemical with conventional. More and more thoughts are that we can do that without having to respond with a chemical attack against a chemical attack and so on.

Are you saying we are in another era now where, basically, "deterrence" is not the right word to even think about in this area? Mr. DEUTCH. I would say—yes. I would not cast it as a deterrence problem. First of all, it may very much be a peacetime problem, an ongoing peacetime problem.

Senator NUNN. So it is not a deterrence problem, or is deterrence just no longer a tool, because deterrence has been the big tool. What you would like to do is not have to deal with an attack at all because you would like to prevent it from ever occurring. Are you saying that the word "deterrence" is not applicable in this case, that we are not going to be able to deter these kinds of attacks, that we have just got to deal with them—because I think that is what I heard you saying.

Mr. DEUTCH. Well, let me say that "deterrence" to me means to try to stop somebody from doing something by the threat of force, either an equivalent kind of force or a different kind of force.

Senator NUNN. Or punishment.

Mr. DEUTCH. Or punishment. I do not want to say that it has no role to play, but the way I think about it is more preventive defense, putting in a series of defensive levels which will buy you a certain amount of protection with the resources you are willing to commit and the ingenuity that you bring to the problem being important in that regard. I think of it more in those terms than I do in terms of deterrence, especially in the kind of peacetime situations we may find ourselves in in this ongoing problem.

I mean, it is going to be very hard for me to believe that if you have an information penetration and even a shutdown of one of your major systems, which may create all kinds of inconvenience and property loss, to know how to use military force as a balancer to that. But I regard—

Senator NUNN. I am not speaking of military force, but I am speaking of perhaps using some of the tools of information warfare to basically back up on the system that carries out the attack, so that the information system itself is the subject of very severe punishment and counterattack wherever it is coming from. I am not talking about using conventional or a weapon of mass destruction to go out to a computer hacker in London. What I am talking about is having some way in this information age to make it unattractive for the attack to take place in the first place. If we do not think in that vein, then we are just going to be into game-playing where everybody tries to hit us, and it becomes a game as to how we can defend against it.

It seems to me we have got to leap into the thought process at least of trying to use information warfare itself to be able to make an attack or even a serious illegal probe very unattractive to the potential perpetrator.

Mr. DEUTCH. Well, I want to say to you that I really think the first issue should be to make sure that the computer systems on which we rely most strongly have been thought of as being made as secure as is reasonably possible, and I think there is a way of thinking about that problem where you kind of defend in-depth. I think that that is important for this Nation and other countries to do.

Now, if you say to me what about deterrence or the ability to react by our own addressing other people's information networks, that is a subject that I am not prepared to discuss here today. Senator NUNN. But we are not forsaking that whole area that basically, if you fool with us, you are going to get hurt?

Mr. DEUTCH. No.

Senator NUNN. In the area of weapons proliferation, the intelligence community has a good idea of which countries pose threats—at least, that is one of the big goals we have—and what weapons they have; we keep up with the potential, we look at possible chemical production facilities in certain countries of the world, we look at the nuclear proliferation issue—we are taking that whole area of nonproliferation increasingly seriously, which is good.

Do we have at least as a goal to develop a similar intelligence baseline in the cyber world?

Mr. DEUTCH. We certainly do, and I think that we are making progress in that area. I described two or three steps that have already been taken. One is a very careful look at attacks on network control systems or publicly-switched networks, where those threats might come from. We are going to have a national intelligence estimate here by December 1. There are available some interesting and important first looks at vulnerabilities of military systems and exercises related thereto. So I think we are on our way to doing this, but the beginning of an intelligence priority or intelligence effort is by no means at the same level of development that the nonproliferation intelligence—

Senator NUNN. We are just beginning.

Mr. DEUTCH. We are beginning—everybody is together on the fact that it needs to be done, and resources are being allocated, and the importance of the subject is indisputable.

Senator NUNN.

We do not know now, though, which countries would pose the greatest threat in this area.

Mr. DEUTCH. No, I would not agree with that statement, sir, but I would not be prepared to go into greater detail on that.

Senator NUNN. We have some idea?

Mr. DEUTCH. Yes, sir.

Senator NUNN. Would you say it is not a mature assessment yet, that this is a beginning effort? How would you describe where we are now in terms of determining at least a sovereign state threat in this area?

Mr. DEUTCH. I would say we are pretty good, in pretty good shape in that—sovereign state, state-directed threats.

Senator NUNN. What about terrorist groups?

Mr. DEUTCH. Less certain—and of course, individual criminal elements or individual hacker activities, we are significantly less capable.

Senator NUNN. Without getting into any countries—I will not even ask you to name any countries at all—without getting into that at all, can you confirm whether foreign governments have indeed sponsored information attacks on our infrastructure?

Mr. DEUTCH. I do not want to get into it here, if I may, Mr. Chairman.

Senator NUNN. OK. The intelligence community ultimately will only be responsible for assembling a threat estimate or assessment of a foreign threat. What are we going to do in terms of the domestic threat—if there is a domestic threat—and based upon all the information we have, there very well could be. Whose job is that?

Mr. DEUTCH. That is the Attorney General's job, and I think that we do have in place working relationships that I am very, very optimistic about through this Critical Infrastructure Working Group that are going to address these issues from the perspective of domestic threats against domestic facilities, which is really not at all a foreign intelligence job.

We will, as I mentioned earlier, be producing techniques that we will provide to help and support and assist the law enforcement community to do their job with domestic threats against domestic infrastructure, and I am going to take every possible step to make all of those techniques available to Jamie or to Louis Freeh—

Senator NUNN. Jamie being Jamie Gorelick?

Mr. DEUTCH. Jamie Gorelick, right, who is Deputy Attorney General Counsel to the Department.

Senator NUNN. Is any assessment going on as to whether we need any laws changed in order for this coordination to take place between the foreign and the domestic? We had a chart up here at our last hearing—and I do not know if your people briefed you on it—that showed some real situations where the attack was coming through seven or eight different countries and basically could have originated here, going through all of those countries, and then coming back here for a target. So that the attack could have started in New York City or Atlanta, Georgia and gone through terminals all over the world and come back with the target right here. So it could have been made to look for weeks and weeks as if the attack was coming from a foreign source when it was actually domestic or vice versa.

Mr. DEUTCH. Those kinds of situations, whether hypothetical or real, are extremely easy to specify. But what is not clear to me is what does a legislative or legal solution look like. In other words, I am not prepared, but I do not know that anyone is prepared, to put forward any changes that might deal with these situations.

What there is, both at the policy level and at the working level, is an absolute commitment to share information or work as closely together as possible on these subjects. But I think we are far, far from——

Senator NUNN. We are a long way from being able to come up with any kind of——

Mr. DEUTCH. With a crafted piece of legislation that we would know to do more help than harm to the situation

Senator NUNN. The most serious challenge, it would seem to me, legally and jurisdictionally, is when the attack was really coming from a foreign country but it appeared to be coming from here. If all appearances were that the attack, on let us say a Pentagon filing system or computer system was coming from a foreign country, but it was disguised through six or eight terminals here first, that would basically make it difficult to have our intelligence apparatus fully engaged, would it not?

Mr. DEUTCH. It does, but there are other situations where that difficulty arises, counter-narcotics being a prominent example, where the real origin of where a drug or money laundering operation comes up is also unclear at first glance. And we all know, if we had clarity, where the responsibility lies; we all know that there is both policy guidance and, at the working relationships, progressively better ability to cooperate to go after these problems, and therefore, well-intentioned people will make progress on this issue. So the point you mention exists in counter-narcotics and international crime as well, where there can be an ambiguity of where is the source and where is the destination.

Senator NUNN. The difference here is that you can carry out this attack in the matter of 2 or 3 minutes.

Mr. DEUTCH. Yes, that is right, and it is more challenging, but conceptually, it is not—I do not know how to get rid of this problem by a piece of legislation.

Senator NUNN. Nor do I; I do not have any recommendations on this now. I do think we have got to start thinking through it, though.

Mr. DEUTCH. Yes.

Senator NUNN. I think we have really got to do some thinking about it.

Mr. DEUTCH. Well, what I can report to you is an absolute convergence of views on this matter between the Attorney General and myself, and all the way down the line in my organization and I believe in the Department of Justice as well. We have spent a lot of time talking about this. Janet Reno has been extremely interested in this subject, and from crisis response all the way to these longerterm issues, we are determined to work together on it, as are our organizations.

Senator NUNN. In our staff report published earlier this month, the staff recommended that the Director of Central Intelligence complete a threat assessment and include an unclassified version that would be available to the private sector so they could better manage the risks posed by this threat.

First, do you think that is a good idea, and second, is there another, better way of dealing with the private sector?

Mr. DEUTCH. Well, I think in matters where there is a threat to the private sector—kind of a counterintelligence problem, a threat to the private sector—there are mechanisms that we have to share the results of the threat assessments and the vulnerabilities we see directly with companies, and I would expect that the results of any of our assessments would be shared in an appropriate way with U.S. companies to give them information about the threats that we see.

Senator NUNN. I believe in your statement you said that is pretty difficult to do right now, isn't it?

Mr. DEUTCH. The unclassified statement, I think is what it said, isn't it? Just the unclassified statement, but we have ways of communicating with companies when there are direct threats; with law enforcement officials, we can communicate classified information.

Senator NUNN. But haven't you found the private sector very reluctant to share information in this area?

Mr. DEUTCH. Well, no, not with us; no, sir. We find the private sector on this problem is very cooperative indeed and very, very conscious of the character of the threats they face but, like us, not clear how to solve them quickly and efficiently. Senator NUNN. I was just reading your statement at page 7: "I believe that foreign organized crime is behind some of these events, and we are eliciting the private sector's help in looking for evidence of foreign involvement and sponsorship. However, obtaining computer intrusion data from U.S. banks, telecommunications companies and other institutions has been difficult. Although the situation is improving, many of these firms are still reluctant to share information on intrusions for fear of losing consumer confidence."

That is what we found, and it sounds to me as if that is what you found as well.

Mr. DEUTCH. I am not sure exactly how to square the circle here, but let me say to you that if you are talking about public admissions by companies about the problems that they have encountered, this is certainly an accurate statement, the one that is written, if you are talking about public admission about this, public discussion of it. If you are asking about cooperation of companies, certainly with us or with the law enforcement community, about the kinds of problems they are worried about and perceive, I would phrase this differently, and if you permit me, I will make that clarification for the record.

Senator NUNN. Well, we have run into exactly what your statement says. That has been our experience, that there has been great reluctance by the private sector to discuss the threat that they face and even the attacks that have already occurred because they fear that the word would go out that they are vulnerable and therefore could destroy or damage consumer confidence and thereby cost them business. At some point, there has got to be communication here.

Mr. DEUTCH. That is correct, and I think that this is only an issue about whether it is done completely publicly or whether there are more channels for more confidential exchange of what their impressions are and their vulnerabilities are.

Senator NUNN. I think there has got to be some confidential exchange here; I do not think there is any doubt about it. The question is how to set up—is that one thing that you all are looking at? Are you looking at that?

Mr. DEUTCH. Yes, yes, we are. We have actually ways of doing that now. That is why I want to clarify the statement.

Senator NUNN. We would be interested in hearing more about that.

In March of this year, the Brown Commission said that collecting information about the information warfare threat is a "legitimate mission of the intelligence community." They went on to say that "while a great deal of activity is apparent, it does not appear wellcoordinated or responsive to an overall strategy."

Do you agree with this Brown Commission assessment?

Mr. DEUTCH. Well, the moment I saw this, I asked my friend Secretary Brown about it, because I certainly agree with the statement. What I was curious about is that the Commission did not make a hint of what the character of that solution should be.

The problem here is a complicated problem, and it is much easier to note the absence of a solution than to begin to craft the character of a solution.

Senator NUNN. But they said there was an absence of a strategy.

Mr. DEUTCH. A strategy for achieving a solution—I think it is a correct statement. What I am saying is that it is a very complicated problem, and we need to have really a lot of thought about how to do this right, and it has to involve the private sector; it cannot be done by the government alone. So it is a complicated issue, and noting it is not enough. A hint of what a strategy would be would be very welcome.

Senator NUNN. In other words, you are saying to Harold Brown: "What is the answer?"

Mr. DEUTCH. You've got it.

Senator NUNN. OK.

Mr. DEUTCH. And he did not have one, I might say. [Laughter.] Senator NUNN. In our staff report, we recommended the creation of a national intelligence infrastructure threat center, which would include representatives from the law enforcement, intelligence and defense communities as well as liaison with the private sector. This proposal would include real-time, 24-hour response capability, and the center would serve as a clearinghouse for intrusion reports. Is this the type of response needed in some form, or is this something that has not been decided yet?

Mr. DEUTCH. I noted that, and it is an interesting proposal. The way I think about it is a little bit different. One is a crisis response, if you like, or a near-term, real-time response center, which I think—I am speaking here for the United States, civilian infrastructure, not military; military would be handled slightly similar, but differently, and it is a Department of Defense responsibility. That would be a Justice Department responsibility.

Longer term, the threat assessment is the intelligence community's responsibility, and I think we are going to be addressing that both through our efforts at this information warfare technology center that I mentioned to you earlier and in our normal estimative process. But the idea that you have to have both a place to go for response to threats in the near term, or incidents in the near term—an incident response capability is very important as well as a continuing way of getting a community-wide focus on the assessment of what the threats are at any point in time and in the future from there. So both are needed. I would think that you would want to separate the incident response or near term part of the responsibility—that is in the Justice Department for the civilian infrastructure—and in the Department of Defense for military national security systems. The longer-term assessment is really an intelligence community responsibility.

Senator NUNN. If you gave some sense of priority in terms of the threats we face in the future, where would this overall threat we are discussing this morning—the whole threat of cyberspace attack, both in terms of defense resources as well as infrastructure, economy and so forth—fit in the scale of potential threats?

Mr. DEUTCH. I would say it is very, very close to the top, especially if you ask me to look 10 years down the road. I would say that after the threats from weapons of mass destruction, from rogue states and the proliferation of nuclear, chemical and biological weapons, this would fall right under it; it is right next in priority, and it is a subject that is going to be with us for a long time. It is not going to be handled in the next 6 months or 18 months. The threat is going to evolve, and our ability to deal with that threat is going to take time. The scale of time here, I think, is more like decades than it is months.

Senator NUNN. Have you at this time identified any subnational groups that pose a threat to our information infrastructure? If I ask you something that is better classified, then just so respond, but do you have subnational groups that you have identified, and are you watching this area?

are you watching this area? Mr. DEUTCH. Yes, we are very closely, as I mentioned in my statement and my comments, and I think that is a subject that is better not addressed in open session, Mr. Chairman.

Senator NUNN. If you were laying out now where you would like to see our intelligence community in terms of capability 2 years from now, what would be the major goals that you would enumerate in this area? What would be the areas of significant improvement in the intelligence community between now and, let's say, 2 years?

Mr. DEUTCH. Well, I can give you three or four. I would begin by saying that I am very keen on seeing a central community place to work on the technical tools necessary to work on this problem of protecting our military or civilian infrastructure. So the creation of this information warfare technology center, with an appropriate charter to serve both domestic and military security, is very important and is high on my agenda.

The second is to assure that we put into place in collection and analysis a very strong capability to track what the threat is going to be from nations or subnational groups—serious threat.

The third subject would be one which I think I would call "defense in-depth" and you would call "deterrence"—making sure that we are able to deal with these matters should they occur, wherever they may occur and under whatever circumstances they may occur, respond to them.

So those are the three that I would say for the intelligence community. Now, that does not talk about a strategy for dealing with protecting the infrastructure. That is not an intelligence community role; that does not deal with the problems of protecting the national security infrastructure, and it does not address, although it is an important part of my own thinking, the international aspects of intelligence community activities, how we talk about this with our allies.

Senator NUNN. How far along are we in terms of talking with our allies in intelligence areas? Is this an area where we can make dramatic improvements in terms of dealing with our allies, or have we already embarked on that?

Mr. DEUTCH. Dramatic improvement is possible—and needed. Senator NUNN. So it is on the agenda?

Mr. DEUTCH. Yes, sir. I tried to point out four things there.

Senator NUNN. Would our allies, generally speaking, without getting down to specific cases, be receptive to working with us in this area?

Mr. DEUTCH. It depends on which ally you are talking about. Of course, their capabilities for doing it differ very much.

Senator NUNN. Are we going to run into a situation where our normal allies in the security field may be on the other side of the fence in this area, based on competitive business practices and basically private sector invasions of privacy? Are we going to be in an area where we have a different set of allies than we would in the national security field in the normal sense?

Mr. DEUTCH. Well, it is always a problem. As you know, Senator, it is a subject which I have been very—as has Bill Perry—integration of our security is very important, and you are in a situation here where, when we put forward proposals in this area, especially the Europeans feel that they do not have as much capability in this telecommunications computer network as we do—software. So it is a problem. There is kind of an industrial problem in dealing with them on the subject, yes, but it has to be addressed and it has to be worked out with them.

Senator NUNN. Without getting down to specific cases, are you aware of private sector companies attacking each other's information systems for competitive economic purposes, both within this country and abroad?

Mr. DEUTCH. Not within this country, sir. That is outside of my purview. Outside of this country, yes.

Senator NUNN. So there have been private sector attacks on other private companies from outside this country against American businesses?

Mr. DEUTCH. Well, not only against American businesses, but industrial espionage does exist in the foreign world, sir, against everybody.

Senator NUNN. And it exists also in cyberspace.

Mr. DEUTCH. Yes; cyberspace, yes, sir.

Senator NUNN. To whom would we ask the question about American companies attacking American companies? Would that be the Attorney General?

Mr. DEUTCH. Louis Freeh.

Senator NUNN. Again, if this attack came from a foreign source, it would presumably get your attention before you immediately threw up your hands and said, "This is not in our jurisdiction," because for a while, it would look like it was coming from another country.

Mr. DEUTCH. Yes, you are absolutely right. And of course, there is also the problem of what do you mean by a domestic or a U.S. company at the same time. Some of these countries are spread all over the place. They are certainly conscious of this, despite page 7 here; they certainly are very conscious of this.

Senator NUNN. Has the executive branch started working out its own procedures? Is the CIA likely to get into a situation where you basically, in an effort to prevent foreign attacks on our infrastructure, inadvertently run into a domestic situation that should have been from the very beginning handled by the Justice Department? Do you have rules and regulations now that are going to be able to protect you from that kind of jurisdictional problem?

Mr. DEUTCH. Yes, sir. First of all, I want to point out that I am speaking to you today from the perspective of the whole intelligence community, not just CIA.

Senator NUNN. Right.

Mr. DEUTCH. A lot of comments I have made are for the National Security Agency and the Defense Intelligence Agency; I want to make that point.

But the answer is that we have routinely—routinely—when we encounter things which are not in the jurisdiction—we encounter an American citizen in some situation—we have a routine, absolutely sound basis of turning it over and looking at it cooperatively with the FBI or the DEA or the appropriate law enforcement agency, and it will certainly come up in this case.

Senator NUNN. There are some who believe we are going to have to have an electronic Pearl Harbor, so to speak, before we really make this the kind of priority that many of us believe it deserves to be.

Do you think we are going to need that kind of real awakening, or are we fully alerted to this danger now, and are we allocating sufficient resources?

Mr. DEUTCH. I think that we are fully alerted to it now. I do not know whether we will face an "electronic Pearl Harbor," but I am sure we will have some very unpleasant circumstances in this area, or our allies will have unpleasant circumstance in this area. So I think that while we are fully alerted to it, it is not as if we are asleep on the subject, but I am certainly prepared to predict some very, very large and uncomfortable incidents.

What about resources? I think resources are being allocated to this problem in its many different dimensions, everywhere from protecting the infrastructure to intelligence collection, which are reasonable, and they are moving in a direction of greater allocation. So the answer to your question is I think the resource stream is moving in that regard; the priority has been given, and it is moving along, sir.

Senator NUNN. Right now, you do not think there needs to be any more budget for at least the agencies within your jurisdiction in terms of being able to prioritize and put the resources required into this area.

Mr. DEUTCH. I believe we have the resources necessary to do the job, sir.

Senator NUNN. The Department of Defense has stated that there were some 250,000—that is their estimate—attacks on unclassified but sensitive networks. The question that arises there is, based on your previous hat that you wore in DOD as well as your present, are we putting too much information on these networks, making it impossible to protect, or is this a necessary flow from the information age we are in?

Mr. DEUTCH. Well, first of all, I want to tell you that I congratulate Emmett Paige, the Assistant Secretary, and General Edmonds, the head of DISA, for their initiatives on doing this examination in a rather clever way of the likely intrusions on DOD computer systems and networks.

My answer to you is that the benefits of those networks are huge, and so if you ask have we done too much, that has to be measured against the benefits of wanting the network. And the answer is that I think it is wise all the way over on the benefits that come from making use of telecommunications networks, that indeed there are so many benefits, we become so reliant that we must go back and do a little bit of work on the vulnerabilities in the defense. That is really what we are talking about—how much and how, and how to do it best. But we are not going to see this threat roll back the information age. It is a part of what is—

Senator NUNN. It would be counterproductive if we allowed that to happen.

Mr. DEUTCH. Absolutely, and I hope that no comment that I have given to you suggests that we should not be moving to take advantage of this tremendous security and commercial advantage that we have in pushing information technology. We do have to recognize that there are some elements that have to be—like buying the lock to go with owning a house—paid attention to; they are not going to be perfect, but they will minimize unauthorized penetration or manipulation of these telecommunications and computer networks.

Senator NUNN. It seems to me that what is different now is that there is a lot of information that is sensitive but not classified, so that the chances of linking up a lot of that information creates a situation where the whole becomes much more dangerous in terms of release to your adversary than the individual parts. In other words, it would have been very hard for someone to link up 10 or 15 different parts of this different information. Today in the computer age, all of those parts that are sensitive could be linked up sometimes in a matter of minutes. Are we going to have to take another look at how the whole product could be put together and thereby take another look at what we call sensitive versus classified?

Mr. DEUTCH. I do not know that that is the key, the key of sensitive versus classified, but you do make a very good point. What is different here is that geography and time have been completely changed around. It does not matter where you are at to remotely go after a piece of information or to put pieces of information together, so geography becomes significantly less important, and time becomes significantly more compressed.

So I would say that it is geography and time here which have changed from the days when you had paper and file cabinets. That is what makes this such a challenging problem and indeed introduces some of the difficulties that you mentioned earlier in terms of the historic rules about the difference between foreign intelligence and law enforcement and trying to do that around the boundaries of the United States. The protection of U.S. citizens is one distinction, but also the international/national distinction is broken down here.

Senator NUNN. As you know, Director Deutch, we have had continuing dialogue and some disagreement between the Armed Services and Intelligence Committees on the whole reorganization of your community and how that interrelates with DOD, and jurisdictions and so forth. Is there anything in any of those proposals that relates directly to this? Do you have sufficient authority now in this area, from your point of view, and sufficient jurisdiction?

Mr. DEUTCH. Yes, sir.

Senator NUNN. So there is nothing in that kind of dialogue that would basically play a big role here?

Mr. DEUTCH. That is correct. There is nothing, I think, in this subject—there is nothing in this subject which really bears on that on the present discussions, and I actually think we have managed all that—in fact, I think that whole issue is, hopefully, behind us. Senator NUNN. We do, too.

Thank you very much. We appreciate your testimony and your cooperation. We are going to continue our focus in this area, so we look forward to continuing the dialogue with you and getting your best advice.

Mr. DEUTCH. Thank you, sir.

Senator NUNN. Thank you.

I am going to ask all of our witnesses to please remain standing for just a moment, let me introduce you briefly, and then we will have each of you take the oath and go from there.

Our next panel this morning will be Roger Molander and Robert Anderson of RAND Corporation, and Peter Neumann of SRI International. These witnesses will discuss the threat outlined by Director Deutch and present an "info war scenario" that will help illustrate the challenges we may confront in the future. Along with these witnesses will be other contributors to RAND's war games scenarios.

Dr. Molander has been with RAND since 1989 and has testified before the Armed Services Committee in many other areas. He has been a project leader on a variety of national security studies on nuclear proliferation, information warfare, and has been a leading defense thinker for a long number of years and has been very valuable to our Committee.

Dr. Anderson has been associated with RAND Corporation for 28 years serving in various capacities including head of its Information Sciences Department and Director of its Information Processing Research Program. He has written extensively on the topic of information security.

Dr. Neumann has been involved with computer security issues for most of his career, has worked with numerous government agencies including those involved with national security, law enforcement, air traffic control and space exploration. He is chairman of the Association for Computing Committee on Computers and Public Policy and runs the Internet News Group, "The Risk Forum," which he started in 1985. He recently published the book, "Computer-Related Risk."

Why don't we take a 1-minute break, and as soon as Dr. Neumann comes, we will swear everybody in together.

[Pause.]

Senator NUNN. Dr. Neumann, you have been well-introduced, and if you will remain standing, I will ask everybody to take the oath. Do you swear the testimony you will give before this Subcommittee will be the truth, the whole truth and nothing but the truth, so help you, God?

Mr. NEUMANN. I do.

Mr. MOLANDER. I do.

Mr. ANDERSON. I do.

Senator NUNN. Thank you.

Dr. Molander, I believe you are going to lead off; I know you all have a fascinating little scenario you are going to unfold for us this morning. We appreciate you being here. I read your excellent publication, and I am really gratified that you all have been working in this area.

TESTIMONY OF ROGER C. MOLANDER,¹ NATIONAL SECURITY RESEARCH DIVISION, RAND CORPORATION, ACCOMPANIED BY PETER WILSON AND ANDREW RIDDILE

Mr. MOLANDER. Senator Nunn, thank you for the opportunity.

We are going to use some slides and basically, over the next hour and a half, go through something that is very close to the kinds of exercises that we have been conducting at RAND on this subject. With a little luck, technology will produce the first slide.

I will first describe what we mean by a term that we use, "strategic information warfare." Then, Peter Neumann of SRI and Bob Anderson of RAND will give you some additional perspective on this problem, drawing on their own lengthy experience dealing with both the technological aspects of the information revolution and the issue of information security.

We will then go through an example of the kind of strategic crisis that we have been employing in a series of RAND exercises which have focused on the decisionmaking challenges that would face a President or a Congress—really, the country—in dealing with a real crisis in which a strong strategic information warfare, a strong cyberspace warfare component, would take place.

Then, finally, as a wrap-up, I will give you some additional perspectives obtained from our work to date in this area and look at a number of key unresolved issues.

Strategic information warfare can best be thought of as the intersection of two either ongoing or candidate revolutions—"revolution" is a big word. The first is that ascribed to information, of which you have heard much in these hearings; but at virtually the same time that the information revolution is washing over us, there is also taking place in the world of international politics and warfare a change of possibly comparable revolutionary magnitude in what is called "strategic warfare."

In the period of the Cold War, strategic warfare came to be synonymous with nuclear warfare, but then the end of the Cold War came very fast and very unexpectedly, and no one had thought very much at all about what strategic warfare would be like in a multipolar world where adversaries might have regional rather than global strategic objectives and where they might choose to use nuclear and other weapons of mass destruction to achieve regional strategic objectives and possibly choose to use information warfare tools and techniques for such purposes as well.

It is the intersection of these two ongoing revolutions, strategic information warfare, a very new subject which has been emphasized and should be reemphasized as we look at this subject that we are talking about here today.

If you were in the strategic warfare business in the Cold War like some of us were, you were principally in the business of holding at risk to nuclear attack key strategic targets and in particular key infrastructure targets.

¹ The prepared statement of Mr. Molander appears on page 337.

When we look at the prospect of strategic IW, if you will allow me to use that shorthand, it is again the holding at risk of key infrastructure targets that is a principal concern, such as those highlighted in the graphic here.

Two principal categories of strategic IW attacks appear to warrant careful attention. The first, a carryover from the Cold War, a direct threat against the U.S. homeland, the possibility that the same infrastructure targets that were held at risk to destruction or massive destruction by nuclear weapons might be held at risk to disruption, possibly massive disruption, by information warfare tools and techniques by a peer competitor—a Russia or a China.

The second concern, which I mentioned earlier, is the possibility that a regional adversary could attempt to use strategic IW attacks to deter or disrupt U.S. involvement in regional conflicts either by successfully disrupting U.S. deployment, as was mentioned earlier, or by possibly targeting a key regional ally or coalition member who, under strategic IW attack, might refuse to join a coalition, or quit one in the middle of a war.

But would a regional adversary choose to use strategic IW tools and techniques from among the many other candidate strategic weapons that he might have in his armory? We need to ask in this situation what kind of strategic objectives such an adversary might have in, say, the Persian Gulf or East Asia and the risks and tactics that he might undertake to achieve these objectives in a strategic campaign.

Would cyberspace attack be more attractive than, say, a CW or BW attack to deter U.S. involvement? Would an adversary see value in the launching of an anonymous cyberspace attack which is potentially at his disposal? Would he target current U.S. regional allies or coalition members first or very early? Would U.S. conventional capability deter a cyberspace attack?

These are the kinds of issues that render thinking about strategic information warfare and adversary strategic campaigns both challenging and relevant.

With these kinds of concerns in mind in December of 1994, OSD(C3I) asked RAND to take a methodology that we had been using to examine the counter-nuclear proliferation problem and apply it to the strategic IW problem with the objectives shown here to try to get at the major features of this new subject, to try to illuminate some of the policy and strategic issues, to sharpen senior executive focus—following your comment about people over 30 struggling with this subject—in the defense and intelligence communities, and in particular also to engage broader government and, as mentioned very strongly, industry leadership on the major implications of strategic warfare.

The next chart, which I will not go through, summarizes the more extensive exercises that we conduct in these exercises. Very briefly, we conduct a half-day of exercises, three steps, in which the first two steps, which are the two on the right, take place in the context of a challenging escalating future crisis, which is what we are going to present to you a little later. The challenge to the participants—usually several groups with the same tasking, partly to keep people from fighting the scenario—is to devise an issues and options paper for the President in the midst of a crisis in preparation for an NSC meeting—a classic kind of principals get-together.

And then, in the third and final step of the exercise, participants return to the present and consider the challenge, as you are doing in your hearings, of deciding what issues in this arena might be ripe for decisionmaking in the relatively near term, possibly ripe for legislation, basically to initiate an action plan on this subject.

Last year, several hundred senior participants from government and industry took part in a series of exercises similar to the one you are going to go through here shortly. We have recently completed another series of exercises on a new and more challenging scenario.

In looking at these kinds of scenarios in contrast to traditional concerns about, if you will, overseas power projection in a regional crisis, we are instead looking at basically four theaters of operation—the possibility that a threat could come against the U.Z. zone of interior, the possibility of a threat against U.S. deployment taking place in some region, and here, calling up the particular scenario that we are going to go through, the possibility that threats could take place against Saudi Arabia in its own zone of interior, and then the whole business of what would happen on the battlefield. This last threatee has not been the subject of our exercises but is something that we all know, as Mr. Deutch mentioned, is a serious problem.

With that as an introduction, what I would like to do now is turn to Bob and Peter and let them give you some of their perspectives, drawn on long experience in the whole cyberspace world, and then with the help of two of my colleagues, Peter Wilson and Andy Riddile, we will go through the exercise and invite you to put yourself in the kind of situation that we might face in the future in this country.

Senator NUNN. Mr. Neumann.

TESTIMONY OF PETER G. NEUMANN,¹ AUTHOR AND PRIN-CIPAL SCIENTIST, COMPUTER SCIENCE LABORATORY, SRI INTERNATIONAL, MENLO PARK, CALIFORNIA

Mr. NEUMANN. Thank you. Senator Nunn, I would like to commend you for bringing into an open forum a lot of issues that have been discussed very obliquely in the past, and in particular, a lot of the discussions that have gone on in the past relating to, say, classified information, where the statement is made, "Well, if you knew what we knew, you would not do that."

One of the most fundamental conclusions of our National Research Council study of cryptographic policy was that not only must the debate about United States cryptographic policy be conducted in the open, but that it can be conducted in the open, and that after having looked at a lot of the classified information, our panel—which consisted of a former Attorney General, a former Assistant Attorney General, a former Deputy Director of NSA, and so on, and the Chairman, who briefed a Senate Committee last week—Ken Dam, who was a former Deputy Director of State—this group came to the conclusion that the debate must be conducted in

¹ The prepared statement of Mr. Neumann appears on page 350.

the open and that it is easily possible for the major arguments to be made in the open.

With that much as a preface, I would like to say that in the 10 minutes that I am supposedly taking, I can give no easy answers. There are no easy answers, and it would be fatuous of me to try to suggest that there are easy answers. The most fundamental recognition here is that the problems are, as Director Deutch said, very difficult.

The main thing is that we need to recognize this, we need to recognize that the infrastructure, from the point of view of the computer operating systems and the networking software and the uses of cryptography and the uses of the electrical power distribution and the telephone switching networks, are all very much at risk today. The computer systems have not had a great deal of emphasis on security. Even though the vendors will tell you in general that those systems are secure, experience shows that essentially every digital system can be taken apart with relative ease by somebody with a little bit of knowledge.

Director Deutch suggested that it takes a good bit of knowledge; it no longer takes a good bit of knowledge because the underground bulletin boards and E-Mail distributions tend to distribute information faster than the people who need to defend themselves can take care of the systems. The vendors are much slower in patching systems. In general, patching does not work; you cannot patch a system that was badly designed in the first place. You may patch it until you are blue in the face, and every time you put in a patch, you introduce several new errors or flaws.

I would like to very briefly run through the talking points at the beginning of my printed statement, and I will leave the rest of my testimony to be read somewhat leisurely—I think perhaps you have read it already——

Senator NUNN. The 10 minutes is just a guideline; if you spill over a minute or two, that is all right.

Mr. NEUMANN. Well, I am known for going for long periods of time, so I would not want to get started. [Laughter.]

The first point is that we are massively interconnected. Bob Morris, who was formerly chief scientist of the National Computer Security Center, made a statement back in September of 1988 that to a first approximation, essentially every computer in the world is connected with every other computer in the world. It is 8 years later, and it is vastly truer now than it was then.

The second point is, as I have already suggested, that there are enormous vulnerabilities. I have suggested that maybe there are security flaws in the operating systems, in the networking software and everything else, but I should also point out that there are great dependencies on the reliability and the system survivability of that infrastructure and that the security issues and the reliability issues are very closely coupled. If you have a system that is not reliable, it is not secure. We have had cases where the entire password file was printed out as the message of the day because of a design flaw in the system. We have had cases where a security flaw resulted in the entire system becoming unreliable. So these two things are very tightly coupled, and in my role as designated holist, which I often play, I would point out that the issues of system reliability, system security, even safety, in terms of air traffic control systems and things like that, are all very tightly interrelated.

So the problem we are dealing with is not just palliatives of what can we do to make things look a little bit better. It is a very fundamental retake of the entire infrastructure. And I think the important thing here is that the infrastructure itself is fundamentally vulnerable whether you are talking about all of the things that are on this chart on display or whether you are talking about the Internet and the way it is going to be in the future, with massive commercial interests saturating the Net with junk mail. The problems are getting worse faster. As Yogi Berra once said, "It gets late early." And it is getting late, very late, in this process of trying to resuscitate an infrastructure that, although it may look pretty good, is riddled with holes.

Experience shows that, as I said, essentially any digital system can be taken apart by a skillful attacker. More likely, it is going to fall apart of its own simply because it was not designed to anticipate all of the strange conditions that might occur.

So there are many cases in the past that you need to look at. You have already heard about the Rome Lab case, and you remember the Citibank penetration. You have heard about some of the crypto attacks on 40-bit crypto; 40-bit crypto is no longer very adequate.

There are many problems that are similar in terms of their mechanisms where we need to learn the lessons of the past. I go way back to the power outages in the early days, in the sixties and seventies. In the eighties, we had the entire ARPANET go down for a long time, 4 hours, which was a major outage at the time, in a manner that people said was absolutely impossible and could never happen—where one node in the network in fact contaminated every other node, and the entire network was shut down.

Ten years later, we had the AT&T long-distance problem where, for 11 hours, you could not get a long-distance call through; the same mechanism was involved—one node contaminated all of its neighbors, which contaminated all of its neighbors, and after a period of time, the entire network was effectively useless. NETCOM had the same experience last Wednesday in the sense that it had to shut down its operations for 12 hours.

We keep having similar problems, and you can say, well, that is a reliability problem, not a security problem. In the case of both the ARPANET collapse and the AT&T collapse, it could have occurred as a result of a penetrator triggering the event that eventually caused the actual reliability problem.

So my point there is that we really need to look at the problem in a much broader context. It is not merely a security problem. It is also a system survivability problem, it is a reliability problem, and these are all very tightly coupled.

So our defenses against isolated attacks are fairly bad, but when you start talking about coordinated attacks, the situation is much gloomier. A skilled set of attackers who were to have sufficient knowledge of how the infrastructure works could bring us to our knees, and I think you will see a little bit of that in the RAND scenario that is coming up. So we need to be able to deal with coordinated attacks. We always look for weak links, and we try to build systems that have no weak links. No matter how hard we try, there are always weak links. There may be multiple events that trigger the weak links, but in the ARPANET case, for example, back in 1980, it was not a single event that caused the massive outage. It was a combination of circumstances, each one of which by itself would not have done the job; but it just happened, due to Murphy's law or whatever you want to call it, that this combination of circumstances led to the total collapse of the network.

I would like to make a few comments on cryptography, having just spent a year and a half with our National Research Council study group—and I hope you will look at that report (if you have not already) in considerable detail.

Cryptography is an absolutely essential ingredient for confidentiality, for authentication, for user authentication and system authentication, and for information integrity. At the moment, we do not have a lot of guarantees that any of the information that we are getting out on the World Wide Web and the Internet is in fact valid or that it has not been tampered with. So there is an integrity problem.

There is clearly an authentication problem.

Senator NUNN. There so far is no "truth key" on the computer, is there?

Mr. NEUMANN. That is certainly true. We also do not have any idea of who is doing what to whom, and in your questioning of Director Deutch, the answer that needed to be made is that we really have to ratchet up the concepts of authentication, and the only way to do that is to use good cryptography.

Now, the past situation has been that the U.S. Government policy has been to limit the use of good cryptography rather than to encourage it. One of the problems with, say, the U.S. export controls has been that it is very hard for system developers to put adequate encryption into their systems to do authentication if that authentication encryption could also be used for confidentiality. That has been a tremendous stumbling block. On the other hand, authentication is absolutely essential for the sanity of our electronic world. If we have no idea who is doing what, digital commerce will fall on its face.

So the confidentiality problem is of course important and has always been the one that is elevated in terms of national security considerations, but the authentication problem and the integrity problem are equally important.

So I think U.S. cryptographic policy must reflect national needs in a broader sense. The law enforcement issues are very important; the intelligence issues are very important. But the survivability of the Nation as a whole is exceedingly important, and one of the fundamental conclusions of our National Research Council crypto study was that those considerations may in fact be more important. That is a very, very critical argument to make, and we have made it in considerable detail.

I will make a couple of concluding remarks. I would suggest, in anticipating some of the questions that you may ask—and this will be useful in later discussion—that there are fundamentally three gaps that need to be closed, and I would like to address them very briefly.

The first one is the gap between the actual behavior that the computer system produces and what it was supposed to produce. In other words, we have all this wonderful new software, Net Browsers and things of that nature, but they are full of holes; there are serious security problems. The intent was that those things should be secure, but they are not, so we have this gap between what should happen and what actually happens.

Then we have the gap between the social policy, the expectations of what should happen, and what the computer systems are expected to enforce. And third, we have the gap between actual human behavior and the expected social policies.

Now, I claim that there are fundamental gaps in all three of those areas, and one of the fundamental questions that we have got to deal with is how do we close those gaps. One might say that it would be great to have laws that made computer misuse illegal. It is very hard to define things like that. It is very hard to say, looking at the Computer Decency Act, for example, what is indecent. It is very hard to define things like that if the computer systems cannot even support the policies that have been established by the laws.

So the laws have a role to play, but in order to make those laws meaningful, we must solve some of the technological problems. We must have meaningful authentication because if you do not know who an attacker is and where he is coming from, the laws are meaningless. If somebody is coming from Bulgaria, for example, and there is no way to track that particular person, U.S. laws do not make much of a difference because we are now dealing with an international problem.

So we have to look not for technological solutions to social problems, but for better technological solutions to technological problems. I claim that a lot of the so-called technological solutions that exist today are not adequate. So we must ratchet up the infrastructure substantially in terms of its reliability, its security, its survivability under crisis—and it may not even be a crisis. It may be just a sequence of unanticipated events that result in that system becoming useless.

Then, we have to substantially alter our view of the importance of all of these issues. I am a technologist. I also spend a lot of time on policy issues. I do not believe that the technological solutions by themselves are adequate, but I do believe that in the absence of the technological solutions, the legal solutions may be meaningless. So I think it is very important that we strengthen the infrastructure, that we take a proactive view toward a lot of the problems that we have seen.

If you look through my handout, you will see that I have attached a list of many, many cases at the back of my written testimony. Now, I am not going to go through any of those today, but I would urge you to look through the diversity that is represented by all of these problems. There are many problems that we must deal with, and we really have to take a broad, system perspective on the whole thing rather than looking for little palliative solutions. I have lots more comments, but let me stop there and just remark that there are no easy answers. It is a very difficult course that we must take. And any efforts that you can make to help will be appreciated.

Senator NUNN. Thank you very much, Dr. Neumann. We appreciate your testimony, and I look forward to reading with great care all of the examples you have talked about; I have not read them yet, but I look forward to doing that.

Senator NUNN. Dr. Anderson.

TESTIMONY OF ROBERT ANDERSON,¹ RAND CORPORATION, SANTA MONICA, CALIFORNIA

Mr. ANDERSON. Thank you. I will not go through my resume because you read it to me at the beginning of the hearing. My statement today is based on work I have primarily performed with my colleague, Richard O. Hundley, over the past 5 years, with support from the Defense Advanced Research Projects Agency, the Information and Warfare Office of the Assistant Secretary of Defense for C3I, the U.S. Air Force, and portions of the U.S. intelligence community. This statement, however, is my own and does not reflect the policies of RAND or its research sponsors.

In our investigations, Dr. Hundley and I have talked with computer security researchers, computer emergency response teams, law enforcement professionals, legal professionals, the national security and intelligence communities and providers and users of information systems. Our discussions have ranged across many countries in Europe, Australia and Asia.

I have provided the members of the Subcommittee a recent article by Dr. Hundley and myself on cyberspace security and safety published in the winter 1995/1996 issue of the IEEE Technology and Society Magazine, containing a more thorough discussion of our perceptions and findings on this topic than can be presented in this forum.

The risks to the U.S. infrastructure from actions or events related to cyberspace is a confusing topic. By "cyberspace," I refer to the global collection of internetted computers and communication systems. The term originated, I believe, in the novel "Neuromancer" by William Gibson in 1984. The public telephone network and the Internet provide the main backbone for cyberspace, but cyberspace also includes the computers that run many of the other control, communication and information systems.

The key word in the definition is "internetted," just in the same way that Dr. Neumann referred to the "internetting" of our computers as being the essential question in our society—the characteristic that makes it possible to access some systems from others perhaps half a world away.

I am familiar with the documents introduced the first two of these hearings, particularly the recent GAO report on information security and the staff statement presented on June 5. I concur with the findings and recommendations in these reports. Given this background, I believe two additional points need emphasis and attention regarding challenges in providing security in cyberspace.

¹The prepared statement of Mr. Anderson appears on page 364.

The first point is that the U.S. cannot just solve today's cyberspace security problems. As the information revolution continues, we need structures and forums within which new problems can be addressed as they arrive.

As the chart shown there indicates, during the last 15 years, we have experienced at least three major information revolutions, each introducing unique security problems, with additional revolutions expected in the indefinite future.

The personal computer revolution in the lower left corner there, starting around 1980–81, began viruses passed by floppy disk or downloaded from bulletin boards.

The second revolution we have experienced even in the last 15 years—the explosive Internet growth brought greatly increased hacking and its related "packet sniffers" and "packet spoofers" that easily crossed international and organizational boundaries.

The third revolution indicated there is the explosion of the World Wide Web in the last 5 years, with its browsers and the "Java language" and "applets"—"applets" are small application programs that are downloaded into a personal computer for local execution there.

The promotion of all this allows downloadable executable code from strangers while bypassing normal firewall protections, a combination that is ripe for exploitation by malefactors.

By their nature, the progress of future revolutions could not be predicted. However, a good candidate for the next revolution shown there is widespread electronic commerce. It is quite possible that billions of dollars a year of commerce will be conducted by citizens and corporations online within the coming decade, including millions of micro payments of pennies or hundredths of a cent for various forms of information access.

The opportunities for abuse within such a system are manifold, and many are very likely unforeseen today.

A later or possibly coincident revolution might involve widespread dependence on electronic monitoring and control systems, indicated as "widespread sensing and control" in the right lower corner there.

U.S. residents' automobiles will soon be in automatic communication with toll booths, smart roads and even gas stations. Meters within their houses will increasingly be read remotely and automatically, and smart houses, with many more control and feedback systems, are in our future.

The market for goods and services is driving these revolutions, and for years now, the market has emphasized increased functionality, not security. If this trend continues, new vulnerabilities will arise that are unexpected and unaddressed.

My second point, therefore, is this. Since there will not be a plateau with information system developments during which the existing security problems can be solved, I believe the only viable solution is the development of a framework for a continuing partnership between government and industry within which new vulnerabilities and risks can be addressed as they are encountered. The government cannot ignore market forces, and it cannot ignore the private sector. There are, however, examples in which government and industry have worked and are now working together effectively, such as in improving the safety of automobiles and the commercial airline industry. Such continuing cooperation, focused on safety and security, is needed today across all aspects of our national information infrastructure, including energy distribution, transportation control systems, financial networks, the traditional telecommunications and inter-networking sectors, and any future infrastructures established, for example, to support electronic commerce.

In RAND's studies on these topics to date, three issues are repeatedly raised which should form a portion of the national dialogue on cyberspace security. These issues are good candidates for the continuing structured dialogue between government and industry that I recommended earlier.

First, there has been considerable discussion of the advisability and feasibility of creating a minimal essential information infrastructure, or MEII. If all of our systems cannot be adequately protected to enable deployment of military forces or to protect key transportation links to operate, or to allow other key societal activities to continue, is there some fallback level of system that will allow essential services to continue with temporary graceful degradation of other services? If there is, a number of questions to which the United States does not yet have answers must be addressed. These include: What are the essential services, and what are the minimum levels of these services that our society requires? What types of communication and computation systems are required to support those essential services? How would an MEII be formed from the existing infrastructure—by hardening certain parts of it? By creating sufficient redundancy and resilience that a minimum portion of it would always survive? What would the costs of an MEII be, and how do these compare with the expected benefits?

Second, we should consider simple ways to increase the robustness of the U.S. infrastructure systems. For example, it may be possible through incentives or regulations to increase the "biodiversity" of the software and hardware of our systems, especially the public telephone switch system. Today, those systems are too dependent on a few suppliers; a flaw or bug once uncovered could be exploited literally within thousands of switches, much in the same way that Dr. Neumann talked about one flaw being perpetrated in the Internet and in the public-switched long-distance telephone system.

Mr. NEUMANN. Perpetuated.

Mr. ANDERSON. Yes. Third, I reiterate a point introduced in earlier hearings because of its importance. Roles and missions among organizations having necessary roles to play need clarification. Although responsibility must be distributed within the United States, someone must coordinate the activities of the national security and domestic agencies of government, the U.S. public and private sectors, and the national and international communities.

To me, this would imply explicit coordination at the highest levels of the executive branch, within the executive office of the President.

Let me closing by saying that your hardest task will be putting the insecurity of our infrastructure into perspective. Is it more dangerous to our society than the threat of biological or chemical weapons or nuclear proliferation? I do not believe anyone has a clear answer to this question yet. At present, I do not believe that a standalone information warfare attack upon the U.S. civil sector would produce significant and enduring consequences. However, in time of war or troop deployments, a coordinated cyberspace attack could have adverse military consequences, and it could be used by foreign elements to affect U.S. public opinion regarding an intervention or an operation.

Of course, there are positive forces at work, too. In particular, online commerce may create a market for better online security to everyone's benefit. In general, our country's infrastructure is very resilient, as various natural disasters and various incidents to date have shown.

There is much more to be said on these topics, and I trust further detail on many of these issues will be forthcoming in future hearings of this Subcommittee.

Thank you for your attention.

Senator NUNN. Thank you, Dr. Anderson.

Dr. Molander.

Mr. MOLANDER. We would now like to introduce you to the possibility of a crisis occurring at some point in the future and to elicit your perspectives on what kind of reaction might take place in such a situation.

For this purpose, let us say we would like you to envision that you will be dealing with a setting in the year 2000, which will be explained in some detail. Imagine that you have been invited to a classic kind of crisis meeting, like the excom meetings that accompanied the Cuban missile crisis, with attendees such as Cabinet members and other advisers. Basically envision a situation where you are at a meeting that is in advance of a decisionmaking meeting with the President of the United States where some tough decisions are going to be made about an escalating crisis.

I would now like to introduce Andy Riddile, who is currently at National Security Research, Inc., but was at RAND when this work was done, Andy, along with Peter Wilson and Bob Anderson and Dick Hundley and myself, were members of the design team that produced this exercise.

We are asking you to think about being in a situation set in the future, and to think about what kinds of issues should go to the President, what perspectives should be brought to the table, and as you can well imagine, what kind of political perspective should be brought in a situation that would undoubtedly be challenging to the President.

With no further ado, Andy Riddile.

Mr. RIDDILE. Good evening. It has been a long day, and we have a lot to brief, so let us get started. This briefing will review the current situation in the Gulf, the objectives of this meeting and the draft memorandum to the President.¹

To help you think through the long-term aspects of this crisis, let me remind you of where we are in the information revolution. Today, one-third of all U.S. business transactions occur electroni-

¹Slides presented by Mr. Riddile appear on pages 369-379 in the Appendix.

cally; 25 percent of American, European and Japanese adults now carry a cellphone. The national information infrastructure and the global information infrastructure are heavily used by activist groups linked in networks focused on a broad range of environmental, human rights, and other global issues.

Most U.S. defense communications now pass over the commercial public-switched network. There continues some anxiety about the safety and security of this practice.

To remind you, the new U.S. contingency plan for the Persian Gulf region, code-named Green Hornet, includes annexes with both offensive and defensive IW options.

Finally, continued public concern in the United States about acute domestic problems weighs heavily against seeking military solutions to various international problems.

In this challenging political context, the now well-known Consortium for Planetary Peace, or CPP, is an important new grassroots political force with broad support from the left and the right.

These next four maps give information relating to the current crisis. Let us look at the first map. I will briefly review some major IW events that we know have occurred over the past few years. Tension in Saudi Arabia between Islamic fundamentalists and nationalists is growing. Much of the dissident movement has coalesced around the goals of the CIRD, the Campaign for Islamic Renewal and Democracy, an increasingly powerful Islamic nongovernmental coalition working for social and political change throughout the Islamic world.

In 1998, the Bank of Saudi Arabia was looted of nearly \$1.2 billion by a sophisticated electronic attack with strong evidence of both Iranian and Syrian involvement. In 1999, French intelligence services discovered an attempt to place a lethal computer virus in the airbus industry's AB330 flight control software, apparently by Algerian agents acting under the direction of Iran.

In the summer of 1999, Israel experienced a series of electronic attacks on its military command and control system by an array of "sniffers" and "logic bombs" of uncertain origin. Also in 199, three Indian nationals, including an acknowledged world class software writer, were arrested by the Indian authorities after penetrating supposedly highly secure Indian defense networks. In the course of plea-bargaining, the Indians confessed to selling Iran a variety of 21st Century information warfare tools. The events depicted here in blue occurred during the last few

The events depicted here in blue occurred during the last few weeks. Those depicted in red occurred during the last several days. Recall that 14 days ago, Iran proposed (1) that the oil-producing countries of the Persian Gulf declare a major reduction in oil production to raise prices and (2) that the GCC and other Gulf States gather under a newly-declared security umbrella with hints of an imminent nuclear weapons capability as an Iranian security element. In response, Saudi Arabia and Kuwait each mobilized military forces.

Thirteen days ago, 90 percent of the power in Cairo went out for several hours; the cause is still unknown. Twelve days ago in the Gulf, a sea-air battle resulted in the loss of several Saudi and Iranian warships and aircraft. Some time later, an S3B Viking off the Ronald Reagan was fired upon by an Iranian missile frigate. Thirty minutes later, U.S. aircraft from the Reagan shot down three MIGs and sunk the Iranian frigate.

Eleven days ago, the largest ARAMCO refinery near Dhahran experienced a catastrophic flow control malfunction that led to a large explosion. A radical Islamic group linked to Iran released a war communique which threatened that the Saudi economy could be brought to its knees with the touch of a button.

Eight days ago, Scotland Yard detected three different "sniffer" devices in the main fund's transfer system of the Bank of England. Following this, in a CNN special report on the cyberspace threat to the economic fabric of the United States and Western Europe, the London Stock Exchange Index fell 10 percent.

In our hemisphere, 13 days ago, the public switch network for Northern California and Oregon suffered a series of massive failures. Nearly simultaneously, the base phone system at Fort Lewis, Washington was subject to a mass dialing attack by personal computers orchestrated via the Internet. This paralyzed phone service to the base for several hours.

It has been 10 days since the Metro Superliner slammed into an apparently misrouted freight train near Laurel, Maryland, killing over 60 passengers and crew. U.S. agencies agree that this disaster was the result of electronic intrusion into the rail control system, but debate over its origin continues.

A week ago, the New York Stock Exchange fell nearly 200 points; spot oil prices increased to \$75 a barrel, and the price of gold rose 10 percent.

Six days ago, the U.S. Commander-in-Chief Central Command requested authorization for the imminent execution of phases 1 and 2 of the Green Hornet deployment plan. At an emergency NSC meeting, there was a lengthy debate about our ability to attribute recent IW events to Iran versus domestic political forces opposed to intervention in the Gulf. The President announced execution of Green Hornet, the immediate convening of the NATO North Atlantic Council, his decision not to pursue diplomatic initiatives with either Iran or the CIRD, and his intent to pursue congressional approval of his actions.

The British Prime Minister and the President of France agreed that the UK and France would join in the U.S. military deployment.

This last map summarizes events around the world during the last 6 days. In the Persian Gulf, you will recall that 4 days ago, Iran began massing special forces north of Bandar Abbas. These units can rapidly cross the Persian Gulf. Simultaneously, armored and mechanized divisions have fully mobilized south of Des Fool and may soon cross the newly-built bridge south of Basra to menace Kuwait and northeastern Saudi Arabia. In response to these moves, the Saudi Government mobilized additional military forces.

Yesterday, our fears of a possible coup against the Saudi monarchy were realized with a well-coordinated attempt by the CIRD to overthrow the government. Large-scale demonstrations have occurred in all major Saudi cities. Also, the Saudi public switch system partially failed, and the CIRD seized control of both national television networks. Several hours later, U.S. Commander-in-Chief Central command reported that several of our JSTARS radar surveillance aircraft were disabled by a computer worm triggered by some external source.

In the United States, the ATMs of two of the largest bank chains in Georgia suffered major malfunctions which led to a local run on the Georgia banks. Adding to public anxiety has been speculation by the television media that the United States is under strategic IW attack.

Three days ago, the Committee for Planetary Peace, or CPP, successfully organized a major demonstration on the Mall of over 400,000 people against our policy to shore up the Saudi monarchy.

As you know, 2 days ago, Continental Airlines AB340 crashed near O'Hare International with no survivors and more than 30 people killed on the ground. Preliminary reports from British, French and FBI sources indicate that the aircraft's flight control software was infected by a sophisticated logic bomb. Further, the FBI has two suspects sympathetic to the CIRD and CPP who worked for a Texas software firm which made modifications to that aircraft software.

Today the Chairman of the Joint Chiefs of Staff indicated that our deployment plan, Operation Green Hornet, has been delayed by a full-scale information warfare attack.

The Chicago Commodity Exchange has experienced some of its wildest fluctuations in history, with evidence of electronic manipulation. The value of the dollar has fallen by 5 percent against major currencies. Spot oil prices remain above \$100 per barrel.

The President has asked for another meeting of the NSC 2 hours from now to make a set of IW decision consistent with going forward with a military deployment to the Persian Gulf region, including dealing with a deteriorating IW security situation here at home. The purpose of this meeting is to complete an issues and options paper for the President for the NSC meeting in a couple of hours. These are our objectives.

You each have a copy of the draft memo to the President. Its organization looks something like this. In preparation for the NSC meeting, you now have an opportunity to review and comment on the situation and the issues in the memo.

This concludes my briefing.

Mr. MOLANDER. If we were in such a meeting in the Cabinet Room of the White House, Senator Nunn, you would have an opportunity to engage a group of experts like some of us here at the table and colleagues from the administration about what to do in a situation of this character.

We invite you at this time to raise questions about the situation, the cyberspace aspects of it, about the political situation that would exist in this country if we were suffering under such an IW attack, and the media was championing what was happening in the sense of serious crisis.

What should we do in this situation?

Senator NUNN. The first question I would have is what has happened to CNN. [Laughter.]

Have information flows been disrupted in terms of reporting from the region?

Mr. MOLANDER. I think in the situation that we are looking at right now, CNN is on the air and operating. I think one could anticipate there could be problems with such networks and the possibility of intrusion of the kind that Peter described earlier.

I would invite my colleagues to comment on these prospects.

Mr. ANDERSON. In some of the versions of the exercise we conducted, we did have CNN taken off the air for a couple of hours, which then heightened awareness when they came back on the air, and they created a set of special programs highlighting the cyberspace security incidents that were happening and the information warfare attacks we may be under.

So taking them down or leaving them on, either way, they become a potent force for public opinion.

Senator NUNN. So the public in this country is aware of everything, basically, that you demonstrated up there.

Mr. ANDERSON. Correct.

Senator NUNN. In your war games, do your participants believe that we have enough intelligence to have a fix on where the attacks are coming from?

Mr. MOLANDER. Quite the contrary. In the exercises that we do, we tend to emphasize the extreme difficulty of identifying the sources of the attack in contrast to classic strategic crises that we envisioned possibly taking place during the Cold War, where we would have the detection systems for missile launches and the like that would identify whether an attack is taking place and the source of the attack.

There could be substantial ambiguity in such attacks in terms of the source. As was mentioned, there is the possibility that the attacks might be coming from domestic sources, opposed to intervention. What we might see is a turn of the century version of the anti-Vietnam War effort—but here armed with cyberspace techniques that might be far more effective than some of the techniques one saw in the sixties and seventies of trying to stop troop trains and material going to Vietnam.

Senator NUNN. Are the Saudis publicly asking for our support? Mr. MOLANDER. The Saudis in this situation, I believe in the details of the scenario, would be asking for our support, and in particular, asking whether we would be able to make available to them defensive techniques. Here, we would face a very serious question as to whether we would provide them, either in the escalating period of the crisis or in the heat of the crisis, with the best that we have, or whether we would provide those, for example, to the Egyptians, who are also in this scenario suffering from attack on their electric power grid. I think that that would be one of the most difficult questions that would be addressed by the country in such a situation.

Senator NUNN. Do you have a representative from the Federal Reserve system in the situation room who could tell us about the risks to the financial structure and the psychology of the bank runs?

Mr. MOLANDER. Well, presumably, the Secretary of the Treasury would be there and possibly a representative from the Federal Reserve. I think one of the things that we all realize is that—just like Willie Sutton said when asked, "Why do you attack banks?", answered "Because that is where the money is"—the banking system is probably the most important front, so to speak, in which action is taking place. Because that is where the money is, it is the place where the testing of offensive and defensive techniques is likely to be most highly developed.

Senator NUNN. Given the scenario that you have outlined, it appears that certainly one question which would come up is whether we believe that a foreign country is behind this, and with the attacks internally on Saudi Arabia, do we believe that the radical fundamental groups are behind it? Do we believe that that is being directed by a country like Iran? Mr. MOLANDER. I think that would be very much the kind of

Mr. MOLANDER. I think that would be very much the kind of question that would be brought to the fore in such a situation. Certainly, it would be what the President would want to know: Who is behind these attacks?

I think it is very hard to be optimistic at this stage that we'd know the answer. Barring some very aggressive action in programs of the kind that people have been talking about launching, but yet are not yet in place, in this period of time we would have extreme difficulty in being able to provide the identification of the attacker that would be so critical in the President and his advisers and congressional advisers deciding just what kind of action to take. We just cannot count on that.

Senator NUNN. Do we have our offensive people in the room who can tell us what our options are in the event we conclude that these attacks are coming from a sovereign country?

Mr. MOLANDER. As sure as Director Deutch this morning turned down the opportunity to speak in open testimony about offensive capability, I think one could be assured that that question would be at the table. But as depicted in the schematic where I talked about strategic information warfare, entering a crowded strategic field, there is also the possibility that one would be talking about not responding in kind, but possibly by escalating with more conventional military capability.

I think one of the real questions when one talks about offensive capability, of course, is what is the total impact of using such techniques, which is another part of the assessment that would accompany any such consideration.

Senator NUNN. In your scenario, different aspects of our infrastructure are being attacked in the year 2000. To what extent do you believe this scenario would apply today, in 1996?

Mr. MOLANDER. Some of the things that are included in the scenario are speculation on our part about current trends, plus anticipating that we would have taken a lot of action in the interim. It is very hard to speculate about the future course of the information revolution or just what kinds of capabilities might be undertaken and developed by foreign nations. But certainly today, I think people are more or less confident that, while episodic attacks of one kind or another might take place, that the kind of systematic and structured, well-coordinated attack that had a lot of planning in advance by another nation, even a Nation like Iran or China or Russia, is something that is more down the road—but I would invite others to comment.

Mr. NEUMANN. I would add that historically, the technology has been advancing exponentially in terms of the power of the computing. We are about to see a tera-bit computer that is vastly more powerful than anything we have ever seen before, and certainly memory sizes are getting enormous. But the security and reliability issues have never grown commensurate with the growth in the technological capability, the power of the computer. I would suspect that by the year 2000, assuming we have over-

I would suspect that by the year 2000, assuming we have overcome the calendar problem of a lot of our computers collapsing on January 1 of the year 2000, that the situation will not be substantially better than it is today proportional to or relative to the rest of the situation. As I mentioned earlier, every time you produce new systems, you produce new vulnerabilities, and new threats keep arising continually. It is a continuing spiral. The attackers are getting more sophisticated, and the risks are getting much greater when we talk about putting massive amounts of financial property on the infrastructure. Suddenly, the risks become quite enormous for organized crime or other concerted attacks. It is a very lucrative source of revenue.

So I think my answer would be that in 2000 or 2004, we are not going to be well-off enough unless we take very strong actions now, and I think the important message that we are getting out of this particular scenario is that we must take very significant steps now to improve the infrastructure.

Senator NUNN. What would be the vulnerabilities that the collective intelligence and law enforcement officials would basically list for the President in terms of other parts of our infrastructure that could be taken down now—in other words, what would be the scenario that they would be unfolding to the President about what is likely to happen next?

Mr. ANDERSON. Clearly, I think one of the underpinnings of our entire national infrastructure is the public switch telephone system. Hackers and phone freaks routinely get into the switches of that system. They system, unlike in the old days, when you could go to AT&T and say "Help," is now provided by about 1,500 different providers with shared trust among their systems. There is no one place to go to get the telephone system fixed quickly, and I think the heavy dependence of our DOD on a public switch telephone system and of the Internet itself on leased lines through those switches creates the most fundamental infrastructure problem that needs to be addressed.

Mr. NEUMANN. Let me make a comment on that. The telephone providers have in fact in the last 3 or 4 years done a considerable job in lessening their vulnerabilities. I did a study 4 or 5 years ago for the office of the manager of the National Communications Service and pointed out a large number of vulnerabilities. At that time, it was possible basically to break into the maintenance port of the telephone switches, all of which had the same password, with relative ease. If you had ever worked for the telephone company, you knew that password, which had not changed in a long time, and things were exceedingly vulnerable.

Things have improved, but there are other vulnerabilities that need to be addressed as well. So I think the comment that the PSN is in fact a very serious source of vulnerability is exactly right-on.

Senator NUNN. Do we have options for the President to choose from in this scenario where we would be able to send certain strong messages to potential adversaries that we are capable of taking strong retaliatory action with information warfare ourselves, so that they get a warning without basically raising it or escalating it to the point where it would be a crippling attack?

Mr. NEUMANN. If you knew who they were. If you do not know who they are, it is hard to retaliate.

Senator NUNN. But in this situation where the regional developments are taking place, you could surmise that it might be coming from the same sources.

Mr. NEUMANN. Yes, but the domestic things in this scenario, you are not at all clear at this point who has done what to whom.

Senator NUNN. The domestic side of it would be the most difficult.

Mr. ANDERSON. Or the domestic CPP advocates could be conducting their own attacks overseas. You really do not know where it is coming from, and one of the key problems is that you do not know until far down the pike where the attacks are coming from, so you do not know quite whom to hit.

Senator NUNN. Have we got a problem at this stage—a jurisdictional problem—between intelligence and law enforcement as to how much of our intelligence resources we can bring to bear, since we do not know whether the source of the attack may be domestic?

Mr. MOLANDER. You have certainly identified one of the most challenging issues that I think the country faces as we engage on this problem. You are well familiar with the traditional separation between those two communities. But just as is the case with the terrorism threat, I think it is increasingly clear that some greater cooperation and communication overlap in the activities of those two communities is necessary. How to effect that, whether additional legislation is necessary in order to have the kind of debate that will probably need to take place to have people comfortable with that greater overlap and exchange of information is part, I think, of the challenge that we face. But certainly in a crisis situation, one would anticipate that there would be a demand that there be greater cooperation almost independent of what the law at the time says. You can certainly imagine that the President would be making these kinds of demands.

Senator NUNN. What about the private sector that is under attack—the banking system, the railroads and so forth—what are the demands from them in this scenario? Are they in touch with the administration? Are they going public with their concerns, saying the government "must do something"? What is the role of the private sector here?

Mr. ANDERSON. There is no current forum in which the private sector can bring its needs and wishes and demands to government. Since they do not know whether the incidents are coming from overseas or domestically, they do not know whether to go to the FBI or the CIA or NSA or whomever.

I commend the staff report that was introduced at an earlier hearing of this Committee in suggesting a national threat center for the NII as possibly being a place to which industry could come and make requests and make their incidents known. But one thing that ought to be considered in that policy is the need for security and privacy of that information so that perhaps industry would be more willing to be fully open about what is happening within pri-

vate industry if they were assured that their information would not be able to be used by competitors against them and become publicly known on the front page of the newspaper, for example.

Mr. MOLANDER. This is certainly a big issue when it comes to producing an action plan, which is how to effect much grater information exchange, not only within the government, between the likes of the law enforcement and the intelligence communities, but also between industry and government. As we have looked at places where necessary but not necessarily sufficient action needs to take place, some means needs to be found whereby the private sector, which is probably going to be the place where the hits, the attacks, are taking place, can engage in a systematic exchange of information between the government. As Director Deutch said, the government might know something about what nation states might be preparing these kinds of capabilities, but the private sector will likely be the first to feel the hit. As Bob mentioned, this is the sort of problem where information exchange forums do not exist today. save possibly in the telecommunications sector where, through the efforts of the National Communications System and the President's National Security Telecommunications Advisory Committee, the NSTAC, there have been some exchanges in what is known as the national security information exchange process.

We think that the latter telecommunications sector process which, incidentally, is not only concerned about cyberspace attacks. but possible conventional HE attacks-high-explosive attacks-on key nodes, might provide a template and approach that is applicable to other key information sectors, like the electric power grid in the banking community. However, exercise participants from these other sectors tell us that this is going to be a long process to effect this kind of cooperation in their communities. There is not a trust relationship in existence today that would facilitate that.

Senator NUNN. If we decide to have some kind of demonstration of our own information warfare capability just in case a certain country were the perpetrator, and we just decided to do that, do we have the ability to know what kind of damage we are going to cause? Are there certain things that are taboo that we would not use, and are there certain things that would be used in this sort of situation? Have we developed to that scale by the year 2000?

Mr. MOLANDER. I would be engaging in speculation about that because I am not directly involved in that business. I do not know whether any of my colleagues would care to comment. Senator NUNN. We would certainly want to have some dem-

onstration capability, wouldn't we?

Mr. MOLANDER. Certainly. One of the things that we have seen in the exercises is a real frustration in dealing with an inability to say, 100 percent, yes, this is Iran, or yes, this is some other per-petrator. This raised the possibility of someone saying, "Well, it is probably them, so let's just fire one across their bow and see if they change their behavior. This is the kind of possibility that would come up in the kinds of meetings we are portraying. Hopefully, at that point in time, one would have some ability-just like with dial-a-yield nuclear weapons-to vary the intensity of the cyberspace attack one might make against any developed infrastructures in the other country.

Senator NUNN. Do you run into a Third World problem, where they have developed offensive capability, but they are so far behind with infrastructure, they do not have the same kind of vulnerability that we do?

Mr. MOLANDER. Well, this is kind of the situation today, but it is changing in the sense that a lot of these countries that are sometimes characterized as being in the Third World are very rapidly adapting some of the systems of the information revolution.

My colleagues would know more about this.

Senator NUNN. Our testimony was that our air control system was not as vulnerable as many of our other systems because they are so far behind in being able to update their computer capability that they have had to maintain the ability to go hands-on. [Laughter.]

Mr. MOLANDER. That is going to change if the efforts underway which have been underway for a while—are successful. The kind of invulnerability that came from this cobbled together air traffic control system is going to go away, not only when the changes are put into effect, but in the transition period. When one goes from the current system, disparate sort of construction as it was, to an open architecture system or common architecture, you are going to have real start-up problems, and during this transition period people will be able to learn a lot about the new system.

Mr. ANDERSON. I should also point out that one should also look beyond any particular system. Even though we have tube computers running some of the FAA systems, they use leased telephone lines to communicate among FAA centers, and they are dependent to some extent on local power systems—they have temporary power, but over the long run, they are depending on power—and therefore, there are other portions of the infrastructure on which other portions depend, and one can get at them through a variety of techniques.

Mr. NEUMANN. In my list, you will find a whole bunch of cases where the power outage caused—and you may have been flying on those days—entire airport complexes, for example, New York, to be down for hours because of the cutting of a single cable accidentally, for example. There are a lot of cases where in fact the air traffic situation is fundamentally dependent on power. It was the New York case where they had standby power, but they did not realize they were running off the standby power in the power failure, and they ran out of standby power without realizing they had been using it, and then they were really out of business.

So there are a lot of risks there.

Senator NUNN. What about the added cost? You talked about certain things that need to be built into the infrastructure now relating to security, safety, reliability and so forth. Are you talking about huge jumps in cost in order to build these into the system?

Mr. NEUMANN. Well, here, the attitude is that if you try to retrofit something to a system that was not designed to be secure or reliable in the first place, it does potentially add significantly to the cost—to the operational cost as well as the development cost.

The key here is that we have to plan in advance for emergencies. We have to anticipate some of these problems. We should not be building systems where a single cable cut can bring down an entire infrastructure. We should not be building systems with horrendous weak links.

Senator NUNN. We ought to have redundancy built in.

Mr. NEUMANN. We should have redundancy built in.

Senator NUNN. Who pays for that? Do the market forces take care of that, or is this going to have to be a government expense Is the market going to drive people toward more security, or is the market more likely to penalize those who go for more security because their cost of equipment is——

Mr. NEUMANN. It is an interesting question. In the past, the users have not been organized enough, they have not recognized the security problems, and they do not worry about the reliability problem until they are off-the-air. At that point, they all start screaming, "What can we do?"

Now, in answer to the reliability question, there are many systems in which over half of the software is devoted to the maintenance of the reliability and the fault tolerance and the recovery and the backup and all of these things. This introduces new com plexities. As soon as you have a system with 100 percent more software than you thought you needed to do the job in the first place, you dramatically increase the number of bugs and flaws and operational problems.

So the answer to who pays is that we have to do this very carefully. If we design systems ahead of time, understanding the requirements—and I go into this in my written statement in some detail—if we understand the requirements for security, reliability, safety, availability and whatever else, and we make those an explicit part of the system development—

Senator NUNN. Is that happening out there now? Is the marketplace beginning to move in that direction?

Mr. NEUMANN. Not really. The government has to move more in that, and in many of the government procurements, the requirements are not stated adequately. Let me give you an example.

In the Vincennes Aegis shootdown of the Iranian airbus, the system design was archaic. It was very difficult if not impossible for the operator of that system to know what was really going on.

I gave a talk at Carnegie Mellon University some years ago, and I talked about how the Aegis system was a terrible example of a user interface. Somebody in the back of the room raised his hand and said—this was somebody I knew because he was a graduate student of a close colleague of mine—he said, "Peter, you have to know that I am the guy who wrote that code, and I have to explain what happened. The government did not require the information that was necessary for the operator to know what was going on to be on the screen. My boss, when I pointed out the problem to him. said, 'You cannot put it on the screen because the government did not ask for it, and secondly, there is no room on the screen to put that information; we would have to take something off," because the system was so archaic.

So we are dealing with a very wide range of problems, and one of the problems is that the requirements are not well-stated. Another problem is that the system development process is not wellestablished, despite the fact that we have been doing it for many years—I have been involved in writing code for 43 years. The problems are immense, especially in crticial systems.

Senator NUNN. What about on the private sector again—are private sector companies, banks, utilities, power companies and so forth, insuring with their insurance policies against this kind of serious loss? Are insurance companies writing policies for power companies or to utilities?

Mr. NEUMANN. There are beginning to be some inroads where an insurance company will look at whether you have used best practices or not.

Senator NUNN. I was going to say that if they are insuring, their insurance companies are very exposed, aren't they? Is this an insurable risk—I guess that is my question. Is the taking down of a power system by a computer hacker a risk that the power company absorbs itself; is it self-insurance—the same thing with telephone companies—or are the insurance companies in play here? Do we know?

Mr. ANDERSON. I do not know the answer, but it is an important question, and in other things we have written, we emphasize the possible role of the insurance industry in creating codes of best practices.

Senator NUNN. Because if the insurance companies are exposed, we could have the possibility of catastrophic losses here, and if that is the case, you would think they would be requiring some best practices and that that would drive the market in the right direction without the government necessarily—

Mr. NEUMANN. I think the answer is basically no; the insurance rates on something like that would be high, and the companies are self-insuring.

Senator NUNN. So you do not think it is insured; you think the companies are self-insuring.

Mr. NEUMANN. I doubt it very much. On the AT&T collapse of 11 hours of long-distance, they just absorbed the lost revenues.

Senator NUNN. What about train wreck? Certainly, that is insured.

Mr. NEUMANN. Ah, now we get to the case of lawsuits resulting from damages. We have gotten to be a very litigious society. I think we will see some monster lawsuits against folks who have not designed systems well.

Mr. MOLANDER. I think one of the questions on this cost business is at what point the government might incur costs or should incur costs. In the participation from private industry in these exercises, there is a strong message that says, "Let us, let the market, do the best it can with some of these threats." But I think what we may see emerging is a situation where private industry says that it will take care of the hackers, the disgruntled insiders and maybe the storefront terrorists, but if it really turns into a Nation state threat of a sophisticated, coordinated attack, then it becomes the government's responsibility to put up the costs. I think this kind of division of responsibility is going to be one of the big issues that the country is going to have to deal with—can we let the market defend against the smaller threats while the government takes on some of the costs that may be required to deal with some of these larger threats. Mr. RIDDILE. Another comment on cost. We are talking about very serious national security problem, but it is a tractable one. I mean, this is America, we are Americans. Research, analysis, development of procedures, education and training, professionalism, development of policy—that stuff does not cost much, and it can get us a far way down the field in solving this problem.

Senator NUNN. Do we have to have some kind of electronic Pearl Harbor before we are sufficiently alert to get out in front of this scenario in the next 3 or 4 years so that it does not happen in the year 2000 or, if it does happen, we are better-equipped to deal with it than you now project?

Mr. NEUMANN. That may be up to the response that you get from the series of hearings that you are holding. If the vendors realize that there are serious problems that they have not been addressing-----

Senator NUNN. Define the term "vendors" in this context.

Mr. NEUMANN. Yes. If the government realizes that there are serious problems that they have not been addressing, and if the user community realizes that there are serious problems that they have not been addressing, there is a good chance that we could, as I say, ratchet up the infrastructure substantially. But again, historically, this has not been encouraging. Every time there has been a collapse like the two that I have mentioned or the "Internet worm" of 1988, palliative solutions have been taken, and people have said, "We fixed that, so it will never happen again." (But it does.)

In the case of the year 2000, there is a tremendous amount of money being expended in trying to anticipate what is going to happen. The result of that is, I think, useful. It may be costing the government a lot more than it needs to, but the reason for that is that people have been oblivious to the problem up until now. There have been numerous reports of calendar clock problems. There were massive banking systems that went down a few years ago; they started in New Zealand, an hour later in Australia, and then an hour later across the world. By the time they got to England, naturally, they had figured out what the problem was and were able to fix it.

But the year 2000 problem is much more endemic because it is very, very pervasive.

Mr. ANDERSON. Senator, regarding Pearl Harbor-type attacks, let me just mention that to some extent we can do it to ourselves in a positive way. The Defense Information Systems Agency has for a number of years now been conducting attacks on its own system—red team attacks—and those have been very successful in raising the awareness of commanders at bases who really could not care less until they were hit and suddenly realized that their computers went down.

Senator NUNN. Is anything comparable going on in the private sector that you are aware of?

Mr. ANDERSON. Not to my knowledge, but I would think that that would be a strong message that this hearing could send, that more of that kind of proactive probing of the system could be done. The dangers in the private sector, of course, are that if you take down a system accidentally, and someone gets hurt, they will sue, and on and on and on. So you would need perhaps some legislative action to protect people who are trying to protect our infrastructure so that certain tests of the infrastructure could be undertaken without massive liability. It might be one way to encourage that.

Senator NUNN. Dr. Anderson, in your statement, you recommend that we think about the feasibility of creating a minimum essential information infrastructure, and you show that up on the board, the various key pillars—I believe you have six of them up there. Could you tell us what, in your view, the minimum essential information infrastructure that we need to build maximum redundancy and survivability into—what would be those ingredients?

Mr. ANDERSON. It is a very tough question. I think research has to be done on answering the questions that I raise in my statement. We simply do not know what percentage of the telephone system, of the power system, of the financial system our society could survive on for a day, for a week, or whatever, and therefore we simply do not have answers to those questions other than to tell you that the public telephone system is critical, the energy system is critical, the financial system is critical, and there are other things like pipelines and refineries and things that are necessary. But major research should go on regarding what are the minimum levels that our society can withstand temporarily, and how should we ensure that those minimum levels are always available. I do not have an answer to that question yet.

Senator NUNN. Do any of you know whether we have any legal problem like antitrust laws that come into play if the utility industry or the telecommunications industry decided to get together and work collectively on protecting their infrastructure?

Mr. ANDERSON. I would think that the NSTAC, the National Security Telecommunications Advisory Committee, is an example of various competitors getting together under a government aegis and that that has worked successfully. Perhaps that model might be replicated in other industries.

Mr. NEUMANN. The NCS is another example of that, the National Communications System.

Mr. MOLANDER. That is the hope, that one can transcend or deal with the antitrust laws with what is at stake here. But as has been mentioned frequently, we are really at a very early stage in terms of both understanding the level of risk to the various infrastructures and in getting organized, both in industry and in the government, and between the two.

Senator NUNN. There have been discussions about forming a national information infrastructure center staffed by representatives from the Department of Defense, other government agencies and the private sector. The center would address problems encompassing the full breadth of critical infrastructures, develop infrastructure assurance policy and coordinate infrastructure assurance plans and programs. Do you have any comments on this concept and whether it should be a government agency sponsoring it, or the private sector, or some combination?

Mr. MOLANDER. This is one of the ways of getting going and certainly one that brings together in the same place many of the people with responsibilities attendant to this problem. We have speculated about such centers being set up in the exercises that we have done. In general we have gotten a positive reaction to the idea with some qualification in terms of how industry and government would work together.

One comment at a recent exercise by a member of industry was: "What you guys need to do is find some way of providing the information to us, and then we will respond, rather than us providing information to you and having it come back in some digested fashion." Some kind of two-way street needs to be established, and just based on long experience in this city and working with government, I do not see how that could be done without establishing some single focal point in some institution which is probably associated very closely with the Executive Branch, at least initially.

Senator NUNN. Do you think there is an awareness in the private sector about the vulnerability, generally speaking? That is a very broad question, but are there parts of the private sector that would be more aware than others? Are there particular examples of private concerns having been expressed?

Mr. ANDERSON. Certainly the banking industry and the financial industry in general I think were illuminated by the Citibank case, and in general our financial systems are quite secure and quite well-protected, and I think they have sort of pioneered being as secure as current technology allows. I believe other sectors are much less aware.

Mr. NEUMANN. The banking industry is now desperately trying to get on the Internet, which will greatly increase their risks. There are some serious security flaws there that need to be addressed.

Senator NUNN. If you were out there in the private sector, and you were becoming more aware of this, is there anybody in the government on whom you can call for help?

Mr. NEUMANN. Well, that has been one of the key problems, that there is no organization that really represents the private interests. But there are certainly a lot of government agencies that one should go to and jawbone them and tell them that something needs to be done, and the fact that we have been invited here today indicates that you really believe there is something that we can do together.

Senator NUNN. But there would not be a place to call right now if you were private sector and you thought you were being invaded; there is not a single number to call, or a group of people to go to?

Mr. NEUMANN. No. One of the biggest problems has been that the banking folks and a lot of other infrastructure folks do not like to report when they have been attacked or when they have been had.

Another problem, though, is that there may be cases that we do not know about—that nobody knows about. If in fact the "Internet worm" of 1988 had done what it had intended to do, it was an exercise to demonstrate how bad the infrastructure was at the time; but if it had succeeded in doing what it was supposed to do, no system would have perceived any attack. It was not intended to be destructive. It was intended merely to find out how bad the situation was.

The generalization of that is that there could be many attacks, implanting Trojan horses, time bombs and whatever else, that you never realized had happened until perhaps the time at which they were triggered. But the idea that there may be a lot of things going on that we do not know about that the corporation involved, or the banking industry or whatever, do not even realized has happened to them, this represents a very serious potential problem.

Senator NUNN. What about somebody out there who has a personal computer and would like to know how to increase their own privacy and their own security? Do you have any words of advice for someone in that category?

Mr. ANDERSON. I would defer to Peter, because I think there should be much greater use of effective encryption technology throughout our society, and Peter is the expert on that.

Mr. NEUMANN. I certainly agree with that. I think the routine use of cryptographically-based authentication would be a tremendous help. The idea of privacy is something that has not even come up very much in this context. Privacy is perhaps one of the most difficult problems. I know Senator Glenn has a strong interest in that one, and I was hoping that he would be here so we could discuss it a bit.

Privacy is something that you really do not realize you have until after you have lost it, and there are a lot of cases in my anthology of horror stories where people have, as a result of losing their privacy, whether it is their Social Security number or certain information about themselves, had attacks on their person; for example, they have had other people masquerading as them.

There is a large collection of problems that result. If you just look at the FBI-Secret Service-White House case that is going on at the moment, when you try to keep information within a closed community, it is very difficult.

So the privacy issues, whether you are talking about your home computer or the databases in which your identity appears, medical health records, Social Security records and everything else, all of that stuff is fundamentally vulnerable.

Senator NUNN. What would you advise someone listening in? Where should they go? Is there a publication? Is there a book? Is there a magazine article? Is there something that you have written that would tell a personal computer owner how they can take certain steps that would be affordable to increase their privacy?

Mr. NEUMANN. Well, on the Internet, there are a lot of news groups that deal with these issues. I run one of them, called "The Risks Forum." I would urge all of the people who have their own personal computers, as well as the entire Senate and House, to start getting involved in the Internet and get online and realize the glorious benefits and the considerable risks, and how you can balance them.

Senator NUNN. So you can go online and find various sources of protection, including encryption, including, I assume, code words; right?

Mr. NEUMANN. There is a Swiss bulletin board that will give you some wonderful crypto that you cannot bring into this country and then export again, but you can bring it in from Switzerland—or anywhere else in the world.

There is at the moment a good bit of work in the research community, and that really needs to get out into the practice, I think. Mr. ANDERSON. Peter is being uncharacteristically modest, but his book, "Computer-Related Risks," published about 2 years ago is a wonderful compendium. The first thing that private citizens and industry should do is be aware of the risks so that then, they are sufficiently scared to implement various procedures. I think the book is a wonderful compendium of what can go wrong, either accidentally or deliberately, and I would commend that book to anyone wanting more information on this subject.

Mr. NEUMANN. Why, thank you.

Senator NUNN. What about the government effort so far, Dr. Molander? The U.S. Government, DOD, CIA, the broader intelligence, the Department of Energy and others—have you looked at what priority government has given this problem and whether you believe there is enough priority being given?

Mr. MOLANDER. This is, as Director Deutch emphasized, a very new subject. I would say that up until relatively recently, you could characterize the government response as a collection of cottage industries that are taking responsibility for these problems within their individual government agencies. In the course of obtaining participation in the exercises from different government agencies, both on the defense/intelligence side and the domestic side, we have been able to find in virtually every agency people who are concerned about these problems along with a growing recognition that some kind of coordinated effort is required.

The anticipated commission to be set up under the Attorney General's aegis is a major step in this direction. I think, as in lots of subjects, and one which Peter Wilson and I are particularly familiar with—counter-proliferation. The first look at this problem is real sobering, and it is easy to say, well, let me work hard on today's problem. This is tomorrow's problem.

But I think increasingly, people are recognizing, as your hearings have brought out, that it might be tomorrow's problem, but as sure as the sun is going to rise, it is going to come, and the effort that is underway right now is encouraging. But with the number of different equities that are involved and the challenge to achieve cooperation and communication and information exchange across institutions, within infrastructures and between infrastructures and the government, there is a long way to go. But I think the signs right now are very encouraging, and I probably would not have said that a year ago.

Senator NUNN. Mr. Wilson, do you have any comments you would like to make, or Mr. Riddile?

Mr. WILSON. Just briefly, Senator, I think that the proposal that your staff has considered of creating a threat center of some type is really vital. We really do need some sort of mechanism to coordinate within the Federal Government agencies as well as amongst industry.

However, our problem is that we do not know what the baseline is, and as Dr. Neumann talked about, we do not know what "cyber peace" is, much less "cyber war" in a certain sense, and that is one of the major challenges. It is sort of like doing weather forecasting without having any past record of what has happened in the systematic sense. Therefore, I think that that is probably one of the most important early initiatives that has to be given very serious consideration—how to build a credible system to do risk assessment, to do threat assessment.

And then, finally, I would just make a comment to follow up on some of the other comments that Dr. Anderson and Dr. Neumann made. It is really vital for the government early on to start communicating to the American public about the risks, if you will, the down side, of this extraordinary revolution which Dr. Deutch alluded to, which is incredibly compelling. I mean, after all, we are constructing kind of a new. high-performance free enterprise system, so there are very powerful forces to go down these directions of exploiting this technology, but we have to acknowledge that there are profound both public and private risks. So one of the early roles of an organization as positive as the threat center might well be in the public education process, somewhat analogous if you will to the CDC of Atlanta—that is, warning and informing industry and individuals about both the power and the down side of this extraordinary revolution.

Senator NUNN. Sort of a "computer disease center."

Mr. NEUMANN. Yes.

Mr. WILSON. Yes.

Senator NUNN. Interesting.

Mr. Riddile, do you have any other comments??

Mr. RIDDILE. Dr. Molander describes my thoughts very well. This is a serious problem to national security, but it is not too hard it is not too hard to solve this.

Senator NUNN. Dr. Molander, I think you have some closing observations based on the exercise. How would you summarize the lessons learned, and what are your recommendations now? I will also ask Dr. Anderson, Dr. Neumann, Mr. Wilson and Mr. Riddile if they have any comments or additions.

Mr. MOLANDER. This is a quick overview of some of what we have gleaned from the exercises and our participation, just very quickly. What are the features of this problem as we see them? There is the problem of low entry cost that you mentioned—almost anybody is going to be able to mount some kind of attack. The real issue is whether we can deal with coordinated attacks in the effective way that we would like to as a country. The whole area of blurred boundaries, whether it is the boundaries between law enforcement and intelligence, geographic or otherwise, is another big part of the problem.

Perception management is another problem. We have all seen "Forrest Gump;" you have to wonder if it is really going to be the President who is on the television at some point in the future.

The emphasis on strategic intelligence from Director Deutch understanding what adversaries are out there now working on this subject and what their capabilities are going to be. It is not like being able to do photo-reconnaissance of the Soviet Union and seeing missiles silos and submarines being built.

The problem of tactical warning and attack assessment is a big problem. Are we under attack? The President, I guarantee you, will be pounding the table at some point in the future, asking that question and not being able to get a definitive answer. The coalition's problem in terms of our national military strategy could be one of our most severe problems. I think you could anticipate that an adversary, especially in regional strategic crises would target our coalition partners in order, for example, to take away the use of Saudi or Egyptian air bases in a future Persian Gulf crisis.

And of course, there is the problem of the continental U.S. being vulnerable.

The next slide is one that we like because people frequently ask well, how hard is this problem, and where are we on solving it This runs the perspective from, hey, this is not a problem; we are the sole surviving superpower, and we will be able to get a handle on this—just give us a little time and a little money—down to well, maybe this is a serious problem, but it is a little early to tell and all the way down to my God, it could not be worse.

What we have tended to see in the exercises, where people from both sides of government and from the private sector engage to gether on this problem, is that as people share the exercise experience and hear other people's stories about their particular sectors people move down that spectrum and generally come away feeling like this is a more serious problem than they thought when they entered.

The next couple of slides just highlight some of the things that we have been talking about here, the unresolved issues. It is a healthy agenda, but as Andy says, none of this looks beyond the ability of this country to take on. What will be the roles here whether it is in the threat center or in the costs associated with responding to this threat? The whole issue of risk assessment—how big a risk do we face right now and might we face in the future, which means combining what does the threat look like and what are our vulnerabilities. This has really not been developed yet. We do not really know what our vulnerabilities are in these various key infrastructures.

Indications and warning, as has been mentioned, would be an important function in the threat center. How should we organize to do this exchange of information; what is happening in the key infractructuree sectors versus what is happening with the government, what does the government knows about threats, etc.?

There is also the whole issue of reconstitution. As we have tried to emphasize, this is in terms of thinking about Nation state threats, a threat of potential massive disruption, not massive de struction. And the disruption might be made quite temporary. It is one thing for someone, if you will, to blink the lights at Wrigley Field during the World Series—if I might be so fanciful—it is quite another thing to turn them off. And in this whole issue of reconstitution and recovery, I think, possible financial incentives from the government to establish more effective reconstitution capability might be part of the legislation agenda that you have.

Attack assessment—the whole issue of where should this be performed in order that we can understand better who is attacking and what has been attacked.

The next and final slide has a few more of those—damage assessment—how bad have we been hit? In the nuclear business, we took a lot of trouble to ensure that we could tell just what kind of damage had taken place in an attack. Here is a real challenge here, because that will, of course, dictate the kind and character of the response that the country might make to an attack.

The whole information-sharing business one cannot emphasize enough.

Education—there is an issue of a national education strategy here, and not just for one's personal computer, but just in the same sense of AIDS education, the kind of education that would carry you through all of your life in terms of safe practices, whether one is at home or at work, in dealing with these kinds of threats.

And finally, quite obviously—and these hearings bear testimony to it, as has much of the work that is ongoing in the executive branch right now—is really a rethinking of national security strategy and our national military strategy as it now exists, with its emphasis on high-performance, power projection, just-in-time logistics. All of that is going to have to be rethought in the face of the kinds of threats that are occurring here.

Again, I commend you and the Subcommittee for your efforts.

Senator NUNN. Well, thank you for this excellent work. I understand you have another one in process.

Mr. MOLANDER. Yes. We have just finished a series of exercises. The exercise scenario that you were exposed to here today is one of a regional adversary trying to interrupt power projection. The one we looked at most recently was a peer competitor and a more direct attack on the United States, and hopefully, within a matter months, we will have another report that tells what we learned from these exercises.

Senator NUNN. Good. Any closing comments—Dr. Anderson, Dr. Neumann?

Mr. ANDERSON. I guess I would like to close on a positive note. There has been a lot of "sturm und drang" here about this problem, as there should be, but over and over, our society has demonstrated that the functionality that we are getting out of cyberspace, out of the interlinking, the electronic commerce that is coming along, those advantages are dramatic, and this should not dissuade people from moving cautiously into cyberspace and using this functionality. I would say that in general, echoing some earlier comments that were made, cyberspace is a net good, and I believe we can handle the problems if we coordinate our attention and do the actions that are required. But it is a net good for our society, and we should be enthusiastic about cyberspace.

Senator NUNN. Dr. Neumann?

Mr. NEUMANN. Thank you. I urge you to look at my written statement, which has a whole bunch of recommendations that the government might consider——

Senator NUNN. I will.

Mr. NEUMANN [continuing]. And the conclusions that I came to. I would like to make a few final remarks that I have not covered and that are not in the printed statement.

The first is that we are dealing with an international problem, and we are going to be very much handicapped if we try to find national solutions to some of those problems. We clearly have to defend ourselves first, but we have to find ways that make things work internationally. Second, there is a lot of good research and development kicking around, and we have to find ways of getting that into the products. The government increasingly has to rely on commercial infrastructure. It is very difficult anymore for anybody to specify a custombuilt system that is totally incompatible with everything else, that takes no advantage of all of the standards and techniques that are well-established today. The idea of building an air traffic control system out of rubberbands and bailing wire is not very appealing anymore. It should use readily available, standardized components

Now, to deal with that, we have to look at the history. The air traffic control system is a fine example; the IRS is another exam ple. Having served on the Commissioner's advisory group for the last 2½ years, I have been trying to help them in developing then modernization system. The government is now saying let us turn that over to the DOD. The DOD's track record is maybe marginally a little bit better than the IRS', but when it comes to issues such as privacy, which both Senator Glenn and Senator Pryor have had a hand on the IRS—I mention in my statement that I appeared in a tape with them for the IRS training—of trying to elevate the privacy requirements. The IRS has done a phenomenal job in pulling together the privacy requirements. If those requirements go down the drain in the implementation of a system, we have lost a significant step forward because they have done a wonderful job in characterizing the privacy needs.

But what typically happens is that when you go to build a system, you realize that the security requirements are too difficult. and you cannot meet them, the reliability requirements are difficult, the privacy requirements are difficult, and you say, well, we will have to waive those or bend them a little bit.

The idea of building large systems and having those systems satisfy the requirements is very important, and I spend a good bit of time in my written statement dealing with that problem.

I also would end on a positive note, that we can get rid of some of the fundamental vulnerabilities that we have—for example right now, we have fixed passwords flying around over the Internet. When you log in remotely to a different system, your password is vulnerable because it is exposed, and it is very easy for it to be intercepted. So rather than give you guidance on how often to change your passwords, it is important to realize that it does not matter how often you change it if, every time you change it, you send it over a network where it is immediately captured The answer to that one is that we must have authentication that is based on good cryptography that gets around that problem.

If we can in fact get some of the basic infrastructure improvements in place reacting to authentication, confidentiality, privacy, nonrepudiation and availability, then I think the situation will look a lot better in the year 2000 or the year 2005. But if we do not make that move now, we are going to be in very bad shape.

Senator NUNN. Thank you.

Dr. Molander, do you have any closing thoughts?

Mr. MOLANDER. Just very briefly, right now, this is kind of an empty canvas in terms of an action plan about what to do about this problem in the large, and I think that, like with any empty canvas, the first few things that go on it are going to be noticed here. In that sense, it is a real challenge to American politics considering the breadth of equities that are involved here. So I would particularly welcome politicians of skill who have survived many national security debates in these chambers to this problem. It is going to take our best politicians to work out these problems.

Senator NUNN. Thank you very much.

Mr. Wilson?

Mr. WILSON. I will just concur with Dr. Molander's remarks that it is really vital, and I think it is very important that you have been holding these hearings to start to air this set of enormous issues because clearly, we have developed and worked with the Department of Defense, and these problems are far larger than OSD and the Department of Defense, and there has got to be a serious public airing of the large, critical social, economic, and military strategy issues that this extraordinary revolution has brought in front of us.

Senator NUNN. Without public understanding and education on this issue, there would be no government solution that would be sustainable in my view.

Mr. MOLANDER. Correct.

Senator NUNN. Mr. Riddile?

Mr. RIDDILE. No, sir. Thank you for the opportunity.

Senator NUNN. Thank you all. We will stay in touch with you. We will have our next hearing on July 16 with Deputy Secretary of Defense White and Deputy Attorney General Jamie Gorelick.

Thank you.

[Whereupon, at 12:27 p.m., the Subcommittee was adjourned.]

SECURITY IN CYBERSPACE

TUESDAY, JULY 16, 1996

U.S. SENATE,

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, OF THE COMMITTEE ON GOVERNMENTAL AFFAIRS, Washington, DC.

The Subcommittee met, pursuant to notice, at 9:30 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Sam Nunn, presiding.

Present: Senators Nunn, Cohen, and Levin.

Staff present: Daniel S. Gelber, Chief Counsel to the Minority; John Sopko, Deputy Chief Counsel to the Minority; Alan Edelman, Counsel to the Minority; R. Mark Webster, Investigator to the Minority; Jim Christy (AFOSI Detailee); Harold Damelin, Chief Counsel to the Majority; Carla J. Martin, Chief Clerk; Ariadne Allan, Investigator; Mark Forman (Senator Stevens); Gina Falconio (Senator Cohen); Bill Greenwalt (Senator Cohen); Jessica Korn (Senator Domenici); David Plocher (Senator Glenn); Deborah Lehrich (Senator Glenn); Nancy Langley (Senator Akaka); Jeremy Bates (Senator Dorgan); and Greg Rhode (Senator Dorgan).

OPENING STATEMENT OF SENATOR COHEN

Senator COHEN [Presiding]. The Committee will come to order. Senator Roth has been detained and hopefully will be here later, but we will begin in the meantime.

First, I want to commend Chairman Roth and also Senator Nunn for their initiation of a series of hearings dealing with a threat to our computer systems. I think we have learned in the previous hearings that cyberspace is a two-headed coin. It has magic certainly on one side and the potential for monstrosity on the other.

Churchill perhaps foresaw much of this, and he said in a rather metaphorical way that we can glide toward the mysteries of the 21st century, or return to the Stone Age on the gleaming wings of science, and that is precisely the kind of threat that we face today.

Senator Nunn and Senator Roth have raised a number of questions that we have to address, certainly in terms of the fragility of our systems as we leap out into space, how much more dependent our national security systems are upon communications, how fragile those systems are, a long litany of questions that we have to ask and address.

I would like to make just a few brief comments before turning to Senator Nunn. I think, first of all, we need to develop a comprehensive strategy. I don't think we are going to get anywhere if we don't work to reconcile the competing national security issues, law enforcement and privacy issues, which up to this point have prevented any adequate solution.

[^] The lack of trust between individual citizens, corporations, and the government's law enforcement and intelligence communities is immense, and that gap is to be bridged. It is, indeed, a great one.

If we choose piecemeal solutions without meeting the concerns of all parties, I am concerned we are going to end up in perpetual gridlock.

Second, we should not wait for perfect intelligence estimates that specifically identifies which nations and groups have developed information more for capabilities before we act on our vulnerabilities.

Again, we should heed Churchill's advice when he said the dangers which are warded off by effective precaution and foresight are never even remembered.

If we are not to remember the information security problem, we need to protect our security at the first sign of vulnerability, and that is now.

We know that the security of information is critical to the effective functioning of the U.S. economy, and our Nation is increasingly dependent on computer networked information. Our knowledge of the magnitude of the threat is inadequate, as most cyber attacks are not detected, or if detected, rarely reported, and this lack of information makes it very difficult to adequately measure the threat and prepare appropriate responses.

There is a danger, however, that we are spending too much time on analysis and not enough on action. In order to avoid paralysis, we have to assume intent and project capabilities.

If we can penetrate and attack our own systems, we should expect our adversaries are going to be able to do so soon, and we should act accordingly. There are many nations and groups that have, in the CIA director words, the intent, and in today's marketplace it is not hard to purchase that technological capability and the people to do the job.

In addition to the intent and capability, what is also needed to effectively attack the United States systems, as Director Deutch correctly pointed out, is detailed information about the target, its vulnerabilities and access.

Information about these systems will be a prime intelligence objective of our adversaries, and we have to do everything in our power to protect this information.

The third point I would like to raise is that we should not waste too much time emphasizing a legal solution to the problem, but instead should focus on active and passive information defenses.

The goal of the intruder is to get in, to do damage, and to get out and not be detected, and up until now, those intruders have been very successful in this effort.

Strengthening law enforcement measures may not work when the criminal is halfway around the world and has crossed several jurisdictions to get here. It might be helpful to strengthen our laws against cyber attacks, but we must not be too optimistic that better law enforcement and prosecution is going to deter any, but those whose intent is but virtual voyeurism.

As a first line of defense, we need to develop and allocate enough resources for an effective security regime made up of policies, procedures, practices, technology, and oversight that reinforces accountability and sound security.

Finally, a lot has been said recently about the need for greater public/private corporation. As we have seen, the private sector has been reluctant to publicly admit that it has information security problems, probably for fear of provoking a market reaction.

I would suspect that those forward-looking firms will do everything possible to secure that information that is vital to their competitive survival, but at present the private sector seems not to want the government's help. It probably stems from the observation that if the Federal Government can't protect its own system, how can it be much help to the private sector? I fear that some segments of our government may be chasing new missions when they have inadequately performed old ones, and it seems that agencies responsibility for information security are more interested with turf battles and bureaucratic infighting and carving out new territory than they are about securing vital governmental information.

Government information security is in shambles, and we should address that issue as quickly as possible as our first priority. We have to establish the public's confidence in the effectiveness of the Federal Government security measures to protect not only national security data, but private data with citizens as well.

In the meantime, we have to have much greater cooperation between the public sector and the private sector in order to protect the infrastructure that would likely be the target of a terrorist or a wartime threat and then look to market-based initiatives to take care of the rest.

Again, I want to thank Senator Nunn and Senator Roth for their initiative. This is an issue of immense importance to our security, not only national security, obviously a first priority, but also for any law enforcement and the protection and the privacy of our citizens. Senator Nunn.

OPENING STATEMENT OF SENATOR NUNN

Senator NUNN. Thank you very much, Chairman Cohen.

In our previous three hearings, we have heard from numerous witnesses who I believe have established why all Americans need to be concerned about the threats we are discussing.

Our country is becoming increasingly dependent on the information infrastructure for our transportation, for our energy, for our commerce, as well as for our national defense. Unfortunately, hostile nations and terrorist organizations can with relative ease acquire the techniques to penetrate information systems.

Indeed, in response to a question as to where he would place the threat of cyber-based attacks in terms of overall threats to the United States, CIA Director John Deutch stated as follows in our hearing, "I would say it is very, very close to the top, especially if you ask me to look 10 years down the road. I would say that after the threats from weapons of mass destruction . . . nuclear, chemical, and biological weapons, this would fall right under it; it is right next in priority, and it is a subject that is going to be with us for a long time."

Director Deutch's analysis of this threat is quite sobering. It came after the General Accounting Office estimated that the Department of Defense may have experienced as many as 250,000 cyber-based attacks last year.

In today's hearings, we will explore what our alternatives are in responding to this threat. How do we protect ourselves from the threat of attack and what would we do in the event we detected such an attack occurring are extremely important questions which go to the heart of our national security.

We are fortunate to have a series of important witnesses this morning. Senators Patrick Leahy and Jon Kyl have been leaders in the Senate on matters of protecting information infrastructure. They have jointly sponsored S. 982, the National Information Infrastructure Protection Act, and are rightly looked to within this body as experts on the matters of national security and cyber security. So I look forward to their analysis, and I know it will be very helpful to our Subcommittee.

We also have with us Deputy Attorney General Jamie Gorelick and Deputy Secretary of Defense John White. Ms. Gorelick has been the Chair and Mr. White has been a key member of the Critical Infrastructure Working Group, an interagency task force which was established by the Attorney General in response to a presidential directive, Decision Directive 39, to identify and assess the source and nature of threats against key parts of the Nation's infrastructure and to present both short- and long-term options for addressing those threats.

Today, Ms. Gorelick and Mr. White will announce the findings and recommendations of the working group, and we are glad that they are making those announcements here.

The advance of the computer age has presented the United States with a whole new range of national security challenges. Through this series of hearings, the Subcommittee has attempted to define these challenges, to assess our current ability to meet them, and to provide a forum for a discussion of what further steps need to be taken to prepare for the future.

Senator Cohen has captured the challenge, I think, extremely well in his opening statement, and I certainly agree with that.

In this regard, I am particularly interested in hearing the results of the working group by the administration. Their recommendations will, in large part, define the country's policies with respect to the challenge of cyber security. It is, thus, critical that Congress know how the key executive branch agencies charged with protecting our national security view this challenge and what steps they propose to address it, and when I use the term national security, I make that a much broader term than might be construed by some. It includes our critical infrastructure and systems here in this country.

I am pleased that the private sector, as I understand the administration's proposals, which will be outlined this morning, will be clearly involved. Clearly, we do not have private sector/public sector cooperation and trust at this juncture in this important area, and clearly, we must have that if we are going to protect both the public sector and the private sector in the future. So this is an area of serious challenge, and I know that that is part of the consideration that the administration is making in their presentation this morning. Mr. Chairman, I don't see Senator Leahy here yet, but he will be here. We have a 10 o'clock cloture vote. So, perhaps, I would suggest that we try to get both of our Senators as witnesses this morning, Mr. Kyl first and then Senator Leahy, and perhaps we can get through those two witnesses and then come back and hear from Ms. Gorelick and John White.

[The prepared opening statement of Senator Nunn follows:]

PREPARED OPENING STATEMENT OF SENATOR NUNN

Today the Subcommittee holds the fourth in its series of hearings examining cyber-based threats to our national information infrastructure. In our previous three hearings, we heard from numerous witnesses whom I believe established why all Americans need to be especially concerned with these threats. Our country is becoming increasingly dependent on the information infrastructure for our transportation, our energy, our commerce, and our national defense: unfortunately hostile nations and terrorist organizations can, with relative ease, acquire the techniques to penetrate information systems. Indeed, in response to a question as to where he would place the threat of cyber-based attacks in terms of overall threats to the United States, CIA Director John Deutch stated as follows:

I would say it is very, very close to the top, especially if you ask me to look 10 years down the road. I would say that after the threats from weapons of mass destruction . . . nuclear, chemical and biological weapons, this would fall right under it; it is right next in priority, and it is a subject that is going to be with us for a long time.

Director Deutch's analysis of the threat is quite sobering and came after the General Accounting Office estimated that the Department of Defense may have experienced as many as 250,000 cyber-based attacks last year. In today's hearing we will explore what our alternatives are in responding to this threat. How we protect ourselves from the threat of attack and what we would do in the event we detected such an attack occurring are extremely important questions which could go to the very heart of our national security. We are fortunate to have with us this morning an array of eminent witnesses to discuss these issues.

Senators Patrick Leahy and Jon Kyl have been leaders in the Senate on matters of protecting our information infrastructure. They have jointly sponsored S. 982, the National Information Infrastructure Protection Act and are rightly looked to within this body as experts in matters relating to cyber-security. I look forward to this analysis of the situation we face and their recommendations for future action.

We also have with us Deputy Attorney General Jamie Gorelick and Deputy Secretary of Defense John White. Ms. Gorelick has been the Chair and Mr. White has been a key member of the Critical Infrastructure Working Group, an inter-agency task force which was established by the Attorney General in response to Presidential Decision Directive 39 to identify and assess the source and nature of threats against key parts of our Nation's infrastructure and to present both short and longterm options for addressing these threats. Today, Ms. Gorelick and Mr. White will announce the findings and recommendations of the Working Group.

The advance of the computer age has presented the United States with a whole new range of national security challenges. Through this series of hearings the Subcommittee has attempted to define these challenges, to assess our current ability to meet them, and to provide a forum for a discussion of what further steps need to be taken to prepare for the future. In this regard I am particularly interested in hearing the results of the Working Group. Their recommendations will, in large part, define this country's policies with respect to the challenge of cyber security it is thus critical that the Congress knows how the key Executive Branch agencies charged with protecting our national security view this challenge and what steps they propose to take to address it. I am pleased that the private sector will be involved. It is clear that the partnership of trust and confidence between public and private is essential to protect both.

I hope that today's hearing will be only the beginning of a continuing dialogue among Congress, the Administration, and the American public as a whole on the topic of cyber security. This is indeed an area in which great challenges lie before us, but I am confident that by working together we will be able to meet them.

Senator COHEN. Senator Kyl.

TESTIMONY OF HON. JON KYL,¹ A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KyL. Thank you very much, Mr. Chairman.

Senator Leahy, I think, was going to speak primarily to the legislation which Senator Nunn addressed, and as a matter of fact, here he is now. So I will defer to him on that and discuss instead the amendment to the Defense Authorization Bill which the administration should be dealing with right now.

Let me say first, I do appreciate the opportunity to appear before this Subcommittee and especially to compliment both Senator Roth and Senator Nunn for their leadership in addressing the problem.

Last year, Senators Bingaman, Roth, and I successfully offered an amendment to the Defense Authorization Act, which is now public law, which required the President to report to Congress, and I am quoting now, "The outline of a plan to establish procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions regarding strategic attacks by foreign nations, groups, or individuals, or any other entity which invades the national information infrastructure; and an assessment of the future of the National Communications System."

I offered this amendment because there is, at present, no defense against invasions of the nerve centers of our society, which include our defense, telephone, public utility, and others. As you said, Mr. Chairman, I think it is our obligation to act at the first sign of vulnerability.

My fear is that the military has little ability to protect our country from strategic assaults on the NII and no legal or political authority to protect our information systems against another country's offensive. The CIA Director John Deutch said at his Senate confirmation hearing, and I am quoting, that "This is a very important subject . . . which we really don't have a crisp answer to."

The threat is very real. According to the NSA, over 100 countries are working on information warfare techniques. The President and the Congress have an obligation to develop a comprehensive national policy that coordinates national security defense for both the U.S. Government and the private sector users of our national information infrastructure.

Several things have changed in the last 10 years that demand the modernization of our current national security communications and emergency preparedness posture. The increased pace of technological innovation appears to have rendered previous legislation and administration action in this area inadequate. Moreover, standing programs for emergency preparedness have withered, and the cold war's end has encouraged a false perception that these things no longer matter.

Today, we don't have answers to even the simplest of questions. How vulnerable to attack is the national information infrastructure? Who, what, and where are the threats? What is the specific technical nature of the threats? Could we, for example, detect an adversary's intelligence preparation of a simulated information infrastructure battlefield? How can government best engage various private sector elements on national security grounds?

¹The prepared statement of Senator Kyl appears on page 380.

Currently, no department, agency, or individual in the U.S. Government has responsibility for the mission. During the cold war, the intelligence community, with the help of the Department of Defense, had the indications, warning, and attack assessment responsibilities. The cold war concept of indications and warning/attack assessment focussed exclusively on the physical foreign attack by aircraft or missiles, for example, but a strategic attack on the NII is radically different from an ICBM attack, making the old practices, frankly, obsolete. It is one thing to have procedures in place to determine if an enemy is stockpiling plutonium. It is very difficult to determine if someone is planning a strategic attack on our national information system.

Interference with the U.S. information infrastructure increasingly means an attack on privately owned, commercial networks, systems, and facilities, like our banking, utilities, and transportation systems. It is important to note that such an attack might first be visible to the privately owned or controlled entities in the private sector, not to the government.

Until now, concerns about the possibility of a strategic assault on the national information infrastructure have largely gone unaddressed. For example, the President's own National Security Telecommunications Advisory Council, NSTAC as it is referred to, recently wrote to the President with concerns on this subject. The President's response was lukewarm.

My amendment, which required the President to report to Congress by June 10, has also gone unanswered. On May 8, I wrote to the President asking for a status on the report, as well as offering assistance. His reply, which came from Tony Lake was, frankly, quite inadequate.

I am aware that our report requirement is a tremendous task. No one knows the answers. No one expects those answers to be forthcoming immediately.

Senator NUNN. Senator Kyl, on that report, is the main thrust of the report a comprehensive threat assessment? Is that the main thrust of it?

Senator KYL. Yes. It is to assess the future of the system, but also, as I said, to outline a plan, at least to begin the process of outlining a plan to establish procedures, capabilities, systems, and processes necessary to perform the indications, warning, and assessment functions concerning strategic attacks.

As Senator Cohen pointed out, and I will conclude with this, there is a significant strategic element to this, not just a domestic concern.

My point was that our report requirement, which has not been satisfied, was to begin a process, and I am glad to note that perhaps it was work by this Committee that finally sparked some interest.

I understand yesterday the President issued an executive order that established a commission. I am not sure exactly what that commission's mandate is, but presumably it deals with the same subject. So I am hopeful that a report will be forthcoming soon in response to the law's requirement.

I am also aware that Attorney General Reno and Deputy Attorney General Jamie Gorelick have been very active in trying to enhance the FBI's capability to handle a terrorist threat against the national information infrastructure, and that there are intelligence community plans to create a warfare technology center at NSA.

While I commend the Department of Justice for its work, I again reiterate that there has to be leadership at the highest level, the President, and that the threat must be seen as a strategic one.

Rogue countries might attack a system, either directly or by using terrorists, and as I said before, there are reports that over 100 countries are working on developing weapons and techniques to conduct an information attack.

So DOJ, CIA, and DOD are at least some of the important contributors to a national defense against attacks on our information systems.

Mr. Chairman, our amendment was intended to spark planning at the President's level. We hope that that can occur. We hope that the President and the administration will work with Congress, and that this important issue can be addressed before our country's communication system is attacked.

I thank you very much for your interest in the issue and pledge my cooperation with you to try to pursue the matter as rapidly as we can. Thank you.

Senator COHEN. Thank you, Senator Kyl.

Senator Leahy.

TESTIMONY OF HON. PATRICK LEAHY,¹ A U.S. SENATOR FROM THE STATE OF VERMONT

Senator LEAHY. Thank you, Mr. Chairman. Obviously, I agree very much with what Senator Kyl has been saying, and I worry about how we do safeguard our critical national computer networks.

As you know, if you take the U.S. Senate as an example, we have diligently and steadfastly tried to stay at least 10 years behind the curve on computer technology. In the Senate, technology probably upgrades itself amazingly every month or so.

Senator COHEN. I am not sure the terrorists consider us to be a prime target.

Senator LEAHY. I understand. No, I think we are the only ones who consider ourselves as prime targets. Look at the way we make our buildings and our institutions up here as inaccessible as possible to honest people and, of course, absolutely no barricade whatsoever to somebody who really wanted to create damage. We do it to frustrate staff.

Senator NUNN. The Senate made a giant leap, Senator Leahy, when you and Senator Cohen and I arrived by starting to pay off with checks on the payroll rather than cash. So don't forget that.

Senator LEAHY. That is true, and it is hard to find a decent quill pen these days in the Senate. So we are moving. In the real world, many people depend on the security and reliability of their computer networks, and I have been trying for about 10 years now to make them more secure.

We know that our computer networks remain vulnerable to the threat of attacks by hackers and high-tech criminals and spies.

¹The prepared statement of Senator Leahy appears on page 385.

This is the reason why Senators Kyl, Grassley, and I introduced legislation to increase the protection for computers, both the gov ernment and the private ones, and for information on those computers, from the threat of computer crime.

The legislation of the National Infrastructure Protection Act was reported favorably by the Judiciary Committee last month, and I hope it will be taken up by the Senate prior to the August break

Computer crimes are on the rise. Just look at the facts. You have already heard from the Computer Emergency and Response Team at Carnegie-Mellon University. According to their most recent report, over 12,000 Internet computers were attacked, in 2,412 incidents in 1995 alone.

You heard the results of a survey conducted jointly by the Computer Security Institute and the FBI, showing that 42 percent of the respondents sustained an unauthorized use or intrusion into their computer system in the past 12 months. That is not just ε law enforcement matter. It is an economic one, too. The breaches of computer security are resulting in direct financial loss to Amer ican companies from the theft of trade secrets and proprietary information. That hurts our economy.

Take the December 1995 report by the Computer Systems Policy Project. That is comprised of the CEOs from 13 major computer companies. They estimate that the financial losses in 1995 from breaches of computer security systems range from \$2 billion to \$4 billion. Imagine if we had bank robberies of \$2 billion to \$4 billion. This would be a national crisis, but this is what is happening.

Worse than that, the report predicts that these numbers could rise in the year 2000 to \$40 million to \$80 billion worldwide. The estimated amount of loss is staggering. One U.S.-based manufacturer said, "We just lost a major pro-

One U.S.-based manufacturer said, "We just lost a major procurement in a Middle Eastern country by a very small margin to a state-subsidized European competitor. We were clearly breached Our unique approach in financial structure appeared verbatim in the competitor's proposal. This was a \$350-million contract worth over 3,000 jobs." In other words, they were able to get into an American company's computer, steal their whole proposal, drop the price by a tiny fraction after the Americans had done all the work and we lose all these jobs and all of these millions of dollars here in the United States.

Armed with a modem and a computer, a criminal can wreak havoc on computers located here in the United States from virtually anywhere in the world. There are no borders or checkpoints in cyberspace. Communications flow seamlessly through cyberspace across datelines and the reach of local law enforcement.

To give you some examples, the 1994 intrusion into the Rome Laboratory, Griffiss Air Force Base in New York. Who did it? Not somebody in New York. It was a 16-year-old hacker in the United Kingdom.

In March of this year, the Justice Department tracked down a young man who had broken into Harvard University's computers, not from Cambridge, Massachusetts, but from Buenos Aires, and then he hacked into many other computer sites, including the Defense Department of NASA. Every technological advance provides new opportunities for legitimate uses, but also the potential for criminal exploitation. Existing criminal statutes provide a good framework for prosecuting most types of computer-related criminal conduct, but when technology changes and high-tech criminals devise new ways to use technology to commit offenses we have yet to anticipate, we have to assume that we are going to have to readjust and update our criminal code.

To give you an example of a gap in our current computer crime laws that the legislation that we have introduced would address: There is a new and emerging problem of computer-age blackmail. It is a high-tech variation of old-fashioned extortion.

In a North Carolina case, a person threatened to crash a computer system unless he was given free access to the system and an account. I mean, this is no different than saying to somebody, you own a clothing store, I want to be able to have free reign and take whatever I want, or in a few weeks a stink bomb will go off in your store and ruin all the clothes.

Well, it is the same thing with a computer. One can imagine a situation in which hackers could penetrate a system, encrypt a database, and then demand money to tell you how to decode it.

Take your own database, encrypt it, and say, OK, now we will give you the key to get it back, but here is what it is going to cost. So our bill adds a new provision to the law that would ensure law enforcement's ability to prosecute modern-day blackmailers.

We address cyber crime with up-to-date criminal laws and tough law enforcement. That still is only part of the problem. It is after the fact.

Obviously, the best defense is a good offense, and we should encourage Americans and American firms to take preventive measures to protect their computer information and systems. That is where you need encryption technology. It is an important tool in our arsenal.

Encryption enables all computer users to scramble their electronic communications. Peter Neumann has testified in these hearings last month and commented in his written testimony that "U.S. cryptographic policy has generally not been sufficiently oriented toward improving the infrastructure in that it has been more concerned with limiting the use of good cryptography. U.S. crypopolicy has instead acted as a deterrent to better security."

What has happened, unfortunately, is our own government has stood in the way of better encryption policy. It is another example of being years behind the curve.

Our law enforcement and defense agencies can't and should not carry the whole load for the security of our computer networks. We realized this when we passed the Computer Security Act, and we put the standards for developing Federal computer security standards in the hands of a civilian government agency rather than the NSA. The government should play a critical role in gathering intelligence about threats, obviously, to our computer systems. The government can do that, but the government should not control or stand in the way of technical solutions, and frankly, Mr. Chairman, that's exactly what our government has done in the past. Instead, our government's role should be to encourage the use of strong security. Encryption technology is good for Americans. It is good business for American firms. Government export controls that now bar our high-tech industries from selling strong encryption overseas are hurting our economy. They are not really helping our security, but they hurt our economy.

According to press reports, Netscape will start selling strong encryption software over the Internet today, but only to U.S. citizens or green card holders. They cannot sell this to foreign customers, and they will have to take extra steps to verify the nationality of its customers.

These foreign customers are going to be looking for security, but they are going to have to look to some other company, not American companies, and foreign competitors are only too willing to fill the void created by U.S. export restrictions. We are really hiding our heads in the sand in this regard.

Foreign manufacturers are manufacturing hundreds of products using strong encryption that Americans can buy here, but American companies are restricted from selling overseas.

Japan's Nippon Telegraph and Telephone Corporation, one of the largest in the world, is selling triple DES encryption. The reason why that is important, we developed it here in the United States. We are not allowed to sell it abroad, but they can take it and sell it abroad. So I think if we loosen export restrictions on encryption, we encourage the widespread availability of strong encryption. We are going to acting in a pro business and pro jobs and pro privacy manner. It is an area where the government is standing in the way of better security.

I think in Congress we may be able to say to the government get out of the way, there is a better way of doing it. You are behind the curve on this. You are not protecting the security of Americans, but in hindering us to create our own protection.

Thank you, Mr. Chairman.

Senator COHEN. Thank you very much, Senator Leahy and Senator Kyl.

Senator Leahy, I think both you and Senator Kyl have pointed to the essential paradox that we have. I am going to be holding a hearing later this week, as a matter of fact, talking about the need to have greater efficiency in the acquisition of our computer technology. Those of us who sit on the Government Affairs Oversight Committee are looking for greater efficiency, greater interdependability with each other; however, we purchase computer systems that not only can't talk to each other within an agency, but can't talk to other agencies. So we want to have greater efficiency, but of course, the paradox is the greater the efficiency, the greater the vulnerability or fragility.

So the more dependent we become upon technology, the more vulnerable to interruption, destruction, and as you pointed out, extortion. We are looking forward, it seems to me, to a series of electronic Pearl Harbors, not only militarily, but also financially or commercially. As you pointed out, the mere threat to shut down computer systems can cause chaos in the marketplace, in the hospitals, and in medical facilities. It brought to mind, as I was listening to your testimony, both of you, that back in the early 1980's we had testimony dealing with the interdependability of our energy systems. We had a young couple testify at that time. I believe their name was Lovins, and they talked about just a few key places in our electrical grid system, that could be targeted by terrorists to wipe out the energy systems of this country.

We saw just this past week or 10 days several States shut down by a loss of power for lengthy periods of time. It may have been an act of God. It may have been simply a malfunction, but in the future, we might even look for possible mischievous individuals or even terrorists.

So I think the time to act is now, and as we pointed out, I think everybody agrees it has to be comprehensive. It has to involve our national security. It has to include law enforcement and the commercial and private sector as well. We haven't even begun to really address any of the issues, while the problem is out there, racing ahead of us, another galloping horseman that we have yet to confront.

Senator LEAHY. Mr. Chairman, if I might just add, a few years ago, Dr. Robert Kupperman testified before the Judiciary Committee and laid out very graphically in an open hearing, and we have more graphic examples in closed hearings, of what can be done to shut down vast parts of our energy, telecommunication, air travel, banking systems and all in this country.

Some of the vulnerabilities of physical destruction are things like an energy pipeline. Others are using the cyberspace vulnerabilities of our switching stations for communications. The monetary effect of it could be enormous, but the ability to make the United States itself appear vulnerable is even greater.

Senator KYL. Mr. Chairman, might I also just clarify the answer I gave to Senator Nunn's question? You asked if our amendment to the Defense Authorization Bill was a threat assessment only, and I said no, and I want to reiterate that and emphasize it.

We called for an outline of a plan. We recognized that it would be impossible in the 6 or 8 months that the administration had to develop an actual plan, but I am discouraged that the deadline has passed and we haven't even received an outline of a plan yet. Again, I know it is hard. It is going to take years. It will be an evolving process. We are going to have to continue to improve on it, but I think that the best way to begin to prepare both the active and passive defenses that I think Senator Cohen spoke to here is to at least begin.

That first step of the journey is always the toughest, but if we can ask the administration to at least prepare an outline of a plan, then it will force everybody to get into the question of what is going to be necessary to protect the systems, not just what is the threat, and so I am hopeful that that will be included in the report and that it will be submitted shortly.

Senator COHEN. Senator Nunn.

Senator NUNN. Thank you, Mr. Chairman. Thank you, Senator Kyl and Senator Leahy, for your testimony.

I certainly agree with you that the administration does need to come up with a plan and also a threat assessment and the plan needs to be based on the threat assessment.

I would say that part of what we are going to have this morning is a plan of the administration, both an interim and a longer-term plan, but we have a long way to go. There is no doubt about that.

This is the fourth in our series of hearings, and there is no doubt about the fact that we have very significant problems, both in the public and the private sector.

One of the big problems is cultural. So many people who are operating computers don't know that they really are vulnerable and that what they put on the computers, indeed, can be seized by others pretty easily. Therefore, they are not alert to when there is an invasion and, therefore, don't usually detect that there has been an invasion of their computer system. Even when they detect it, the overwhelming statistics show they don't report it. So it is a combination of understanding, of education, of changing the culture, and changing the whole nature of the way we view this without losing the advantages, and that is what we all have to keep in mind.

We have huge advantages flowing from this information technology. In the effort and the quest for security, we don't want to knock out the advantages that we have, and that is the balance that has to be reached here.

I might say, I think we have a 10:10 vote. I think we have two back-to-back votes. So we might go ahead.

Prior to hearing from our next two witnesses I would like to mention that before the hearing on June 25, when Director Deutch testified, I told him the first question I was going to ask him was what the word "cyber" meant. He turned pale, looked as if he was going to faint, and I, therefore, decided not to ask that question, but just submit it for the record.

He came back with a letter, a rather detailed letter,¹ with the official CIA definition of "cyber," which I must say does not shed much light on the subject, but just in case our next two witnesses might want to review this letter and make sure the administration is in complete sync, I would release it. Senator LEAHY. Thank you for not asking us that question.

Senator COHEN. I think it is clear that Director Deutch decided to encrypt the definition.

Senator NUNN. Perhaps, Mr. Chairman, I should read it into the record, just part of it. "In light of my promise to keep the Congress fully and currently informed, I pressed for an answer.

"Central Intelligence Agency's (CIA) research revealed that the term 'cybernetics' was coined by the Father of Cybernetics, Norbert Wiener, in 1948. In Mr. Wiener's words, 'We have decided to call the entire field of control and communication theory, whether in the machine or the animal, by the name cybernetics, which we form from the Greek kybernetes or steersman.

"Department of State concurred with CIA's findings, but wished to point out that the Greek kybernetes is related to the Latin gubernator, meaning 'steersman' or 'governor.'

¹Exhibit No. 19 appears on page 511.

"The Defense Intelligence Agency is not yet ready to make a judgment, and is exploring the possibility that 'cyber' may have come from the Greek kybisteter or 'diver,' from which we also derive the word 'cybister' or 'a genus of large diving beetles.'

"I hope this clears up any confusion."

We are making progress here.

Senator COHEN. Would you care to come forward, Mr. Secretary, Jamie?

Before you begin your testimony, would you please raise your right hand. Do you swear the testimony that you are about to give will be the whole truth, nothing but the truth, so help you, God?

Mr. WHITE. I do.

Ms. GORELICK. I do.

TESTIMONY OF JAMIE S. GORELICK,¹ DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Ms. GORELICK. Thank you, Mr. Chairman and Senator Nunn and other Members of the Subcommittee.

First, I want to commend the Subcommittee for holding this series of hearings and for its foresight in recognizing the importance of this issue to the American people.

The concerns outlined by you, Mr. Chairman, by Senator Nunn, and here today by Senators Kyl and Leahy are ones that have concerned the Attorney General, myself, Dr. White, and others in the Administration. For several months now, we have been hard at work in trying to address this very difficult panoply of issues.

I think it would be helpful for me to begin with the most recent action by the President, then to give you some background as to what led up to that action, and then to answer any questions that you may have.

The call by Senator Kyl for a plan, I think, as Senator Nunn pointed out, will be addressed at least in the first instance by the step taken yesterday by the President and the steps that will follow therefrom.

Yesterday, the President signed Executive Order 13010.

Senator COHEN. Could I interrupt just for a second, Ms. Gorelick?

Ms. GORELICK. Yes, certainly.

Senator COHEN. If you could try to summarize it. I am looking at the clock. The first bells have gone off.

Ms. GORELICK. Yes.

Senator COHEN. It would be helpful. I think we could get both of your initial statements in before the break, if we could do that, because otherwise it would be a 20-minute break between the votes.

Ms. GORELICK. How much time would you like? I can give any version of this statement. So, if you tell me—

Senator COHEN. A shorter version.

Ms. GORELICK. I was already prepared to give the shorter version, not the full statement, but if you just tell me how much time you would like me to take, I will adjust my oral testimony accordingly.

¹The prepared statement of Ms. Gorelick appears on page 390.

Senator COHEN. I would say the next 5 or 6 minutes.

Senator NUNN. Mr. Chairman, I don't believe we are going to have time to get both of them in before we get—

Ms. GORELICK. I am quite flexible.

Senator NUNN. What I would suggest is to see if we can get Ms. Gorelick's statement in and then come back on Mr. White's because I think it is going to be very hard to get both of them. This is the policy, and I think with all the hearings we have had, we probably ought to take a little bit more time here.

Ms. GORELICK. As you wish.

Senator NUNN. I think we have about 10 minutes, 10 minutes for this part, 10 or 12 minutes.

Ms. GORELICK. Let me try to summarize, and I would ask that my full statement be submitted for the record.

Senator COHEN. It will be included in full.

Ms. GORELICK. The Executive Order concerns critical infrastructure protection. The order does two things. First, it creates a presidential commission to formulate policy recommendations to the President, including draft legislation on measures to protect what we are calling the critical infrastructure from both terrorism and other forms of attack. The order cites two types of threats, the physical threat and the cyber threat.

I would like to focus on the cyber threat. The infrastructures to be protected are eight in number. They include telecommunications; banking and finance; transportation; the electrical power systems; gas and oil storage and delivery systems; water supply; emergency services, including police, medical, fire and rescue; and continuity of government. The list is in the Executive Order.

These are infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on the defense or the economic security of the United States. The Executive Order sets a high threshold for defining an infrastructure as "critical." But as Chairman Cohen pointed out, during the energy crises in the late 1970's and early 1980's—and I was in the Energy Department at the time—we were very much aware of what damage could be done to the national security by hitting a few critical nodes of an infrastructure. That is the concept that informed the listing of these eight critical infrastructures.

The second point I'd like to make is that because these infrastructures are privately owned, the Executive Order emphasizes the need for close cooperation between the government and the private sector in the development of any solutions. So the Chair of the Commission will be a presidential appointee from the private sector, and the Commission itself will include representatives from the private sector, and private sector infrastructures in particular.

The third key point is that there must be interim responsibility for dealing with threats to and attacks on, the infrastructures while we deal with these larger questions of how we organize ourselves as a society to confront the problem in the long term. It has been pointed out already in your hearings, and certainly here this morning, that there is no one agency right now with responsibility for the protection of our critical infrastructures. We have many. In fact, we found approximately 22 different government agencies of commissions or task forces who have some piece of the pie, some element of responsibility, or who have been tasked with studying the problem.

We are really going to have to think in new and different ways to organize ourselves to deal with this problem, and it will take a year. I think a year is ambitious, in fact, as a period of time to arrive at an appropriate solution. But we are all uncomfortable leaving things in their current state for that period of time. So the Executive Order creates an interim Infrastructure Protection Task Force at the Department of Justice, the purpose of which is to prevent or respond to an attact on an infrastructure that may occur during the period of time in which the Commission is doing its work and the period thereafter in which the Commission's recommendations are being put into place. The Task Force will be chaired by the FBI, and it will include

The Task Force will be chaired by the FBI, and it will include representatives from other agencies, including the Department of Defense. Its obligation will be to fuse all information coming from across the government on potential physical and cyber attacks and to do what we can in the interim to respond to potential threats.

I think it would be useful for me to provide some of the background on the work that led to the Executive Order. It starts with Presidential Decision Directive 39 which the President signed in the aftermath of the bombing in Oklahoma City. PDD 39 is classified, but in an unclassified portion, the President directed the Attorney General to chair a Cabinet committee to review the vulnerability to terrorism of critical national infrastructures and to make recommendations to the President and the appropriate Cabinet member or agency on how to protect that infrastructure.

The Attorney General convened a subgroup of relevant agency heads, and that included the Director of Central Intelligence, the Deputy Security of Defense, myself, the Deputy Assistant to the President for National Security Affairs, the Vice President's National Security Adviser, and the Director of the FBI. That group, in turn, formed a subgroup (which is the group that Senator Nunn referred to) that I chaired, the Critical Infrastructure Working Group. The Attorney General gave that group the following charges: (1) To identify the critical infrastructures and assess in broad terms the nature and the scope of the threats to those infrastructures; (2) to survey the existing mechanisms in the government for addressing threats; (3) to propose options for a full-time group, which is the Commission, to consider how we should address threats over the long term; and (4) to propose an interim structure to deal with threats and attacks until a long-term solution is in place.

After identifying the eight critical infrastructures, the next step was to consider the nature of the threats. We looked very carefully at what the threats are to our critical infrastructures. We did an informal, not a formal, threat assessment. And, of course, incidents such as the Oklahoma City bombing and the World Trade Center bombing were very prominent in our assessment of the threats to the infrastructures. But the cyber threat was an important consideration as well.

There was debate over how much time we have to address the threat. I think in our first set of discussions, the notion was that the cyber threat was maybe 10 years away. But as we began to discuss it and collect information, it became clear that the horizon is not that far off. It may be only a couple of years before we face ε very significant threat. And we already have had incidents that put us on notice of the threat that we face.

It is our view that a cyber attack can disrupt the provision of services, can disrupt our society as much or even more than a well placed bomb can.

In key infrastructures, the impact of a cyber attack is becoming increasingly apparent. Consider the recent breakdowns that we have had in the air traffic control system. They proved to be the result of an aging system, but they could just as easily have been the result of a cyber attack. This gives you a sense of our vulner ability. The same thing is true for the power outage we experienced 2 weeks ago in the northwestern part of the United States.

We have not yet experienced a cyber attack by terrorists, at leas not that we know of. But the recent case involving the electroni movement of money from Citibank accounts, accomplished by computer intrusions originating in St. Petersburg, Russia, is one example of what we see as the vulnerability.

I can go over with you a number of examples, and I am happy to do that, but in the interest of time, let me skip them and leave them for questions later.

I have many examples, in the banking industry, in the telecommunications industry, and in our emergency services infrastructure, the so-called 911 system. Our emergency alert network is very vulnerable.

Similarly, we have had attacks on the law enforcement establishment itself. We have had cyber attacks on judges, on prosecutors, and on our Marshals Service, attacks which go to the heart of the security of the American public.

The next step was to examine the sources of these threats. If you viewed this threat as coming only from possible terrorists, you might have a solution that would direct our national security community to take control of this effort. But, frankly, while physical threats have come mostly from terrorists, on the cyber side, terrorist's threats are only one potential source of attack. An electronic intrusion can be caused by purely malicious hackers. It can be the work of a negligent or disgruntled employee. It can be part of an extortion or other criminal effort. It can be part of a terrorist attack. It can be part of a clandestine espionage program. Or, in a time of an international crisis, it can be part of an attack by a hostile foreign power.

Because of the varied sources of potential attacks, it does not make sense to cabin our response to the national security arena, though that arena clearly plays a very important part in our efforts. That is why we are looking for a structure that cross-cuts our government and the private sector.

At any point, Mr. Chairman, please let me know if you would like me to pause or stop and turn the podium over to you?

Senator COHEN. I think this might be a good point for us to break, and as soon as the two votes are completed, we will resume. Ms. GORELICK. That is fine.

Senator COHEN. Thank you very much, Ms. Gorelick. Ms. GORELICK. Thank you.

[Recess.]

Senator NUNN [Presiding]. The Subcommittee will come to order. I believe that Ms. Gorelick was just ending up her statement but, since we are rushed for time, if you would like to capsule toward the end of it, and summarize whatever other points of emphasis you would like to make, so we will make sure we have some continuity here. Then we will turn to Mr. White. After you capsule it, though, I would ask for Senator Levin to be recognized for a few minutes.

Ms. GORELICK. Thank you, Mr. Chairman.

I would like to take a little bit of time to give you some examples of cyber incidents that we have been dealing with, so you get a sense of the complexity of the problem, why I think we are ultimately going to end up with some hybrid structure to deal with this, and why we need a commission that brings everyone together—private sector, public sector, and across-the-board within each sector.

I mentioned the Citibank example. In the middle of 1994, approximately 40 wire transfers were attempted from Citibank's cash management system through the use of a computer and phone lines in St. Petersburg, Russia. They compromised passwords and user identification codes.

Citibank was successful in blocking most of the transfers or recovering them from recipient banks and, thus, limited any loss. But, you can imagine what the impact might have been if the intruders were not intent upon stealing funds but on bringing down the entire system or zeroing out the records of thousands of accounts.

Another example involves the telecommunications infrastructure. In 1989 a group of hackers, called the Legion of Doom, in Atlanta remotely accessed the administrative computers of Bell South and actually wiretapped calls and altered phone services. Again, the potential for harm was even greater because the group could have shut down the whole system.

Another example involves the emergency services infrastructure. In 1992, a computer intruder was arrested for tampering with the 911 system in Virginia, Maryland and New Jersey, in order to bring down the system. Imagine, again, the havoc that could be wreaked by such an intruder.

That same year, a fired employee of an emergency alert network hacked into the company's computers and caused them to crash for 10 hours. In that time, there was an emergency at an oil refinery. And the disabled system was unable to alert thousands of residents to a noxious release from the refinery. Beyond that, the computer crash potentially jeopardized hundreds of thousands of people in 22 States and six areas in Canada where that emergency system operated.

We've had similar problems in our law enforcement operations. I mentioned this briefly earlier. A man in California gained control of computers running local telephone switches. He discovered U.S. Government wiretaps in the foreign intelligence area. He also uncovered a criminal wiretap, and disclosed it. Now, imagine what could be done to law enforcement and the national security if by tapping into our phone systems, someone such as a drug cartel or a foreign intelligence service could systematically monitor or disrupt sensitive government investigations.

We also had a computer hacker disrupt the U.S. Marshals Service computer, finding locations of individual Federal prisoners.

So, that is the range of threats we are looking at. As I mentioned earlier, when we first started getting briefed into this issue the horizon seemed to be about 10 years away. We now think it is less than that, and this urgency has made us want to move very quickly and set very tight timetables for the Commission.

Senator NUNN. It sounds like to me you are describing a present threat, not a future threat.

Ms. GORELICK. There is a present threat. And it does not take much to extrapolate from the present threat to see the future threat. We have not yet had a terrorist cyber attack on the infrastructure. But I think that that is just a matter of time. We do not want to wait for the cyber equivalent of Pearl Harbor, before we wake up to the threat and take steps to confront it.

We are sounding the wake-up call now and we are trying very hard to ensure that we have structures in place, policies in place, laws in place, and relationships with industry in place to prevent such an attack and to deal with one if it occurs.

That is the effort that bore fruit yesterday in the President's announcement. I mentioned earlier that we see the threats coming not just from possible terrorists, but also from sources such as disgruntled insiders, malicious hackers, and other criminal organizations. Therefore, this is not just a national security issue, but it is also a law enforcement issue and, as Senator Leahy pointed out, an economic issue.

So we believe that you cannot just look at this from the point of view of the Defense Department and national security. For a long time, our colleagues in the Defense Department had looked at this issue and called it "defensive information warfare." But, as Dr. White will testify at much greater length, the military side of this problem is really two-fold. On the one hand, it involves attacks on DOD's own computer and communications sysyems. That part is addressed right now by the Defense Information Systems Agency. On the other hand, though, it also involves attacks on the very vulnerable civilian platform that DOD, as well as our civilian society, depends on. That is, DOD, like the rest of our society, relies on civilian infrastructures or in carrying out its essential mission. But there is no agency responsible for handling threats to that civilian platform.

Now, this leads us to the conclusion that we need a structure that brings Defense, Justice, and the individual departments, such as Transportation and Energy, that are responsible for particular infrastructures, to the table to consider how we tackle this issue.

And critically, industry has to be there for two extremely important reasons. One, they own the infrastructures. If they do not participate in the development of policy and in the subsequent steps to harden those infrastructures, it will not get done. Two, a huge amount of the expertise is in the private sector.

I liken the process we are starting to the Manhattan Project. And I think the same level of urgency and the same public/private partnership is in order here. Because without combining the best brains in our society, the best technology, the best in private effort and public effort, we will not meet this challenge. And I think this issue requires that level of seriousness and that level of joint effort.

Senator NUNN. That means making it an all-out top priority of the U.S. Government?

Ms. GORELICK. Yes. It is certainly a top priority for me, and I know it is for Dr. White. And it is certainly priority for the Attorney General. And with the President's decision yesterday, you can see that the Administration, as a whole, views it in that way, too

But I think that hearings like this one, and raising the level of consciousness within the public at large are very important. Because if we don't raise awareness, the inertia—particularly in the private sector, which, I think, believes that it can take care of these issues on its own—will prevail.

We need to make sure that the various sectors of our society start to develop a common view of the potential threat so that there is a sense of a common need to address this issue.

Senator NUNN. It seems to me the difference between this and the Manhattan Project—and I agree with you on the importance of it, I think that is a very good analogy—but the difference is this has got to be done with a lot of education. It can't be done by a few brilliant scientists behind closed doors, locked off in the desert somewhere. It's got to be done with people understanding and working together, public and private, and it's got to be an educational campaign.

Ms. GORELICK. Well, I completely agree with that and I think that right now everyone in the Executive Branch agrees with that. There was a time when the public discussion of these issues was very much discouraged for fear of encouraging people to develop the mechanisms for attack. And that is no small problem.

On the other hand, I don't think you can deal with this issue without talking about it in the broader sense.

Senator NUNN. That's exactly the conclusion I came to before starting these hearings and had to decide how much of it was going to be new information that was going to be available to people that might not have thought of it.

And I came to the conclusion after looking at what is already on the Internet—

Ms. GORELICK. Yes.

Senator NUNN [continuing]. That the only people that don't know about it are those people in government and the private sector's top echelon that must know about it in order to get the gears in motion.

Ms. GORELICK. Well, that's why I began my statement, Senator Nunn, commending the leadership of this Committee for having these hearings, because I think they're very, very important. I think the other factor that needs to be borne in mind is that while few people question the government's responsibility at some level for protecting the physical plant of our infrastructure—such as defense bases, dams, and power grids—the notion of government involvement in cyberspace evokes fears of its infringing on privacy or free speech rights, hampering economic competitiveness, and stifling creativity. And, yet, because the security and reliability of information in our communications systems are central to the continued operation of our infrastructures and to our economic wellbeing, we have to take some responsibility at the government level for setting national policy.

Somehow we have to get over this mistrust of government's operating in this arena. Solving the problem cannot be done by the private sector alone and it cannot be done by government alone. That is why we took the rather unorthodox approach to this Commission of naming a Chair from the private sector and having very strong and active private sector involvement in every element of the Commission's work.

I do want to say that we are not without expertise in government. Both the Defense Department and the Justice Department have so-called key asset protection programs. We have been identifying critical nodes, critical elements of our infrastructure, communicating with them to make sure that we know what they can do, what they need from us to make sure we have a system of warnings, etc.

Similarly, there are centers of excellence within the government, such as the National Security Agency, the Defense Information Systems Agency, the National Communications System, our own Computer Analysis and Response Team within the FBI, the Department of Justice Computer Crimes Unit, and the Commerce Department's National Institute of Standards and Technology. We have pockets of expertise. But no one element of our government has the responsibility to ensure the hardening of our national infrastructure, to make sure that resources are marshalled to do the job.

And there is a similar lack of coordination within the private sector. A notable exception is the National Security Telecommunications Advisory Committee, which has worked to establish a national policy for the telecommunications industry with the goal of securing that important infrastructure. We need to have a similar structure for every one of the eight critical infrastructures.

The Computer Emergency Response Team at Carnegie-Mellon University, which was referred to this morning, has done an admirable job in responding to cyber attacks, but does not have responsibility, nor can it, for preventing attacks or for restoring service in the event of an attack.

So, we believe that you have to establish a mechanism to develop policy, coordinate activities within the government, and develop a strong partnership with the private sector. It has to operate at a very high level. The Commission needs to be full-time and it needs to have all of the relevant parts of government and the private sector represented.

We have to take advantage of the technological expertise in the private sector. We have to encourage the private sector to work with us.

Let me close by returning to the Manhattan Project analogy. We need a cooperative venture. And I accept, heartily, your amendment of that analogy to say that we need to bring a great deal of public discussion to bear.

Let me say one word about what we do in the interim and then let me turn to my colleague, John White.

To be effective, this Commission is going to need a year to bring together all of the thinking that has already been done in this country in a cohesive manner. But we are vulnerable to attacks right now.

And, so, as part of the Executive Order, the President has established the Infrastructure Protection Task Force at the Department of Justice, chaired by the FBI, to coordinate existing resources from all over the government to help prevent, halt, or confine an attack; to help recover and restore service; to issue threat warnings; to train State and local law enforcement and industry personnel; and to coordinate with pertinent State and local authorities during or after an attack.

The idea is for the Task Force to be up and running for approximately 18 months and then to terminate its work as the Commission's efforts bear fruit.

We are going to go about that effort immediately. We have already begun, even in advance of the Executive Order signing, to ensure that our interim efforts are as effective as can be within the current governmental structure.

In closing, let me say this: There are skeptics who have said that we have to have the cyber equivalent of a Pearl Harbor to wake us up as a Nation to this threat. I think that the Executive Order, these hearings, and the discussions we have been having over the last few months disprove that pessimistic view. The difficult part of this challenge-devising a solution-remains, but I look forward to working with the Members of this Subcommittee, with other Senators and Representatives, with my colleagues in other parts of the Executive Branch, and with the private sector to meet that challenge. That concludes my prepared remarks. Senator NUNN. Thank you, Ms. Gorelick.

Senator Levin, let me call on you for any opening statement you would like to make and then we will go to Dr. White.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you, Mr. Chairman.

I will be very, very brief, because I want to put my entire statement in the record, but I want to just, first of all, commend Senator Nunn for really his visionary leadership in this area. He has taken over a very, very complex subject. He has brought it to the forefront. He has basically insisted that it be dealt with. It has already led to some very important steps. And I want to just take a mo-ment to thank you, Senator Nunn, for the extraordinary leadership which you have had in this area and taken in this area.

The other thing I wanted to do is just quickly make one point and that is that part of the problem, it seems to me, is that we have conflicting goals. We say that we want to secure our computer data to protect our national security and that is one very important goal. Encryption, for instance, is one way of helping to secure that data.

On the other hand, law enforcement wants access to data, they don't want it so secure that they, under certain circumstances with court orders, for instance, can't have access to it. They don't want the bad guys' data encrypted so much that they can't, even with a court order, get to it.

And it seems to me there's a real problem here that is—I don't think there's an easy solution to it but it's—not just a matter, at least for novices like me, of saying find a way, for instance, where encryption would help to secure it, of coming up with better encryption systems. We have better encryption systems. We have a 56-bit encryption system which hasn't been implemented everywhere, for one reason the technology can't be exported. I don't think our own government uses a 56-bit encryption system.

We have that conflict of goals. The law enforcement community wants to be able to access the very material which a very strong encryption system would defend against such access. So, we are torn, it seems to me, between those conflicting goals.

That's just one of the dozens of complications which these hearings have pointed out. I know Senator Leahy has addressed this issue in some detail, but I just wanted to say that, for the record, I will be submitting questions to our witnesses here today no particularly that encryption issue and that conflict and what the possible resolution is.

Because we can do great work to protect our systems and run into opposition from our own people who want the very access which advanced encryption would deny them. And it's something which, I think, we're going to have to resolve.

Again, I want to thank you, Mr. Chairman, just for your extraordinary effort.

Senator NUNN. Thank you very much, Senator Levin. You have been a partner in this all the way and I appreciate very much your leadership.

Dr. White.

TESTIMONY OF JOHN P. WHITE,¹ DEPUTY SECRETARY, U.S. DEPARTMENT OF DEFENSE

Mr. WHITE. Thank you, Mr. Chairman.

With your permission, I would like to submit my statement for the record and give you a brief summary.

Senator NUNN. Without objection, your entire statement will be made a part of the record.

Mr. WHITE. Thank you. I want to thank you for the opportunity to be here and I want to thank you and your colleagues for what you are doing on this Subcommittee. I think it is critically important in terms of putting a focus on this very important issue.

Senator NUNN. Dr. White, I know you had to change some plans in order to be here and we appreciate that very much, because you have really been a leader in this area and I've heard you on a number of occasions address this subject. So, thank you for being here and we appreciate your rearranging your schedule.

Mr. WHITE. Thank you, Mr. Chairman, it is very important.

I also want to commend you, personally. You described earlier how you had asked a question of the Director of Central Intelligence which made him turn white. I've been trying to do that for over 20 years, Mr. Chairman, and have never succeeded. [Laughter.]

So, I'm truly impressed.

¹The prepared statement of Mr. White appears on page 408.

Senator NUNN. I might ask him the same question again sometime, because I don't think he will remember the answer. [Laughter.]

Mr. WHITE. As you know, the Department of Defense is dependent on a broad range of interconnected infrastructures including telecommunications, electrical power systems, gas and oil distribution systems, transportation systems and others.

These systems are common to all modern societies and the connectivities and interdependencies are both complex and difficult to assess. Hence, there is the potential for vulnerability and threats, and we do not fully understand the character or the magnitude of these so-called cyber-intrusion threats.

Your Subcommittee has focused on cyber security and let me address this from the DOD's point of view. This is a topic to which I devote a significant amount of my own time. First of all, it is very important to the Department of Defense. Second, it represents an area where the technology is moving very quickly and our own introduction of new technology is going at a very rapid rate.

Third, it is not directly under our control. Much of what we purchase comes off the shelf in the commercial area and that's increasingly going to be the case. So, we do not have control over this from our own point of view.

And finally, and perhaps most importantly, the Department of Defense has not yet institutionalized the character of this phenomenal change in technology. So, we haven't yet created the culture that we need from which will evolve the approaches and the techniques that are necessary to solve the problems that are before us.

So, in my view, this does take long-term leadership from senior people from the government such as you, Mr. Chairman, such as the Deputy Attorney General, and others who have come together under the Executive Order which the President signed yesterday.

Let me make two general observations. First of all, this is not a problem that we will solve. This is a dynamic situation that we will continue to try to get ahead of and to resolve but not fundamentally solve. Second, we are not alone. All advanced societies are dependent on these systems and, therefore, this is a global problem.

Let me now turn to the most obvious and most immediate concern from where I sit and that is our military capabilities on the battlefield. As you know, we are devoted to battlefield and situational awareness. That requires us to have a whole set of very complex systems in order to strive for battlefield dominance. We have worked hard to protect those systems and we think, to a very large extent, we have been successful.

Where we have not been nearly as successful, in my judgment, is on the general information and information services front. There, there are tremendous innovations in micro-electronics, computing software and communications. And this technology is put together into a global infrastructure which is affordable by practically anybody who can buy a PC. Unfortunately, the emphasis on innovation is not matched by the emphasis on security and protection.

Herein lies a dilemma for the Department. We are trying to employ the approaches in our unclassified systems now that capitalize on the security that we have expertise in with respect to our classified systems when we are working with industry as our partner to try to do that.

We are aware of the vulnerabilities and the degree of threat which is posed to the Department and we have a number of initiatives underway to deal with those threats. For example, the effective use of existing security tools when we rely on the public switch and Internet, encryption for information, more effective firewalls, security architectures, monitoring and auditing systems that are already in place, so we know when they are being penetrated.

We believe that the recommendations contained in both your staff's and the recent GAO reports appropriately emphasize the more comprehensive and integrated approach that must be employed within the Department of Defense, as well as by others.

We agree with the GAO with respect to the fact that system security is not uniformly and comprensively addressed adequately department-wide. As a long-term effort, consistent with these recommendations, DOD Directive 5200.28, Security Requirements for Automated Information Systems, will be upgraded with increased attention on unclassified systems.

In addition, each of the services is increasing their training and awareness efforts. And I am directing a thorough defense-wide assessment of the adequacy of those efforts, especially in view of the increased threat and dependency on commercial systems.

More broadly these technologies reflect major changes in the way the DOD functions and, therefore, as I mentioned earlier, we have to work harder to institutionalize the reality of these fundamental changes.

Another initiative we have undertaken, and has been discussed with you by the Director of the Central Intelligence, is our joint effort with respect to the joint defense and intelligence community information warfare technical center, which I think again will add more capability to our efforts in this regard.

In our most recent defense planning guidance, issued in April, I task the Department of Defense components to develop capabilities to assess and mitigate vulnerability of our information infrastructure and supporting infrastructures, such as power and transportation, to information warfare and traditional threats.

But even if we are to adequately defend the DOD's critical systems infrastructures we, of course, are supported by a whole set of other complex, interrelated systems in a so-called "system of systems" which relies on commercial support.

And because of the dependence on infrastructure and technologies that are not in our control, we have to work hard to get a partnership to together with the private sector. In that process, we are emphasizing incentives which will help us encourage the private sector to work with us on these vulnerabilities.

Now, Senator Levin mentioned encryption as one of these areas and the Vice President announced our major initiative the other day with respect to encryption policy which is a very important element of this total issue, and one in which we think we have a balanced program which meets the needs of national security and law enforcement but recognizes the very important equities of American business. The Executive Branch is focusing on these broader concerns and several key initiatives and I won't repeat them because they have been well articulated by my colleague this morning.

So, in conclusion, let me say that while we are working hard on information assurance, cyberspace has no geographic boundaries and provides us all with new problems and challenges. It blurs the traditional concepts of sanctuary and jurisdiction and we need to assess what changes in policy, strategy, culture and incentives with industry that will be necessary to deal with these dimensions and concerns.

Within the Department of Defense there has been substantial progress in constructing the information infrastructure, architecture and common operating environments for our critical command and control functions. We intend now, and must expand these concepts and apply them more to our combat support system. This is a long-term effort. There is no going back. I'm confident that with collective cooperation and collaboration with other agencies in the government and with industry we can make significant progress and increase our assurance against these vulnerabilities.

Thank you, Mr. Chairman.

Senator NUNN. Thank you, Dr. White.

This is a little off the subject, but let me ask you while I'm thinking about it, because it has occurred to me two or three times. In this age of technology we are in now, with the expertise you have to develop in this area throughout the systems in the Department of Defense, in almost every facet you need computer experts. Have you all started looking at whether the up or out policy really makes sense in this age we're in now?

To me, I think a strong case can be made that that whole policy needs another look.

Mr. WHITE. Now, that's a good question, Mr. Chairman, and I have not looked at it in that regard, but I will.

Senator NUNN. I know you're a manpower expert in your background because that's where you and I first met.

Mr. WHITE. Yes, that's right. I will look at that. I will tell you though that in the other dimension I have looked at the issue of the services and making sure they have military occupational specialties and career fields which will nurture people in these categories, and what they are doing.

And, as you know, that also is critically important if we are going to have success in the long term.

Senator NUNN. Yes. I would suggest that you all start taking a longer term look at personnel in the age of technology because to have someone who gets to be a colonel and has a tremendous expertise in these areas and he's not selected for a general officer, and he's out, after 20 or 25 years, and you start all over trying to train someone, it just seems like there are whole areas of specialties here that need to have a careful re-look.

Mr. WHITE. I understand.

Senator NUNN. How will the approach that has been outlined today—and I will direct most of these questions to both of you and let you choose who is going to answer them, or both of you can answer them—how will this approach allow us to have a coordinated response? Ms. GORELICK. I think it's the only approach that will allow us to have a coordinated response. I think the burden of my opening testimony, Senator Nunn, was that without a cross-cutting commission to look at this, we are not going to have all of the different perspectives brought to bear.

Ultimately, it is my view that you will have to have some sort of hybrid agency to take responsibility for this. But there may be other approaches that would work as well. The bottom line is you have to have a coordinated response. We need the best concrete thinking about how to get there.

Senator NUNN. To what extent will the interim center have an operational capability? If some kind of charge comes in or allegation of misuse whether it is law enforcement or defense-wise, what's going to be the operational capability of this new group?

Ms. GORELICK. The FBI has operational responsibilities and authorities right now, but they're limited. And they involve hand-offs to the Federal Emergency Management Agency. There are elements of the problem that are much more in the purview of the Defense Department. What we are undertaking to do is to use every authority that we currently have to issue threat warnings, to train, to make sure that we know as much as we can about the critical infrastructures and that we work together with industry to prevent an attack and to be engaged in whatever steps are open to us in preventing further harm.

But I don't want to overstate our current readiness to deal with such a threat.

Senator NUNN. Let's give you an example here and see how this interim capability is going to work. If there is a utility company that has a power grid that's taken out by cyber attack and that closes down a whole segment of the United States to electricity let's say it's in the middle of the winter, so it's a time urgent situation—who is the lead agency? Do you assume this attack is coming from a domestic or a foreign source, and is the FBI the lead agency, is DOD? Are they going to work together to a certain point until they can determine where the attack is originating from?

How is that going to work?

Ms. GORELICK. First let me say that it is very difficult to know what the origin of a system failure is. Even if you can tell that there's been an attack, it is very difficult to determine what the origin of the attack is. And so—

Senator NUNN. You don't know the origin until you've solved the case, do you?

Ms. GORELICK. That's right. And, so at the beginning we are going to operate on both assumptions: That is, that there is a potential criminal case and that there is a threat to our national security. And we will investigate from the very beginning.

The purpose of giving authority to the FBI is, indeed, to give it lead agency status. That does not divest the Defense Department of its responsibilities, and it will not divest the Energy Department of its responsibilities in the example that you gave. We will serve a coordinating function and bring all the agencies together in one place to become operational.

An example would be the loss of power in the northwest sector of the United States just a few days ago. We did not know what the origin of that was. The FBI was, as we like to say, "on the case" at the get-go. We reached out to Defense, we reached out to Energy, and we looked to see what we could find out about the origins of that event.

We believe that there was no malfeasor in that instance and we tried to determine that even overnight. But we served a coordinating function.

We do not have our hands on the levers of switches that allow us to stop the damage from spreading. Ideally, after the Commission does its work, this country will be in that position where it has someone who is firmly in control and does have its hand on those levers. We are not there now.

Senator NUNN. Well, let's assume that this attack is from a disgruntled employee who has been fired and they knew enough about the computer system to, from an outside source, take down the system and the power grid is out and everybody is really, of course, justifiably upset about it.

And let's assume you don't know whether the attack came from England or whether it came from Africa or where it came from on the globe, but you have got to do something about it. Now, at that stage, the FBI clearly would have jurisdiction.

Ms. GORELICK. Yes.

Senator NUNN. What about the FBI and this coordinating group using DOD/NSA when the origin of the attack is domestic?

Ms. GORELICK. If you're asking the question whether we have the legal authority to utilize the resources of our intelligence community, in particular, in that instance, the answer is probably yes. Senator NUNN. Where do you get that authority from?

Ms. GORELICK. We have authority right now to ask for assistance where we think that there might be a threat to the national security from a foreign source. If we know for certain that this is a purely criminal threat, with no national security or foreign intelligence connection, the authority is much more questionable. And that is why we have, in Section 715 of the defense authorization bill, specific authority to task the intelligence community to gather information about non-U.S. persons, abroad, in aid of law enforcement.

Senator NUNN. So, you have enough authority right now to assign Defense and NSA to that even though it turns out, you don't know at the time, but it may turn out to be a domestic attack?

Ms. GORELICK. Where we think that there is a threat to the national security from a foreign power or agent of a foreign power I think we have the ability to task. Where we know it is a purely domestic law enforcement matter, we do not.

Senator NUNN. What if that attack originated in Boston but the attacker has gone through seven foreign countries, and so forth, before he turns around and seizes a computer here and knocks it out?

Ms. GORELICK. We have recognized some jurisdictional limitations on our authority to prosecute cases involving computer crime and that is why we have proposed amendments to the computer laws to expand our jurisdiction.

But, bear in mind, we would have to engage with our foreign partners in a liaison relationship in order to thoroughly investigate. That is, if communication has gone through other countries, we are going to need help from other countries.

Senator NUNN. But right now you think you have adequate legal authority to tackle this, even if it's from a domestic source? If you don't know at the time, you have the right to unleash NSA and unleash the CIA and unleash all the other agencies of the foreign intelligence operations?

Ms. GORELICK. Where we don't know, where we think that it originates in a foreign threat to our national security, then I think we can task the intelligence community. Obviously, they cannot collect against U.S. persons or in the U.S., let's be very clear about that. They can only collect against non-U.S. persons abroad.

Senator NUNN. But this is a U.S. person carrying out the attack in my hypothetical.

Ms. GORELICK. All right, if we know what you know in the beginning of your hypothetical, if we have made that conclusion, we will not use intelligence agencies to assist in the collection of evidence.

Senator NUNN. But you may need them if it is looped through about seven foreign countries before it comes back here.

Ms. GORELICK. That's right. Right now, we will not use intelligence agencies to collect information against a U.S. person. Now, if the target of an investigation is a non-U.S. person and the information is abroad, that raises an interesting issue for us. And one of the reasons we have sought clarification in Section 715 is to ensure that Congress and the Executive Branch know when we have the authority to task intelligence agencies to act in aid of law enforcement.

Senator NUNN. I'm still not sure. Would the Attorney General have to sign off on this if the attack appeared to be coming from a domestic source but it looked like it was being routed through foreign computers? Who would sign off in order to do that?

Ms. GORELICK. We would not utilize, we could not utilize our intelligence agencies to collect against a domestic target, a U.S. person, with or without the Attorney General's, sign off.

That's our responsibility in law enforcement.

Senator NUNN. Well, does the FBI have the capability of going through seven countries then and figuring out where the origin of the attack came from?

Ms. GORELICK. We would use our resources, our liaison relationships with other countries' law enforcement.

Senator NUNN. That's a very time consuming process.

Ms. GORELICK. It is, it is.

Senator NUNN. In fact, it could take weeks and weeks while the middle of the winter has got the grid system shut down.

Ms. GORELICK. That's right. Under our current authorities, we would not collect against a U.S. person via our intelligence community. And even what we have sought in Section 715 would not allow us to task the intelligence community to collect against a U.S. person.

Senator NUNN. Does the President have a constitutional authority to override statutes where the basic security of the country is at stake? Let's say a whole part of the country is, in effect, freezing to death in the middle of the winter and you believe it is a domestic source, but you can't trace it because the FBI doesn't have the capability. What do you do?

Ms. GORELICK. Well, let me say this. One thing you could do is you could detail resources from the intelligence community to the law enforcement community. That is if you are talking about a technological capability that we need. We have done that. Where, for example, we are having trouble decrypting information in a computer and the expertise lies at the NSA, we have asked for technical assistance that would be under our control and operate under law enforcement's rules and coordinants. We could do that.

The President has, in my view, residual authority as President to authorize searches for foreign intelligence purposes that would otherwise be prohibited by the Fourth Amendment. We have tried very hard not to have the President exercise that authority. That is the kind of authority that came into question before we had a procedure to obtain the Foreign Intelligence Surveillance Act, which now provides for court orders to authorize searches for foreign intelligence purposes.

I would have to look at the specifics of your question and see if we could provide you with an answer for the record. But I do think there is residual authority in the President of the United States in foreign intelligence cases. And I would like to see—assuming that we cannot obtain the help we need by detailing intelligence personnel or resources to us, under law enforcement control—whether there are circumstances when you would want to use the intelligence agencies of the United States to help in a case involving, at its best, a U.S. person operating through other countries. Right now, we do not do that.

Senator NUNN. That really poses a tough question. I could give you a hypothetical of a company calling up and saying we got a grid down, and we are really in bad shape. People are going to be suffering within hours. We think it's a disgruntled employee who wrote a threatening note. He was fired 2 months ago. We don't know where he's located. Our initial indications are though that it's coming from this country.

And, yet, you get into it in an initial stage and all of a sudden it unfolds coming from elsewhere. You suspect, your strong basic prima facie evidence from the company is that it is a domestic source, but the routing has taken it all over the globe. We've already seen that. That's not a future threat. I mean that's the kind of threat we've already had.

So, your strong assumption is that it is a domestic source based on the information you have and, yet, it's going through six or seven foreign countries. At that stage, your domestic law enforcement probably doesn't have the capability to deal with it, based on my knowledge of their technological capabilities, and your foreign countries might take weeks, if not months, to be able to put into effect all of their systems and have an adequate coordination, even if it occurs at all, and in the meantime, folks are freezing to death.

That's a tough one, it seems to me, but that's not far from present threat situations.

Ms. GORELICK. Well, it is a tough one. I'm reminded of the analog right after Oklahoma City, where we did not know whether the threat was domestic or foreign. And we used all of our resources. The difference between the two is, once we determined that the threat was domestic, frankly, there wasn't a huge need to pursue, in a real time basis, any leads against those U.S. persons abroad. Now, we can collect information, we just can't collect information on, or surveil, a U.S. person.

And so, there may be things that we could do short of collecting on the U.S. person that would be of tremendous help. But, Senator Nunn, what you've got here is you have focused on two very, very important points. The first is that we are really redefining, and we have been for the last 10 years, the nature of threats to our national security.

During the Cold War, I think we knew what the threats were to our national security. Right now, those definitions are changing very, very rapidly, as we construe, first, terrorism, and then international narcotics trafficking, as threats to our national security. Those are areas in which the intelligence agencies of the United States can operate.

As you move closer and closer, however, to considering threats to our national security from U.S. persons, you get closer and closer to the fairly strong and firm line that this country has drawn between law enforcement and intelligence. Domestic law enforcement, which is covered by the Fourth Amendment, can intrude upon the privacy of U.S. citizens only with a warrant and with the imprimatur of a Federal court. But in some cases, law enforcement may need assistance from our intelligence community, which operates without all of those legal constraints.

We have drawn that line between the intelligence and law enforcement communities in order to protect the American people from unwarranted intrusions. And I spend a lot of my time and energy trying to make sure that the rights of the American people are protected, that the Fourth Amendment is strongly and firmly in place in protecting individuals against unwarranted intrusions.

I think the hypothetical you raise probably presents the most difficult of those choices for us, and I think it is worthy of additional dialogue between us.

Senator NUNN. I think it's going to take a lot of thought on that subject.

Dr. White, another scenario. You have got the Iraqis threatening the Kuwaiti border and you believe they are really coming again. And you start getting up your force deployment plans and you're trying to send various units all over the world to various places, a lot of this on the open lines.

Then, all of a sudden, your orders get switched. You have got naval forces going in the wrong direction. Army forces going in the wrong direction. People going in the wrong direction all over the world and you know somebody has gotten into your computers. It looks like it's a domestic source. There is a computer that you detect that is doing some of this but, in reality—you don't know this—but in reality it's coming from abroad after having seized a domestic computer.

Under this operational plan that you basically have, who is going to have jurisdiction over that? What do you do?

Mr. WHITE. I'm not sure. As you say, Mr. Chairman, if it is, in fact, interrupting national security our obvious focus was to ini-

tially look elsewhere and see whether or not there are vulnerabilities elsewhere in this hypothetical case. If they are domestic, I think we're back in the same dilemma that was mentioned in your prior hypothetical situation. We have to turn to domestic law enforcement agencies.

Senator NUNN. It seems to me that this operational group, in addition to being formed, is going to have to be given some hypotheticals here. Because the hypotheticals will become reality. I mean you look at what's already happened out there, at some point this could happen. I think you are going to have to do a lot of thinking about how far they can go before they're sure. And this gets into all the considerations you mentioned with the Fourth Amendment being very important.

And this is part of why this commission, and I think all of us involved in this area, are going to have to have education because this is the kind of thing that all of us are going to have to think through together, not just government but private sector and individual citizens out there, also.

Mr. WHITE. Let me say also, Mr. Chairman, we've been running some games in this regard where we have included law enforcement people and private sector experts where we pose these kinds of situations where there are threats to the air traffic control system, conflicts going on overseas. We don't know whether that threat is directly coming from the overseas conflict and so on.

Senator NUNN. That's good. That's been very helpful to us.

Will placing your proposed interim response center under the auspices of the FBI tilt its focus too much in the direction of law enforcement response at the expense of intelligence gathering?

Ms. GORELICK. I don't think so. We really didn't have much of a choice though. Because we cannot and should not provide information on U.S. persons to the intelligence community. The same considerations that I talked about a little while ago, involving the important protections of the Fourth Amendment and the desire to have the intelligence gathering process stay separate from U.S. law enforcement, suggests that while we may take information from the intelligence community, it should not take information about U.S. persons from law enforcement.

And, therefore, you really do need to put it with the FBI. The other reason for vesting this responsibility in the FBI—supported as part of the Task Force by the Defense Department, particularly the NSA, by the intelligence community, and by the National Security Council—is that, as you pointed out, at the outset of an event you don't know whether it is a foreign threat or a domestic threat In such a case, I think you need to investigate it as though it were a domestic threat, consistent with the rules applicable to domestic criminal investigations.

The Justice Department—in particular, the FBI—is an agency that has both national security and law enforcement functions. And the FBI's Computer Investigations and Threat Assessment Center, the so-called CITAC, merges personnel and resources from both Division 5 and Division 6, which have criminal justice and national security responsibilities. So, we think we can handle this interim responsibility. Again, though, it is only an interim solution because it is not ideal. But it is the best that we could do under the circumstances. We did consider placing interim responsibility with the Defense Information Systems Agency. We also considered placing it with FEMA. We looked all around.

And we thought the FBI was the best choice.

Senator NUNN. Now, will the FBI have clear directions as to when they should pursue a matter as a law enforcement matter and when they should forget law enforcement and who is going to be prosecuted and see if they can't get the grid going so people don't freeze to death. I mean, it seems to me, that's one of the challenges here. You've got my same example, and people are about to get in real danger of their lives, you've got something really going wrong or the air control system, whatever example you want.

And the FBI is sitting there in charge of the system and they say, well, we have got to make sure we have a train of evidence so that we can put this person in court and we can withstand cross-examination and we can make sure we have read everybody their rights and gotten all the warrants. And DOD or whoever else is over here is saying, people are freezing to death, forget all that stuff.

Now, I mean what philosophy—there is a fundamental, and it is appropriate to be a fundamental different philosophy—what philosophy is going to govern in these emergency situations? And are you going to be able to capture that in terms of clear directives?

Ms. GORELICK. Well, we are not so rigid about making our cases that we forget the other important values and our other responsibilities. We have lots of analogous circumstances in which "making a case" has to take a back seat to protecting the public safety from imminent harm.

As I said, we do often have situations in which we trade off or abandon the ability to prosecute in order, for example, to further penetrate a spy ring in order to limit damage to the national security of the United States. We regularly have to make decisions involving those trade-offs between making a case and other interests beyond prosecution.

Similarly, when you have a crime scene like the Murrah Building, we don't say, "Please, don't go in and rescue people because it's a crime scene." In that case, we made sure everybody that we could rescue was rescued and then we sealed it off as a crime scene. So, that is—

Senator NUNN. That would be a real-time kind of situation and that's what we are dealing in here.

Ms. GORELICK. Yes.

Senator NUNN. Your time and space is so compressed that you have got to make those decisions immediately.

Ms. GORELICK. Right. Basic elements of humanity and common sense will govern this process.

Senator NUNN. In his testimony last month, CIA Director Deutch stated that the intelligence community is planning to establish a community-wide information warfare technology center to be housed at the National Security Agency which would, in his words, provide the tools to deal with the emerging cyber threat. How do you envision the relationship between the new interim group that you're talking about and this group that Director Deutch is talking about?

Ms. GORELICK. The group that Director Deutch is talking about has not really been fleshed out yet, nor has its working relationships with the interim Task Force at the FBI. But, certainly the intelligence community has a very, very important role to play in assessing potential cyber threats by using all of the myriad intelligence sources out there. And we will make sure that that is lashed up with the interim Task Force, which will, of course, be collecting information domestically and will have responsibility for fusing both the foreign intelligence and domestic information.

Senator NUNN. But those are two separate groups. They are not going to be one group merged.

Mr. WHITE. May I say a couple of words about the NSA group which is not yet formed. The Director and I have now asked General Minihan to, under our guidance, to come forward with a charter. But the emphasis is on both defense and intelligence, communities, in terms of cooperation and particularly with respect to technology.

That is, this is not an operationally oriented group. This is a technology oriented group where we will lend other technical capabilities from CIA, from DIA and other parts of the intelligence community, so we have them in one place to focus directly on the technological challenges and defensive measures with respect to cyber assurance.

Senator NUNN. Would it be fair to say at this point, as we sit here this morning, technology is now out-running our ability to organize government to deal with these kinds of threats and our legal system's ability to react to them? Is that too strong?

Ms. GORELICK. I think that that is not an inappropriate characterization. I think we are at one of those turning points with respect to technology and our legal and operational system where we need to take a completely new look at both our policies and our practices to see whether they are adequate to the emerging technology. That is the process that has taken place over the last 6 months and what we have found is that we do not have an adequate system in place.

While the threat is not overwhelming at this point, we can see enough evidence of it that we need to ensure that when the threat becomes substantial, which will be in the next couple of years, we have both policies and practices in place to deal with it.

Mr. WHITE. Mr. Chairman, I want to make a related point. Because I, like my colleague, do not disagree with your statement. During the 1980s, I was the chief executive officer of a software systems company. I think it's important that people in government understand that in much of the software community there is a culture which does not hold in high regard at all the kinds of concerns that we talk about here—people who are not only willing to hack into other people's systems, but proud that they did it and happy to share that information with their friends and colleagues.

So, we have to be aware that we are dealing with a subculture in the society that, in fact, has a different value system when it comes to these concerns. And even in the private sector when we talk to senior executives in corporations, you may see a view that appears to be consistent with your own, I would submit to you that many of their employees do not hold that view.

And it is not necessarily these people are doing anything criminal, it's a different value system. And I think that is a very important element of this puzzle that we're going to have to work on.

Senator NUNN. Does that mean that there are people out there who believe there is no such thing as privacy in the Internet world?

Mr. WHITE. Yes, sir. There are a lot of people who believe there is no such thing as privacy. There are a lot of people who think that intellectual property need not be protected. Quite the reverse, that intellectual property is not important, that it all ought to be shared and so on.

Senator NUNN. Is that philosophy at the high levels of the software industry or are you talking about random employees now?

Mr. WHITE. I'm talking largely about employees, about programmers and so on.

Senator NUNN. Is the private sector doing anything about that? Is the private sector concerned about that? Is the private sector doing something about that? Does it not make any difference to the people at the top, or is the private sector concerned about these things?

Mr. WHITE. I think the private sector is concerned about it, but generally in the private sector, in my business experience, you protect yourself against these kinds of intrusions, just as we do here, but you recognize that you have got a culture in your own institution that, in fact, is inconsistent with what you are trying to do.

I had an instance once where a computer programmer tried to crash the entire company network in order to see whether he could do it. Now, you can fire him, as I did, but he is not the only one who is there trying to do that.

Ms. GORELICK. If I might say something about this, I think that for a number of years, we have had an image of the hacker as a kid, you know, closeted upstairs with a computer, seeing what he could do.

Senator NUNN. He or she.

Ms. GORELICK. Well, actually, it is mostly young boys, but there are a couple of girls who do it.

Senator NUNN. Be careful. Be careful.

Ms. GORELICK. And I think we have as a society thought of it as sort of amusing.

When I go and talk to groups about security in cyberspace, I am often faced with, I think, a sense that I represent Big Brother and that hacking should be completely private because it is not actually terribly threatening.

It is interesting. One of the stories I tell is about a hacker who went into the phone system and arranged it so that when radio contests announced that they would reward the fourth caller or the sixth caller, he would always be the fourth caller or the sixth caller. And he won two Porsches and vacations and a lot of money in a short period of time. Usually, people laugh at that story. They think it is funny. They think it is very, very clever. But you don't have to extrapolate from that story very much to see that if you could fix the phone system to do that, you could wreck havoc. There is somewhat of a sense that what is happening out there is the harmless prank or an exercise of First Amendment activity that shouldn't be interfered with in any way.

This infuses the encryption debate as well, as Senator Levin said. Encryption is a wonderful tool for protecting us against intrusions into our private computer world, but you must also have the ability for a cop to operate on that information superhighway. I am not sure the American people, in fact, have the stomach for the level of chaos that there will be on the Internet and in our interlocked computer systems if unbreakable encryption proliferates, and law enforcement is unable to prevent or investigate acts of terrorism and other serious crimes as a result. But I am afraid that we will discover that too late.

So I think it is important that we have a bit of a dialogue about these issues. We must be mindful of the legitimate desire of people for privacy, and mindful of the tremendous advantages that interconnectedness offers all of us, but we must also be mindful that chaos is a very dangerous thing, and that if we do not have mechanisms and policies that will allow us to protect the public from intrusions that are, in fact, dangerous and have the potential for tremendous harm, we are doing ourselves a disservice.

Senator NUNN. I think you have given us a lot to think about there. That is a good answer.

Dr. White, in this private sector world that you came from last year, when people at the top, CEOs and top officials of a company, know that this is a mentality out there in their group, are they primarily focussed on protecting their own company and their own resources and really not caring whether if you use the word "hacker," the analogy being to a burglar, if the burglar goes in somebody else's windows, as long as they don't get in theirs, or does it go a step further than that? Is there a lot of sabotage going on in the private sector itself between competitors, or a lot of basically stealing of secret information, proprietary information among competitors? Give us just your general view of that.

Mr. WHITE. In general, I think most of these senior people are very concerned about it from an industry point of view because there is an enormous amount of software theft just copying, and people that work very hard in associations and collectively on standards boards and other forums to try to solve those problems for the industries. So I think people are very concerned about it, and in that regard, working together to try to solve the problem and try to turn around this culture, and they have tried to do it in companies, and some in vivid ways of going in and literally having law enforcement people arrest people for copying large numbers of software programs and so on. So I think there is an effort in that regard.

I must say to your other specific question, I am not an expert, but I in my years in the industry was not aware of companies consciously penetrating other U.S. companies trying to get special business information.

Senator NUNN. I know the whole intellectual properties area about private sector has taken a very strong stand in urging our government to crack down on foreign invasions of that privacy. It seems to me that the same philosophy would apply here. In China, for instance, there has been an all-out effort in our trade policies, including escalating up to their high level to protect the American intellectual property. It seems to me the same philosophy which is instigated by the private sector, appropriately so, would also be applicable to here at home.

Mr. WHITE. I think that is absolutely right. I think you would find the business community to be consistent on that issue, Mr Chairman.

Senator NUNN. I believe that Ms. Gorelick mentioned that we did not have a formal threat assessment, but that a lot of the basis of what you have recommended here today came from an informal threat assessment. Could both of you address or either of you address when we will have a formal threat assessment in response to the Kyl Amendment to, I believe it was, the Authorization Act last year?

Ms. GORELICK. The response to the Kyl request, I believe, is in the hands of the National Security Council. I do not know the answer to your question.

Senator NUNN. Is that on a separate track from your work? Ms. GORELICK. Yes.

Senator NUNN. Both involve threat assessment, don't they? Ms. GORELICK. Yes.

"Threat assessment" is a little bit more formal than what we had. When we got involved in this issue, we were on a very, very tight time track. We really wanted to push this fast. So we didn't wait for any written document. We asked for and got briefings at the highest level from each of the most knowledgeable elements of our intelligence and law enforcement communities as to the threat, and it was from that, collectively, that we developed our sense of what the threat was.

There have been papers written. I actually don't know their status and if they are formally considered "threat assessments." I would like to get you an answer for the record on that.

Senator NUNN. Perhaps either one of you could get back for the record and let us know when that report will be due and who is in charge of it and what the expectations of having some kind of threat assessment as well as a plan. It seems to me what you have outlined today is part of that, though. The plan certainly would include what you are doing now, wouldn't it?

Ms. GORELICK. I think, frankly, what we are doing now—the establishment of the Commission and the interim Task Force—is the plan. I don't know what else you could be doing other than giving some entity interim responsibility, and bringing everybody together in a Commission with a very specific charter and a very tight timetable to come up with solutions to these various problems.

I don't see any other plan that you could have right now. If someone has an idea, I would like to know about it.

Senator NUNN. It seems to me that maybe someone, from the President or one of his people, should submit what you submitted today as part of the answer to that because the June 10th deadline has come and gone.

Mr. WHITE. I think that is right, Mr. Chairman.

Let me also say, I think Director Deutch said in his testimony there is a national intelligence estimate which is being developed. So, from our point of view with respect to security issues on computing and computer networking, the community is providing such an estimate. That is a part of this puzzle, but obviously not the total. Senator Kyl's focus is obviously more domesticated, as our discussion here today.

Senator NUNN. In its report on the Defense Authorization Bill, Dr. White, the House Committee on National Security States, "The Department of Defense is devoting woefully insufficient resources to protect from the Department's information systems."

It went on to say, "Senior DOD leadership is reluctant to impose a solution to a nontraditional threat."

Do you agree with this assessment?

Mr. WHITE. No, sir, I don't. I think we have increased the amount of effort we are doing in this regard. Recently, we are looking for innovative ways to deal with these issues. We have a whole set of new innovations in technologies to deal with them. As I testified, we are a long way from a solution, but I think we are very much focussed on this effort.

Senator NUNN. Could you furnish for the record a general budgetary analysis of how much in the way of resources we are submitting to this area, anything you can in an unclassified form—

Mr. WHITE. Yes, sir.

Senator NUNN [continuing]. And then, if necessary, a classified section?

Mr. WHITE. Yes, sir. I will do that, Mr. Chairman.

Senator NUNN. Ms. Gorelick, in his prepared testimony last month, Director Deutch stated that obtaining computer intrusion data from U.S. banks and other institutions has been difficult. My staff found a great reluctance on the part of financial institutions to share information on intrusions. Indeed, the staff was told by some that financial institutions purposely do not report intrusions for fear of damaging consumer confidence in their institution.

First of all, do you agree with that assessment, and second, how are you approaching that?

Ms. GORELICK. I absolutely agree with that assessment. For some of the reasons that John White described, most commercial institutions strive to assure their customers that they can perform the function for which the customer has hired them or has purchased their product, and therefore, they are very reluctant to share information with us.

We know this from direct conversations with industry and from the kind of communications that our FBI Special Agents in Charge have with institutions within their jurisdictions.

One of the purposes of structuring the Commission in the way that we have is to bring on board the key elements of our National Information Infrastructure. You need to have an equivalent of the NSTAC for every critical element of our infrastructure, so that a conversation can take place within the industry and between industry and government, involving thinkers from the private sector who can consider the scope of the problem and how we can harden those infrastructures against attack.

Senator NUNN. Isn't the commission really a way of bringing into the whole picture the private sector and getting their view? Because what you have done, it seems to me, is the government's side of that already——

Ms. GORELICK. Yes.

Senator NUNN [continuing]. And what you are basically now doing is saying let us stop where we are, get the private sector involved, see what they think, and see if we can together think through solutions. Is that what the commission is all about?

Ms. GORELICK. Yes.

Mr. WHITE. And it is structured that way.

Let me also say that, while we all have noted and are disappointed to some extent in some of this private sector reaction— I know you have had the experience on the Committee—the private sector is much more forthcoming when we turn from them telling us how they specifically are vulnerable and have been embarrassed and turn to prophylactic ways that we can help them to solve their problem even though they may not specify exactly the magnitude of the problem, and there we find them much more forthcoming and obviously having a lot of good ideas.

Senator NUNN. Given the likelihood that so many cyber attacks are from other nations or at least at the initial stage it looks like they are, do we need to examine international laws and work with other nations, and if so, what is being done in that regard?

Ms. GORELICK. This is a very high priority for us, particularly in terms of the international community.

The President has, as you know, come out of the meetings in Lyon earlier in the month with a directive to us to work with the other G-7/P-8 countries to formulate a very direct and effective agenda, particularly to address terrorism. The same mechanism that you would utilize to address cyber terrorism would address other cyber threats as well. So we have placed very high on the agenda for ministerial meetings the issues of encryption and the issues of a unified, international legal approach to intrusions into the world of cyberspace.

Senator NUNN. Is the European Community as a community working this problem?

Ms. GORELICK. It certainly is. The European Union and its individual members on a bilateral basis have all been involved with us in discussions, especially about encryption. Those discussions are very much related to the issues that you have before you today.

Senator NUNN. Would you say that the other countries are as far along as we are in terms of both threat assessments and plans to deal with it? Are we out in front? Are we lagging behind other countries like Japan, the European Community, and other industrial societies, or where are we on the scale and where are they, generally speaking?

Ms. GORELICK. I think all of the countries that you mentioned, including ourselves, are muddling along at about the same rate.

I think we are all realizing at about the same time the nature of the threat and are having similar, but not identical, national debates.

It is our hope that by addressing this early with other countries who have not yet established their national legal structures, we can come to common structures. I don't think any country wants to see its own cyberspace unregulated. I don't think any country wants to see the proliferation of unbreakable encryption so that a terrorist could hide what he or she is doing, immune from the security services of that country. So this debate is coalescing around the world at about the same time.

It obviously raises all sorts of very difficult issues about the way in which you balance privacy and law enforcement and national security and economic and other needs. So we see our foreign partners struggling with the same kinds of questions that we are struggling with.

Senator NUNN. Could I ask the same question, Dr. White, on your Defense counterparts in other countries within Intelligence?

Mr. WHITE. I think in the Defense and Intelligence area, Mr. Chairman, we may be a bit ahead simply because, as you know, from the way we have approached modern warfare, we have put a very high emphasis on intelligence and highly sophisticated communications, and from that point of view, I expect we are somewhat ahead of our allies and friends.

Senator NUNN. We are certainly ahead in offensive information. Mr. WHITE. Yes, sir. I mean, in terms of the military options. Senator NUNN. Right.

I want to thank both of you for being here today, and again, Dr. White, thank you for changing your schedule, and all of your staffs who worked on this project. I know we have a long way to go, but I think it is a good beginning, and I appreciate very much you being here.

We will be working up a lot of recommendations ourselves and we will share those with you, and hopefully, vice versa.

Ms. GORELICK. Thank you, Senator Nunn.

Mr. WHITE. Thank you. Thank you very much, Mr. Chairman. Senator NUNN. Thank you.

[Whereupon, at 12:04 p.m., the Subcommittee was adjourned.]

APPENDIX



William March 100 more

Computer and Internet Security: A Brief Introduction

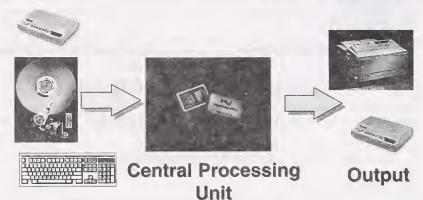
Keith A. Rhodes, Technical Assistant Director, Office of the Chief Scientist

Slide 1

Purpose

 λ To Familiarize the Audience with Computer and Internet Security Concepts and Vocabulary

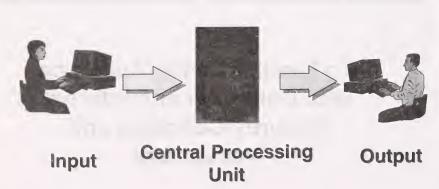
Computer System Components, 1



Input

Slide 3

Computer System Components, 2



Storage & Transmission

λ Perspective
 Assume the typical novel is
 Approximately:

60 characters per line 30 lines per page 200 pages

Equals 360,000 characters per book

Slide 5

Storage & Transmission

λ Bits & Bytes

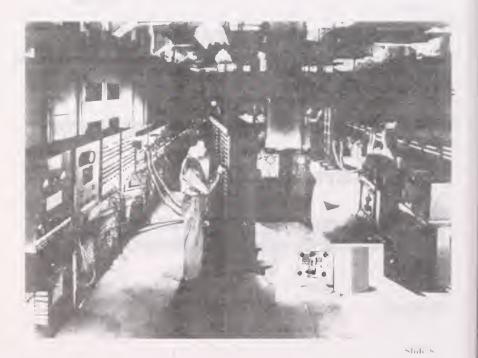
1 bit (1 or 0, On or Off, Yes or No)

- 8 bits = 1 Bytes
- 1 Bytes = 1 Character

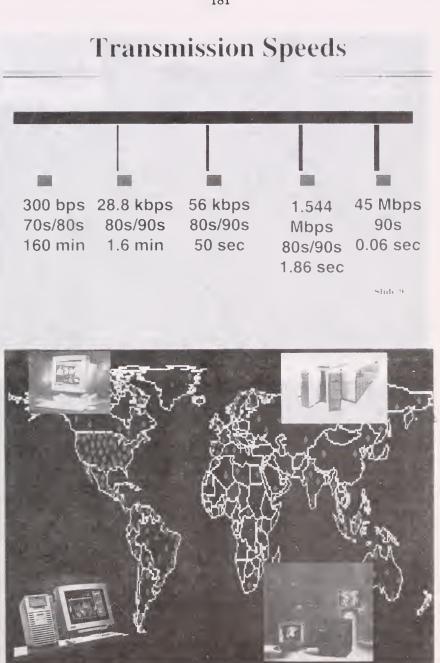
The average novel equals approx. 360,000 Bytes (360 kilobytes)

Storage & Transmission

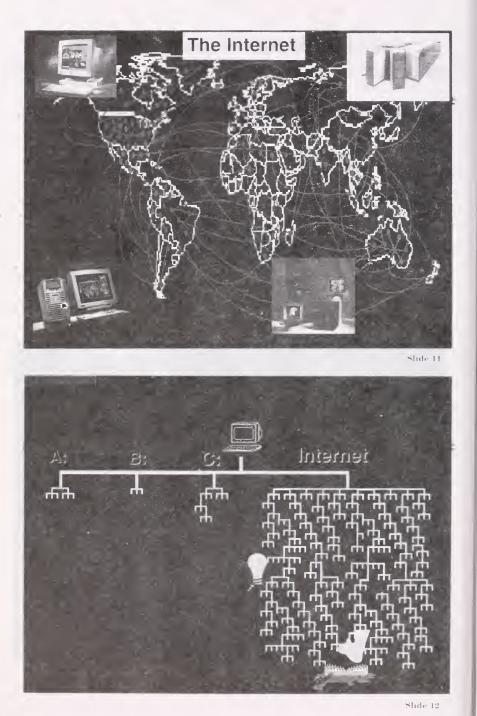
Typical Storage Capacities Memory = 16 M Characters = 44 books High Density Disquette = 1.44 M Characters = 4 books Hard Drive 1.1 G Bytes = 1.1 B characters = 3000 books CD-ROM 600 M characters = 1500 books

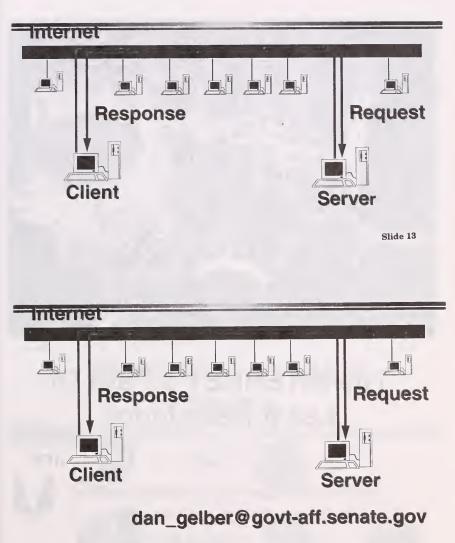


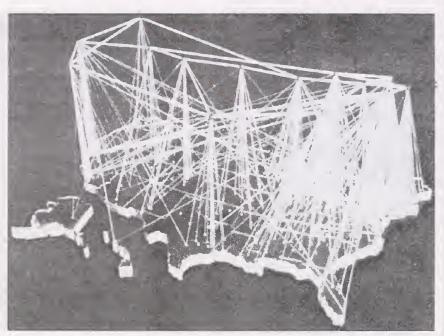
180



slide 10





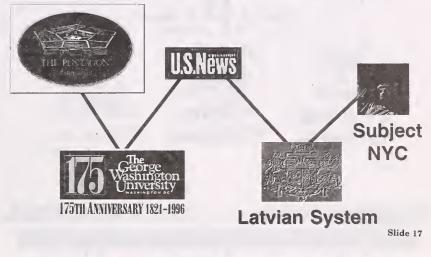


The INTERNET'S Path Of Least Resistance



Shde 16

Hackers Loop and Weave to Prevent Detection & ID



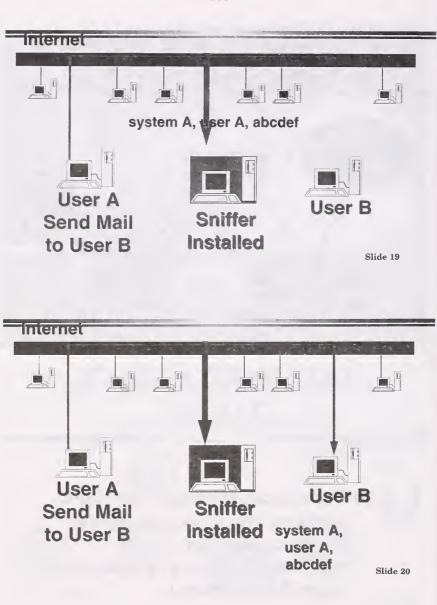
INTERNET ATTACK TOOLS

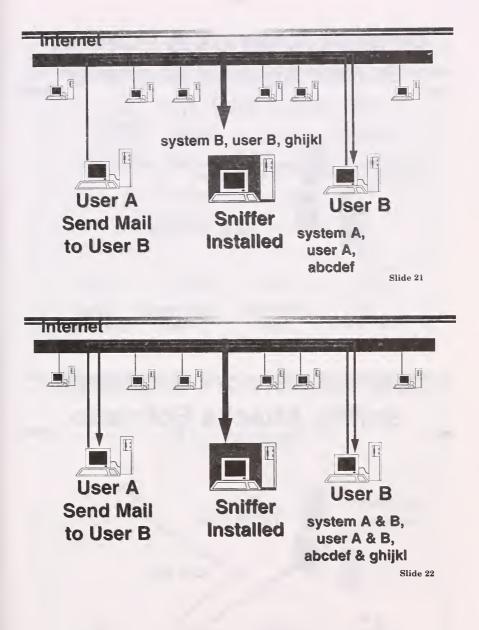
 λ Sniffer Attacks (Software Wiretaps) captures first 128 characters of each session net address logon and password hides data captured

Slide 18

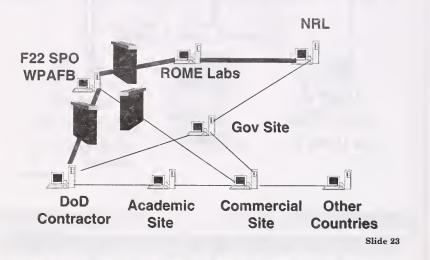
185

14 St. 18'

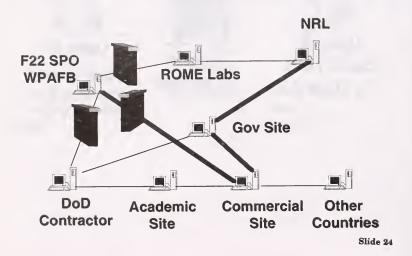




Defense Network & Internet Sniffer Attacks Scenerio



Defense Network & Internet Sniffer Attacks Scenerio

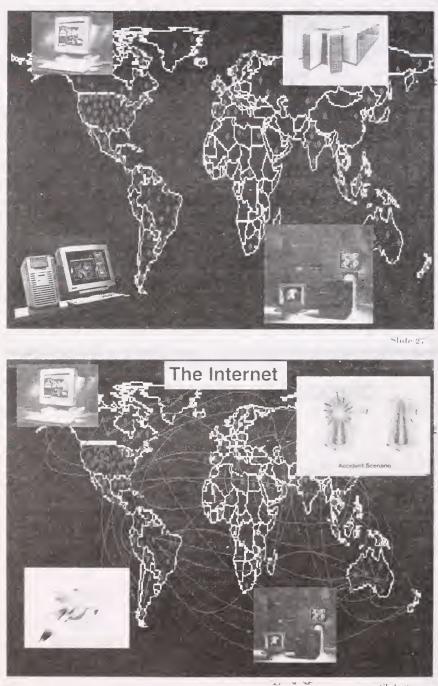


Protocols of the Internet

λ IP, TCP, UDP, ICMP, RIP, DNS, MIME, telnet, SMTP, NTP, RPC, finger, NIS, NFS, portmapper, ftp, X11, WWW, gopher, FSP

Slide 25

The Point?



A Final Thought

λ "The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it."

- Gene Spafford (attributed)

GAO

United States General Accounting Office

Testimony

Before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate

For Release on Delivery Expected at 9:30 a.m. Wednesday May 22, 1996

INFORMATION SECURITY

Computer Attacks at Department of Defense Pose Increasing Risks

Statement of Jack L. Brock, Jr., Director Defense Information and Financial Management Systems Accounting and Information Management Division



years

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks

	Mr. Chairman and Members of the Subcommittee:
	Thank you for the opportunity to participate in the Subcommittee's hearings on the security of our nation's information systems. The Ranking Minority Member and other Subcommittee members have expressed serious concerns about unauthorized access to sensitive information in computer systems at the Department of Defense and directed that we review information security at the Department. These concerns are well-founded. Defense has already experienced what it estimates to be hundreds of thousands of computer attacks originating from network connections, some of which have caused considerable damage. As you will learn from our testimony, these so-called hacker intrusions not only cost Defense tens of millions of dollars, but pose a serious threat to our national security.
Computer Security Is Difficult but Necessary	Defense, like the rest of the government and the private sector, is relying on technology to make itself more efficient. The Department is depending more and more on high-performance computers linked together in a vast collection of networks, many of which are themselves connected to the worldwide Internet. Hackers have been exploiting security weaknesses of systems connected to the Internet for years, they have more tools and techniques than ever before, and the number of attacks is growing every day. These attacks, coupled with the rapid growth and reliance on interconnected computers, have turned cyberspace into a veritable electronic frontier. The need to secure information systems has never been greater, but the task is complex and often difficult to understand.
	Information systems security is complicated not only by rapid growth in computer use and computer crime, but also by the complexity of computer networks. Most large organizations today like Defense have a conglomeration of mainframes, PCs, routers, servers, software, applications, and external connections. In addition, since absolute protection is not feasible, developing effective information systems security involves an often complicated set of trade-offs. Organizations have to consider the (1) type and sensitivity of the information to be protected, (2) vulnerabilities of the computers and networks, (3) various threats, including hackers, thieves, disgruntled employees, competitors, and in Defense's case, foreign adversaries and spies, (4) countermeasures available to combat the problem, and (5) costs.

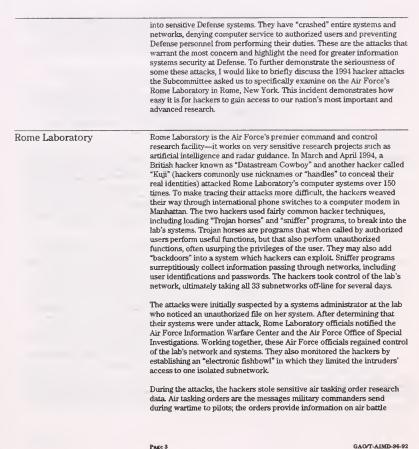
Page 1

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks
In managing security risks, organizations must decide how great the risk is to their systems and information, what they are going to do to defend themselves, and what risks they are willing to accept. In most cases, a prudent approach involves selecting an appropriate level of protection and then ensuring that any security breaches that do occur can be effectively detected and countered. This generally means that controls be established in a number of areas, including, but not limited to: • a comprehensive security program with top management commitment, sufficient resources, and clearly assigned roles and responsibilities for those responsible for the program's implementation; • clear, consistent, and up-to-date information security policies and procedures; • vulnerability assessments to identify security weaknesses; • awareness training to ensure that computer users understand the security risks associated with networked computers; • assurance that systems administrators and information security officials have sufficient time and training to do their jobs properly; • cost-effective use of technical and automated security solutions; and • a robust incident response capability to detect and react to attacks and to
aggressively track and prosecute attackers. The Department of Defense's computer systems are being attacked every day. Although Defense does not know exactly how often hackers try to break into its computers, the Defense Information Systems Agency (DISA) estimates that as many as 250,000 attacks may have occurred last year. According to DISA, the number of attacks has been increasing each year for
the past few years, and that trend is expected to continue. Equally worrisome are DISA's internal test results; in assessing vulnerabilities, DISA attacks and successfully penetrates Defense systems 65 percent of the time. Not all hacker attacks result in actual intrusions into computer systems; some are attempts to obtain information on systems in preparation for future attacks, while others are made by the curious or those who wish to challenge the Department's computer defenses. For example, Air Force officials at Wright-Patterson Air Force Base told us that, on average, they receive 3,000 to 4,000 attempts to access information each month from countries all around the world.

Page 2

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks

195



	Information Security: Computer Attacks at Department of Defense Pose Increasing Risks
	tactics, such as where the enemy is located and what targets are to be attacked. The hackers also launched other attacks from the lab's computer systems, gaining access to systems at NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base, and Defense contractors around the country.
	Datastream Cowboy was caught in Great Britain by Scotland Yard authorities, due in large part to the Air Force's monitoring and investigative efforts. Legal proceedings are still pending against the hacker for illegally using and stealing British telephone service; no charges have been brought against him for breaking into U.S. military computer systems. Kuji was never caught. Consequently, no one knows what happened to the data stolen from Rome Lab.
Damage From the Attacks	In general, Defense does not assess the damage from the computer attacks because it can be expensive, time-consuming and technically difficult. But in the Rome case, Air Force Information Warfare Center staff estimated that the attacks on the Rome Lab cost the government over half a million dollars. This included costs for time spent to take the lab's systems off the networks, verify the integrity of the systems, install security "patches," and restore computer service. It also included costs for the Office of Special Investigations and Warfare Center personnel deployed to the lab.
	But the estimate did not include the value of the research data that was compromised by the hackers. Information in general is very difficult to value and appraise. In addition, the value of sensitive Defense data may be very different to an adversary than to the military, and may vary a great deal, depending on the adversary. Rome Lab officials told us, however, that if their air tasking order research project had been damaged beyond repair, it would have cost about \$4 million and 3 years to reconstruct it. In addition, the Air Force could not determine whether any of the attacks were a threat to national security. It is quite possible that at least one of the hackers may have been working for a foreign country interested in obtaining military research data or learning what the Air Force is working on. While this is only one example of the thousands of attacks Defense experiences each year, it demonstrates the damage caused and the costs incurred to verify sensitive data and patch systems.
National Security Concerns	Even more critical than the cost and disruption caused by these attacks is the potential threat to national security. Many Defense and computer

Page 4

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks

197

	systems experts believe that computer attacks are capable of disrupting communications, stealing sensitive information, and threatening our ability to execute military operations. The National Security Agency and others have acknowledged that potential adversaries are attempting to obtain such sensitive information by hacking into military computer systems. Countries today do not have to be military superpowers with large standing armies, fleets of battleships, or squadrons of fighters to gain a competitive edge. Instead, all they really need to steal sensitive data or shut down military computers is a \$2,000 computer and modem and a connection to the Internet.
	Defense officials and information systems security experts believe that over 120 foreign countries are developing information warfare techniques. These techniques allow our enemies to seize control of or harm sensitive Defense information systems or public networks which Defense relies upon for communications. Terrorists or other adversaries now have the ability to launch untraceable attacks from anywhere in the world. They could infect critical systems, including weapons and command and control systems, with sophisticated computer viruses, potentially causing them to malfunction. They could also prevent our military forces from communicating and disrupt our supply and logistics lines by attacking key Defense systems.
	Several studies document this looming problem. An October 1994 report entitled <u>Information Architecture for the Battlefield</u> prepared by the Defense Science Board underscores that a structured information systems attack could be prepared and exercised by a foreign country or terrorist group under the guise of unstructured hacker-like activity and, thus, could "cripple U.S. operational readiness and military effectiveness." The Board added that "the threat goes well beyond the Department. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected." Given our dependence on these systems, information warfare has the potential to be an inexpensive but highly effective tactic which many countries now plan to use as part of their overall security strategy.
Defense Faces Challenges in Securing Its Systems	Many factors combine to make information systems security a huge challenge for Defense: the vast size of its information infrastructure, its reliance on computer systems and increasing amounts of sensitive information, rapid growth in Internet use, and increasing skill levels among hackers coupled with technological advances in their tools and

Page 5

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks

methods of attack. Defense has taken steps to strengthen its information systems security, but it has not established a comprehensive and effective security program that gives sufficient priority to protecting its information systems.

Some elements of a good security program are in place. Most notably, Defense has implemented a formal information warfare program. DISA is in charge of the program and has developed and begun implementing a plan for protecting against, detecting, and reacting to information systems attacks. DISA established its Global Defensive Information Warfare Control Center and its Automated Systems Security Incident Support Team (ASIST) in Arlington, Virginia. Both the center and ASIST provide centrally coordinated, around-the-clock response to attacks and assistance to the entire Department. Each of the military services has established computer emergency response capabilities, as well. The Air Force is widely recognized as the leader among the services for having developed considerable experience and technical resources to defend its information systems.

However, many of Defeuse's policies relating to computer systems attacks are outdated and inconsistent. They do not set any standards or require actions for what we and many others believe are important security activities, such as periodic vulnerability assessments, internal reporting of attacks, correction of known vulnerabilities, and damage assessments. In addition, many of the Department's system and network administrators are not adequately trained and do not have enough time to do their jobs properly. Computer users throughout the Department are often unaware of fundamental security practices, such as using sound passwords and protecting them. Further, Defense's efforts to develop automated programs and use other technology to help counter information systems attacks need to be much more aggressive and implemented on a departmentwide basis, rather than in the few current locations.

In our report being released today, <u>Information Security: Computer</u> <u>Attacks at the Department of Defense Pose Increasing Risks</u> (GAO/AIMD&S84), we are recommending that Defense take a number of actions to address these weaknesses and improve its information security posture. To ensure it has an effective security program, we recommend that the Department establish up-to-date policies for preventing, detecting, and responding to attacks on its systems; increase awareness among all computer users of the risks of computer systems connected to the Internet; and ensure that information security officials and systems

GAO/T-AIMD-96-92

Page 6

	Information Security: Computer Attacks at Department of Defense Pose Increasing Rinks
	administrators receive enough time and training to do their jobs properly. Further, we recommend that Defense assess its incident response capability to determine its sufficiency in light of the growing threat, and implement more proactive and aggressive measures to detect systems attacks. The fact that these important elements are missing indicates that Defense has not adequately prioritized the need to protect its information resources. Top management at Defense needs to ensure that sufficient resources are devoted to information security and that corrective measures are successfully implemented.
Continued Oversight Needed	We have testified and reported on information systems weaknesses for several years now. In November 1991, I testified before the Subcommittee on Government Information and Regulation on a group of Dutch hackers breaking into Defense systems. ¹ Some of the issues and problems we discussed here today existed then; some have worsened, and new challenges arise daily as technology continues to advance. Without increased attention by Defense top management and continued oversight by the Congress, security weaknesses will continue. Hackers and our adversaries will keep compromising sensitive Defense systems.
	That completes my testimony. I'll be happy to answer any questions you or Members of the Subcommittee may have.
	¹ Computer Security: Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5, November 20, 1991).
(511349)	Page 7 · GAO/T-AIMD-96-92





Senate Permanent Subcommittee on Investigations

Minority Staff

Jim Christy, Investigator

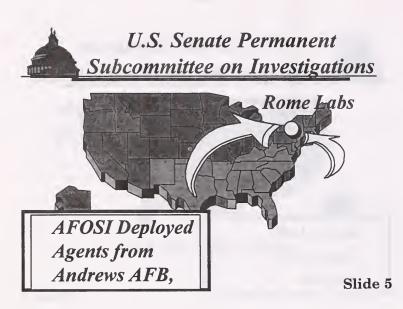
Slide 1



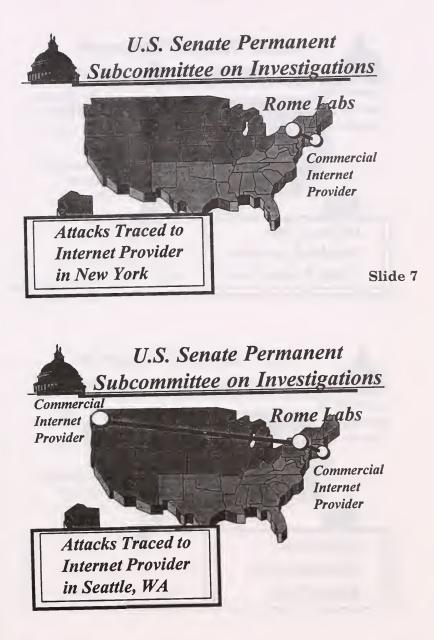
Slide 2

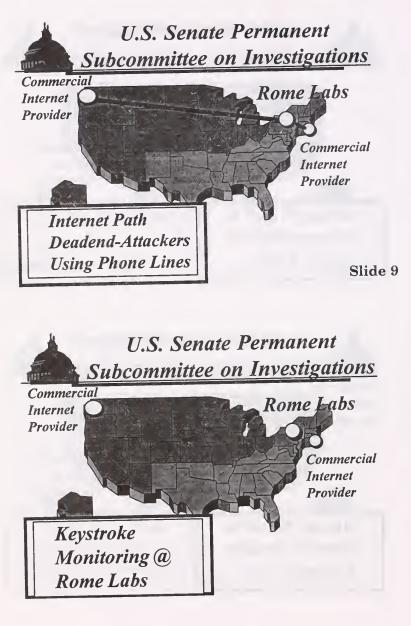
200

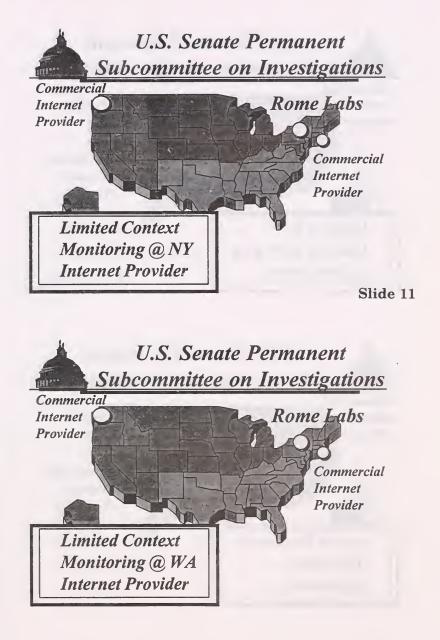


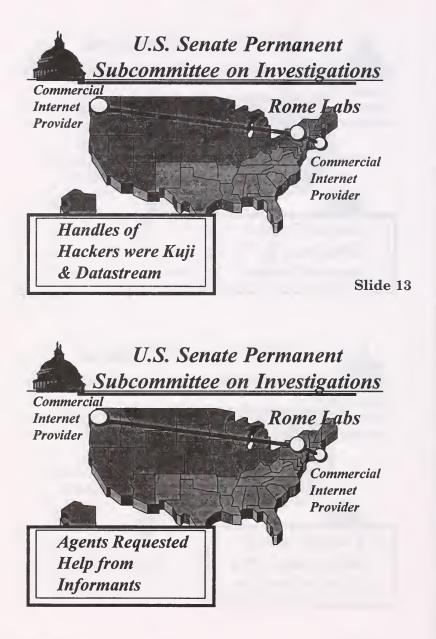


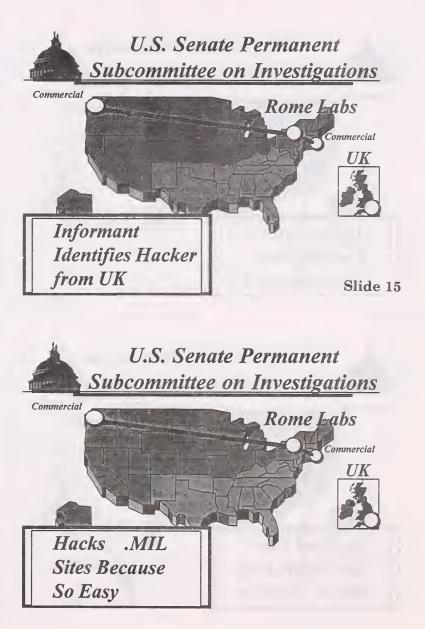


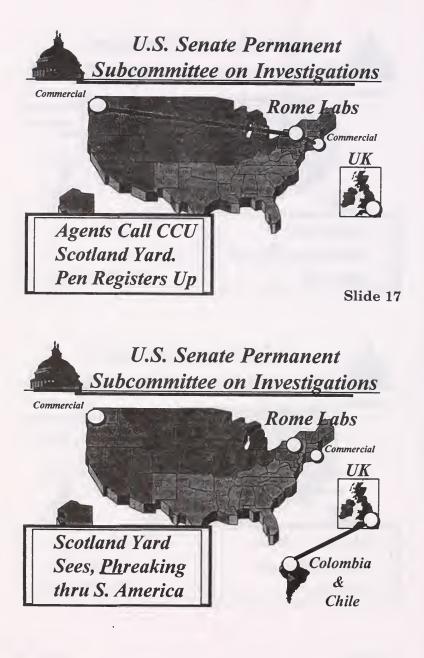


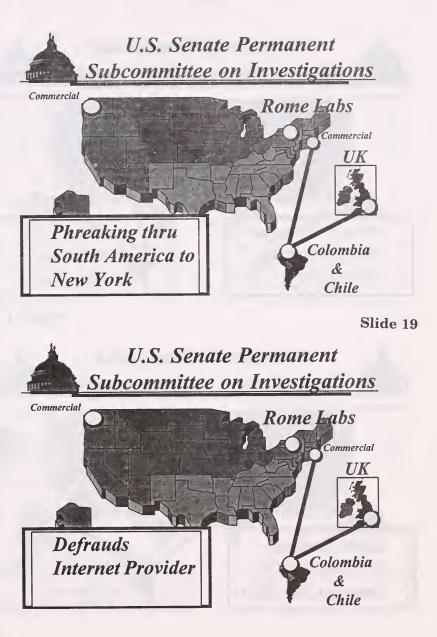


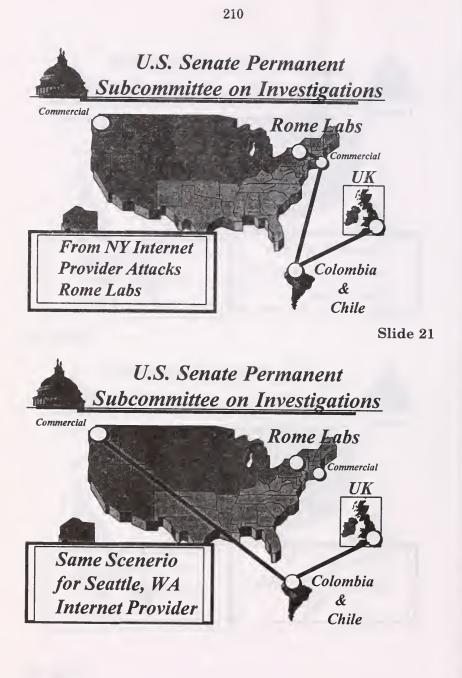


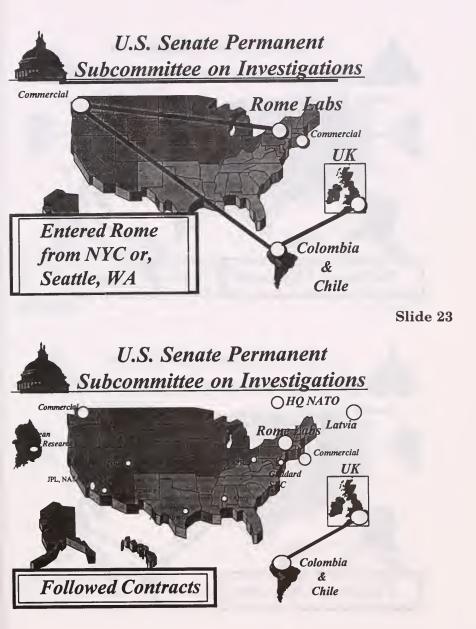


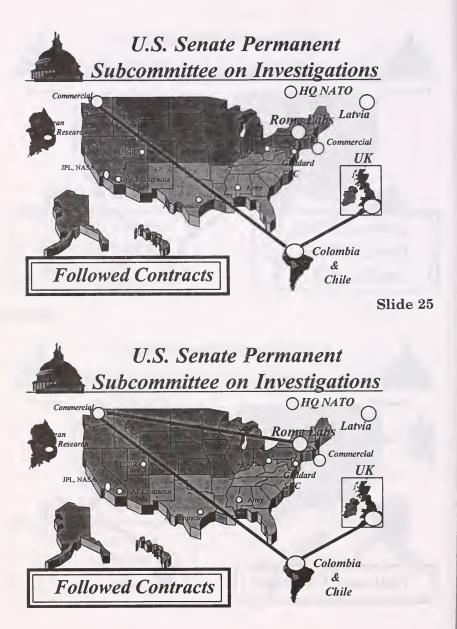


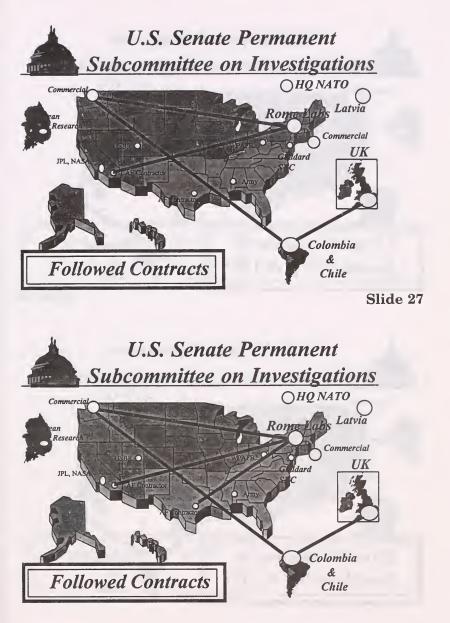






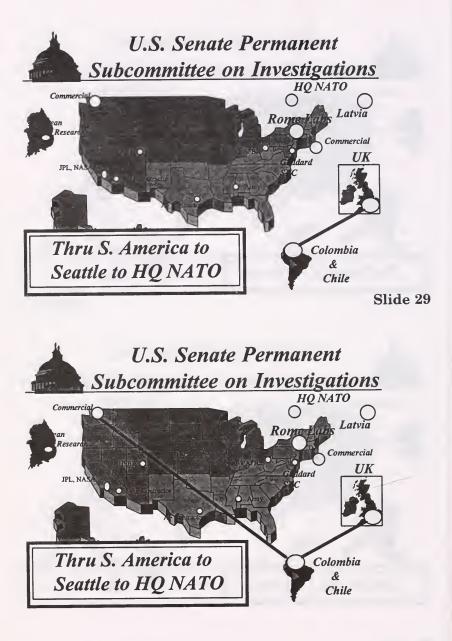


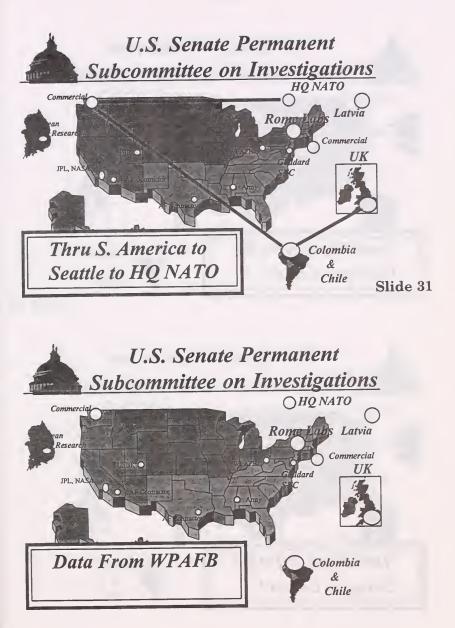


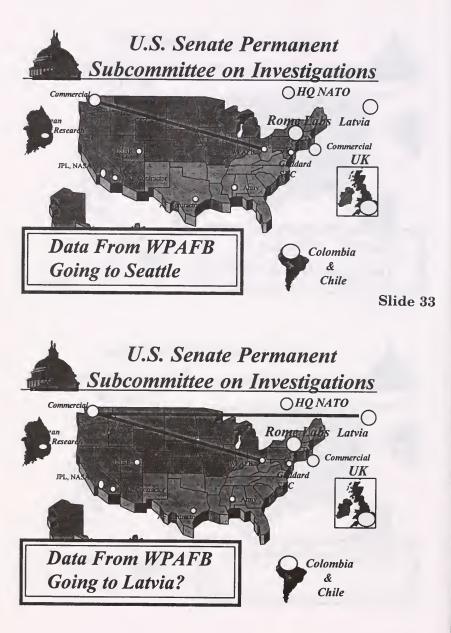


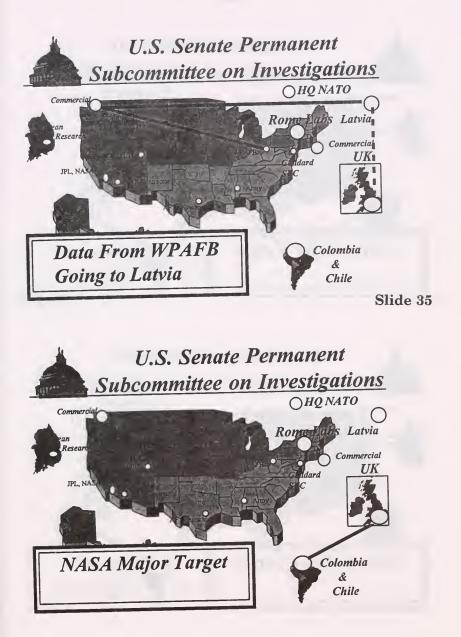
213

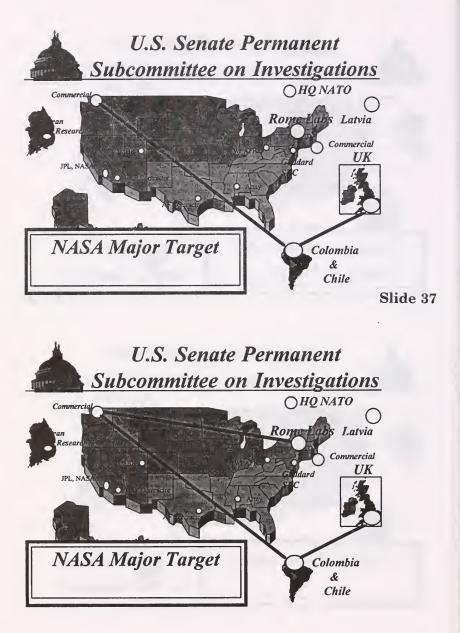
Slide 28

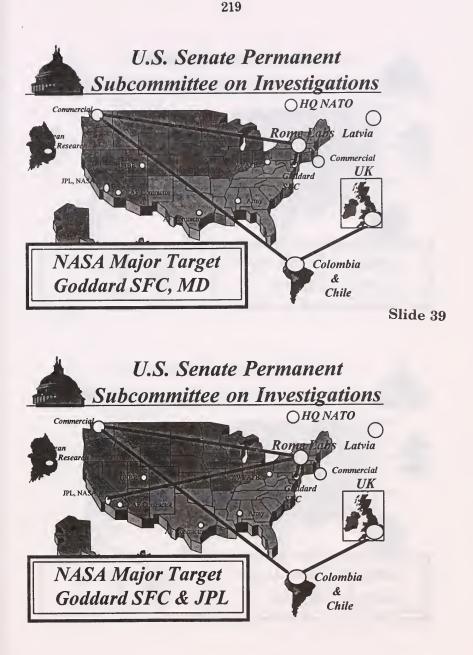




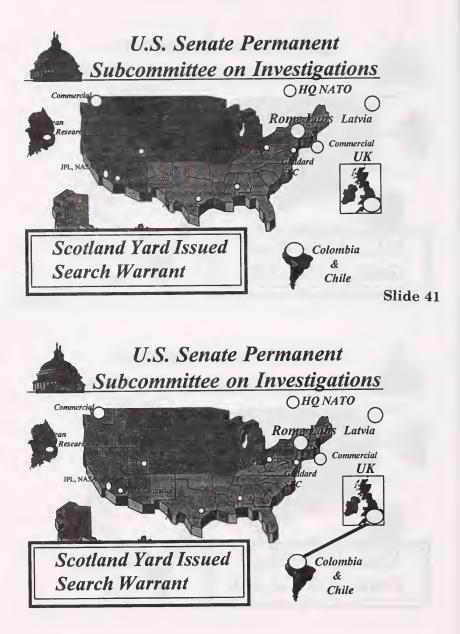


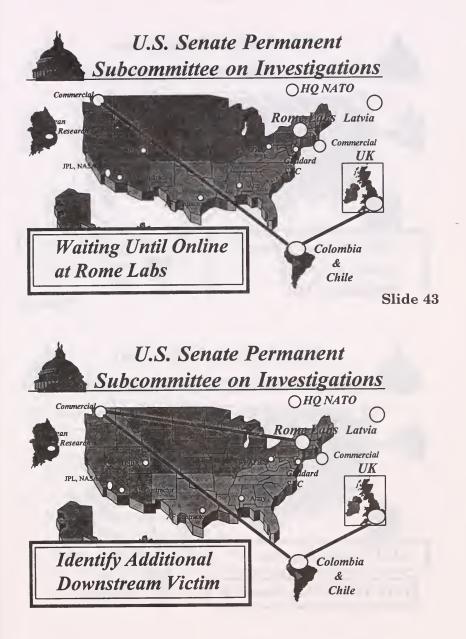


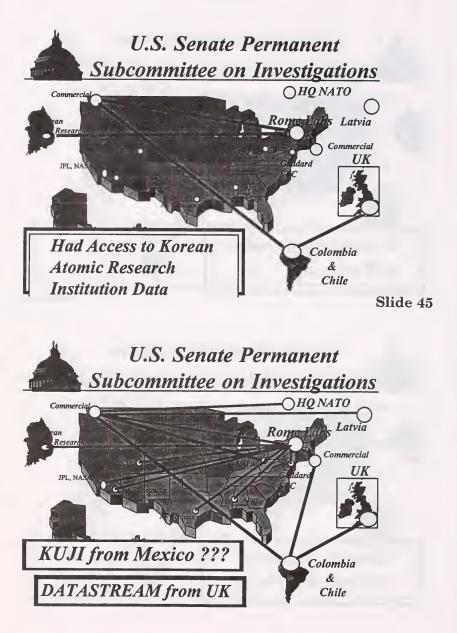


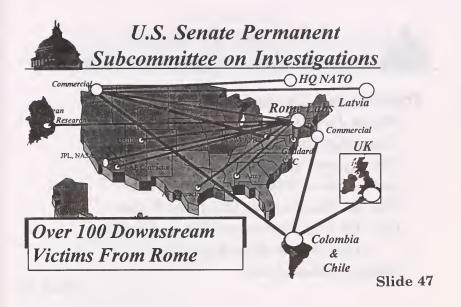


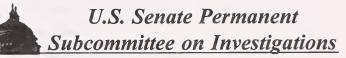
Slide 40











Rome Labs Summary

- 2 Hackers
- 26 Days of Attacks
- 20 Days of Monitoring
- 7 Sniffers on Rome Systems
- Over <u>150 Intrusions</u> at ROME Labs from 10 Different Points of Origin
- Victims Many & Varied
- Law Enforcement Agencies Multiple
- At Least <u>8 Countries</u> Used as Conduit



U.S. Senate Permanent Subcommittee on Investigations

Problems Now Encountered: Whose Jurisdiction? Tracing on Internet Tracing on Public Switched Network Surveillance (Where do you Monitor) How do You Recover What was Stolen How Do You Determine Who had Access to the Stolen Rome Labs Files Damage Assessments

STAFF STATEMENT

U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

(Minority Staff)

HEARINGS ON

SECURITY IN CYBERSPACE

JUNE 5, 1996

* * *

TABLE OF CONTENTS

I.	THE INFORMATION INFRASTRUCTURE A. Defining the National Information Infrastructure ("NII") B. Our Dependency on the NII	. 2
II.	VULNERABILITIES A. Weaknesses in Hardware & Software B. Human Factor C. Lack of Security Culture D. Examples of Vulnerabilities	. 6 . 9 10
III.	THE THREAT A. Lack of Intelligence Collection B. Lack of Detection and Reporting 1. Government 2. Private Sector C. The Potential Attackers	14 17 17 18
IV.	EFFORTS TO PROMOTE INFORMATION SECURITY A. Creation of a National Policy B. Current Law Enforcement Response C. Private Secrot Response D. Computer Emergency Response Team (CERT) E. Encryption and the NII F. NIST and NSTAC 1. National Institute of Standards and Technology (NIST) 2. National Security Telecommunications Advisory Committee (NSTAC) G. International Efforts to Promote Information Security	23 24 26 27 28 30 30 30
V.	STAFF RECOMMENDATIONS	32
APF	PENDIX	35

STAFF STATEMENT U. S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS (Minority Staff) HEARINGS ON SECURITY IN CYBERSPACE JUNE 5, 1996

* * *

The computer age arrived with great promise and expectation. Just four years ago, the Internet hosted one million users. Today that number exceeds 58 million, and is growing at an estimated rate of 183% per year. Advances in computing and networking have affected virtually every aspect of our society, including civilian government, the military, communications, transportation and commerce. Government is more efficient and connected, business is more robust and able to provide more services, and individuals now have access to large caches of information and each other.

The computer age has also brought with it vulnerabilities and weaknesses. As we rush to connect to the information superhighway, are we sufficiently questioning the vulnerabilities created by our growing dependency on computers and networks? As the most critical pieces of our national infrastructure become dependent upon these information networks, have we ensured they are secure and reliable?

The purpose of this report is to examine the vulnerabilities of our national information infrastructure and efforts by our government to promote its security. To prepare this Statement, the Permanent Subcommittee on Investigations (Minority) Staff, at the direction of the Subcommittee's Ranking Minority Member, Senator Sam Nunn, spent approximately 8 months interviewing representatives from industry and government, as well as private individuals expert in the field of information security. The Staff also examined the international aspects of this issue with numerous briefings from foreign officials.

The Staff's conclusions, which are set forth throughout this report, can be summarized as follows:

- Our government and our private sector have become increasingly dependent on computers and networks such that our nation has created a critical information infrastructure that supports the most essential functions of our society.
- Today, our information infrastructure is increasingly vulnerable to computer attack from a variety of bad actors including foreign states, subnational groups, criminals and vandals. Anecdotal evidence documents that these adversaries are organized and already regularly exploiting these vulnerabilities.
- The technology that allows this array of bad actors to exploit networks is becoming more available and user-friendly. Vulnerabilities in hardware and software are giving hackers -- no matter their motive -- greater opportunities and abilities to successfully attack our information infrastructure. Recent Defense Department studies suggest that computer attackers successfully intrude on DoD unclassified but sensitive networks more than 65% of the time.
- Computer hackers use different routes of attack, often crossing national boundaries and using private and public computer network systems. This

presents complex and novel legal and jurisdictional issues that hinder the detection of and response to computer intrusions.

- Our government and private industry's inability to foster a culture that promotes computer security is greatly exacerbating the vulnerabilities of our information infrastructure.
- Our government has been unable to adequately define the scope of the threat
 posed by computer attacks because the intelligence community has failed to
 dedicate sufficient resources to data collection and analysis.
- The private sector -- including the commercial and financial world -- has been unwilling to report their own vulnerabilities for fear of inspiring customer insecurity. As a result, enormous losses occur that escape the attention of the law enforcement and intelligence communities. One informal estimate by a group of computer security firms documents losses among just their clients at over \$800,000,000 in one year alone.
- The U.S. government has recently recognized the potential severity of this
 problem and is only now beginning to address its very serious ramifications to
 our national security.
- Our nation is in need of a comprehensive strategy that addresses the vulnerability of our information infrastructure.
- Our failure to recognize this threat and respond with sufficient resources, will have severe consequences for our nation's security as we become more connected and more dependent upon our information infrastructure.

I. THE INFORMATION INFRASTRUCTURE

A. Defining the National Information Infrastructure ("NII")

The Staff's investigation has focused on threats to the National Information Infrastructure (the "NII") and the potential impact of such threats on the United States infrastructure as a whole. In examining this issue the Staff adopted certain widely accepted definitions. The NII refers to that system of advanced computer systems, databases, and telecommunications networks throughout the United States that make electronic information widely available and accessible.¹ This includes the Internet, the public switched network, and cable, wireless, and satellite communications. The National Information Infrastructure is merely a subset of what has become known as the Global Information Infrastructure (the "GII").

References to the United States infrastructure includes those systems and facilities comprising identifiable institutions and industries that provide a continual flow of goods and services essential to the defense and economic security of the United States, the

¹ This is the definition used by the National Information Infrastructure Security Issues Forum. The Forum is a part of the Information Infrastructure Task Force which was formed by Vice President Gore to articulate and implement the Administration's vision for the NII. A glossary of definitions related to this Report is appended as Appendix A.

functioning of government at all levels, and the well-being of society as a whole.² This includes telecommunications, energy, medical, transportation, and financial systems, as well as government operations and national defense.

B. Our Dependency on the NII

Our society is extremely dependent on both the NII and the GII at almost every level of daily life -- individual, commercial and governmental. Consider the following:

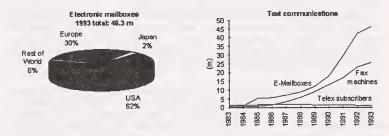
- Our communications, whether via telephones, fax machines, pagers, or cellular telephones increasingly rely on the NII as providers are replacing their analog switches with computer dependent digital switches.
- Much of the way money is accounted for, handled, and exchanged is now done
 via the NII. Salaries are directly deposited into bank accounts by electronic
 funds transfers. Automated teller machines ("ATMs") deposit funds, withdraw
 funds, and make payments. When payment is made for merchandise with
 debit cards and credit cards, transactions are verified using the public switched
 network.
- Much of our national economy also depends on the NII. The vast majority of transactions conducted by banks and other financial institutions are done via electronic funds transfers. For example, one major bank transfers approximately \$600 billion electronically per day to the Federal Reserve. Over \$2 trillion is sent in international wire transfers every day. In addition, most securities transactions are conducted via computerized systems.
- Health care is increasingly becoming dependent on electronic records as pharmacies and hospitals maintain computerized files containing their patients' medical profiles. Medical care is moving toward greater dependency on computer-based technologies; hospitals are testing the viability of "on line" remote medical diagnosis.
- Our civil aeronautics industry is reliant upon computers to fly and land airplanes; railway transportation is dependent upon computers to coordinate tracks and routes.
- Government operations are also heavily dependent on the NII. The government uses computerized systems to do everything from issuing Social Security checks to keeping track of criminal records. Within our national defense structure, over 95% of the military's communications utilize the public switched network. Many of the military's "precision" weapons depend on the Global Positioning System (the "GPS")³ for guidance. In addition, the military uses computerized systems to transmit data and information related to troop movements, procurement, maintenance and supplies.

² This is the definition used by the Critical Infrastructure Working Group (the "CIWG"), chaired by Deputy Attorney General Jamie Gorelick. The CIWG was tasked under Presidential Decision Direction 39 with identifying and assessing threats against the critical national infrastructure and proposing both interim and long-term options for preventing and responding to such threats.

³ The Global Positioning System (GPS) is a space-based system utilizing ground transmitters and orbiting satellites to triangulate locations with pinpoint accuracy.

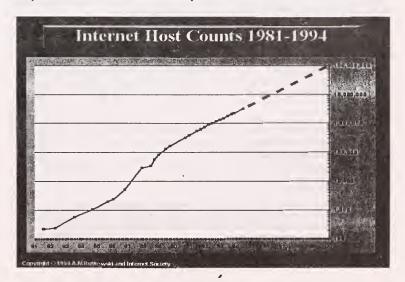
In short, the United States infrastructure has increasingly come to rest on the pillars of the national and global information infrastructures. Should these pillars be weakened or seriously shaken, many of the critical functions of our society could come crashing down or experience significant damage.

As dependent as society is today on the information infrastructure, that dependence will only grow in the years to come. For example, the electronic exchange of messages ("e-mail") is becoming so common that it is challenging other forms of communication, including the facsimile, the telex, and even the postal service. The following charts illustrate the growth of what has become known as e-mail:



The growth of electronic communications is spurred by the ever-increasing speed with which data can be transferred. The speed with which modems can transfer data has changed transmission time significantly. In 1980, a 300 bps (bits per second) modem required 160 minutes to transmit a book of approximately 200 pages; last year a commercially available 28.8 Kbps took less than two minutes to transfer the same book; today's 45 mbps modem speed provides for transmission of the same book over the Internet in .06 of a second. In just a decade, the speed has increased 160,000 times.

This, in turn, has led to a phenomenal growth of the Internet, one of the crucial elements of the information infrastructure. In 1969, the forerunner of the Internet started with just four major systems on what was essentially a single network. Today there are approximately 9.5 million hosts or major computer networks or systems. By the year 2000, the number of hosts is expected to reach 100,000,000.



- 4 -

This increased connectivity, and the enhanced communications that come with it, will no doubt increase the efficiency of the flow of goods, services, and ideas within our society. At the same time, however, this very same connectivity will also increase the vulnerability of our society to new forms of attack.

II. VULNERABILITIES

As technology has given us advanced means of creating, storing and communicating information, it has also made that information more vulnerable. Consider the example of our armed forces.

Our armed forces are the most technologically advanced in the world. The Defense Information Infrastructure (the "DII") operates in support of the military's warfighting, intelligence, and business functions. The Department of Defense (the "DoD") is extremely dependent on computer systems to fly, fight, feed and track our troops. The protection of these systems is thus essential to national security.

For example, computerized logistic systems that direct supplies to the appropriate post or base must in time of crisis or war get the right number of bullets or gas masks to the military installation that needs them. If toothbrushes were to arrive instead of bullets, it would obviously have a dramatic effect on a military deployment, exercise or action. Or if a foreign enemy were able to track the movement of such supplies, strategic decisions would lose their confidentiality.

However, over 90% of the DII is composed of unclassified systems. An unclassified computer system is a system in which each individual file on the system is unclassified. While each of the files, individually, is considered unclassified, the unclassified systems contain literally thousands of "sensitive"⁴ files, including research and development for war fighting systems, intelligence data, troop movement and weapons procurement.

In the days before computer systems this unclassified information was far better protected. Each file was in a file cabinet that was probably locked. This file cabinet would be located in an office that was probably behind a locked door in a government building that might even have an armed guard. This government building would likely be on a military installation that had a fence and gate guards.

To access all of this unclassified information, the adversary would have to get onto the military installation and into each building, each room and each file cabinet. Then, the adversary would have to somehow remove all of the paper documents or reproduce them without being detected. The DoD would never consider removing its perimeter fences, gate guards, door locks or file cabinets, nor would it consider allowing unauthorized personnel to roam its installations or to have access to its paper documents.

In the virtual world, however, all of these unclassified documents may be located on one server that is connected to virtually any other computer anywhere in the world. An intruder could electronically bypass the installation gate guard, enter the building and, with a few keystrokes, rummage through all of the file cabinets -- or only those files

⁴ "Sensitive information" is defined as unclassified information "the loss, misuse, unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled" under the Privacy Act (15 U.S.C. Section 278g-3(d)(4)).

needed by using a keyword search -- and then make copies of all of the files and leave without ever being detected.

Once in the electronic files, an intruder could also modify the information. The intruder could install "time bombs"⁵ that would destroy or change the information at a predetermined time or event. Some might do this as a prank, while others may have a more sinister purpose such as adversely affecting the readiness of military units.

It is not merely the theft of information with which the DoD, or any other agency, must be concerned. Our military leaders must have confidence in the accuracy and integrity of their data and information. A changed mathematical formula could alter the flight path of missiles or aircraft. Shifted decimal points in the DoD's finance system could wreak havoc.

Moreover, the DoD must at all times be able to access its information. The destruction or denial of access to certain information could have severe implications for a unit's ability to carry out its mission.

In the physical world, our Defense Department would never allow its information to be at risk in the manner it is in the virtual, electronic world. Senior leaders and managers understand the threats in the physical world, but are only recently discovering the threat in the virtual world.

What is true for our armed forces is just as true for other parts of the government and the private sector. Identifying and addressing vulnerabilities is critical. What then are the major vulnerabilities of our information infrastructure? The Staff has observed vulnerabilities in three main areas: (1) software and hardware weaknesses; (2) human weaknesses; and (3) the lack of a security culture. Each of these vulnerabilities can be exploite.. to allow intruders unauthorized access to information systems, leaving the information or those systems subject to theft, manipulation, or other forms of attack.

A. Weaknesses in Hardware & Software⁶

Hardware and software flaws and weaknesses arise from the basic assumption of product developers that all users can be trusted. Rarely is security a major consideration in the research and development of information systems. In addition, the pressure of competition forces companies to field applications as quickly as possible, often without the benefit of comprehensive testing for inherent flaws. The industry relies on users to report product flaws -- in turn the industry will either fix the flaw or release a new version of the product. Of course, new versions of products may also have new flaws.

Hackers exploit these inherent flaws and are able to globally disseminate their techniques. The hackers are much better connected and organized and share information about specific vulnerabilities regularly. There are forums for hackers that include physical meetings as well as electronic meetings. Hackers publish glossy magazines where they share vulnerabilities and techniques and trade "war" stories about their individual attacks. *Phrack* magazine -- on-line since 1985 -- is one of the most

⁵ A "time bomb" or "Trojan horse" is a hacker technique used to compromise or disrupt systems. It is usually a hidden function in a computer program that the user-victim is unaware of.

⁶ "Hardware" is the physical computer equipment; "software" is the program that runs computer applications.

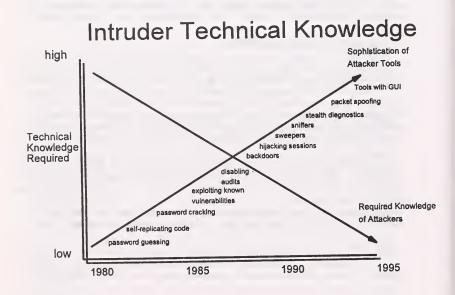
popular of the hacker magazines, providing information to the hacker underground on information about different computer operating systems, networks, and telephone systems.

Hackers also meet regularly on what is called the Internet Relay Channel (the "IRC") for on-line conversations called "chats." Hacking tips and techniques are easily passed through these sessions. In addition, there are well-publicized hacker conventions all over the world during which face-to-face exchanges of techniques are made.

Technology has made it much easier for hackers to exploit hardware and software flaws. In the early 1980's, only very technically competent individuals had the expertise to break into computer systems. Not only were there fewer hackers, there were not as many targets to attack.

This has changed dramatically in the past two years. The proliferation of computers has created a new universe of targets in government, the military and in private industry. Much more of the population has access to computers at work and at home. The vast majority of the people that buy computers today have bundled software packages that give them Internet access.

Similarly, many more people today have the capability to develop hacker tools than fifteen years ago. Colleges, universities and technical schools graduate tens of thousands of computer experts yearly many of whom are highly trained in methods to secure and exploit software program. A small percentage -- but nevertheless a significant number -- of these people can and are developing tools and techniques to break into the computers and networks of others.



Unfortunately, while the hacker's tools are becoming more and more sophisticated, they are also becoming more user friendly, requiring very little expertise to operate. Point and click technology called Graphical User Interfaces have given anyone with a computer, a modem, and access to the Internet the capability to break into someone else's computer anywhere in the world.

For example, point & click software such as SATAN ("Security Administrator Tool for Analyzing Networks"), which was disseminated on the Internet in April 1995, is a series of hacking tools that can be used by individuals with very little expertise. SATAN scans systems to find network-related security problems and reports whether the vulnerabilities exist on a tested system without actually exploiting them. Although SATAN was intended for systems administrators and security professionals to analyze their networks for security vulnerabilities, potential intruders use this tool to identify and attack government and private networks.

Internet Protocol ("IP") spoofing is a technique used by attackers to gain access to someone's system by masquerading as another Internet system that is trusted by the targeted system. This IP spoofing can also prevent identification of the attacker if the attacker is determined to be an unauthorized intruder by the victim system.

These tools and techniques can be extremely effective. The Defense Information Systems Agency ("DISA") has been performing pro-active electronic "Red Teaming" of Department of Defense systems for over three years. DoD commanders can request and authorize DISA's team of computer security experts to attempt to electronically penetrate their systems. DISA's experts will only attack a DoD system using hacker attack software tools or techniques that are already widely available on the Internet.⁷

As of May 1996, DISA is able to electronically break into 65% of the systems they attack using commonly available attack tools found on the Internet⁸. What that means is only 35% of our DoD unclassified computer systems are secure. DISA officials have told the Staff that the 65% figure is really a conservative figure. That figure is the result of an average one week dedicated attack against a particular network. These officials report that if they are given more time to attack a targeted network they could probably compromise upwards of 95-98% of the systems.

Another potential vulnerability in terms of software is in the use of commercial off-the-shelf software ("COTS"). Ten years ago software was developed specifically for the government and generally by the government. The government owned the programming code that ran the applications. The government also knew what was in the

⁷ Furthermore, DISA in a spirit of fairness, will only use hacker tools for which there is a published "fix" and for which DISA has published an official alert.

⁸ This statistic is based on over 30,000 electronic penetrations performed as of May 1996. These statistics have improved over the last two years. Just prior to the Subcommittee's May 22, 1996 hearing, DISA reported they were able to attack DoD systems successfully 88% of the time. The improvement of the statistics may be based on a greater awareness of computer users within the Defense Department, or it may also be based upon changes in DISA's vulnerability assessment protocol.

code. The government knew what the code was supposed to do and exactly what it did. If the government needed changes to the code, it would make the changes or hire a contractor to modify the code.

Today's environment is much different. The government no longer has very many mainframe computer systems that require a specialized programmer code. It is much more cost effective to buy off-the-shelf computer hardware and off-the-shelf computer software packages. The problem with commercial off-the-shelf software is that the software's programming source code is proprietary and usually a trade secret that the government cannot examine. The government only purchases a license to use the commercial software. The purchaser knows what they want to use the software for, but may not know everything the software can do. Software packages can include features that are possibly undocumented⁹ and potentially unwanted.

The typical user is completely dependent on what the vendor provides. As long as the software does what it is intended to do, it is not questioned. What if software purchased off-the-shelf contained a bug that was to be triggered on a certain date and was programmed to change or destroy a system's database? Would government or business be able to recover the information lost? This, unfortunately, is the great unknown that comes with commercial off-the-shelf products.

B. Human Factor

Perhaps the biggest source of information systems vulnerability are the people who use and manage computer systems and networks. The proliferation of computers and their ever-increasing ease of use has put incredibly sophisticated systems containing very valuable information under the control of millions of people who do not yet grasp the need to maintain security or the consequences of a breach of security.

Often the simplest conduct can create vulnerabilities. Leaving a machine on gives anyone who wanders by access; using easy-to-remember passwords affords intruders easy opportunities to access systems; leaving a password with numerous office colleagues or writing it on a computer are also security risks.

People's trust is also often a source of vulnerability. For example, a popular feature on the Internet are "chat rooms" in which individuals anywhere on the Internet can join in and communicate with others through text transmission. Chat rooms, however, provide little assurance of the true identity of the participants -- they could be a student, business person, computer enthusiast, criminal, saboteur, or foreign intelligence agent. Nevertheless, individuals share information with strangers that might include personal information as well as sensitive business or, in some circumstances, classified information.

One such example involves the case of the U.S. Air Force pilot that was shot down over Bosnia. After he was recovered, one of his fighter pilot colleagues went on-line with

⁹ For instance, in the recently introduced and highly popular Microsoft "Windows 95" operating system, the software contained an undocumented feature -- known in the computer field as an "Easter Egg" -- built in that the Microsoft Corporation was unaware of until after production. When using this software application -- which the Staff would emphasize was <u>not</u> sinister and only frivolous -- if you strike a certain combination of keystrokes the names of the Microsoft development team scrolls across your monitor. The data and software for this undocumented feature resides in a very significant number of the world's computer systems and virtually no one knows about it.

a very detailed version of the actual recovery of the downed pilot. Much of the information provided in the open Internet forum may have been classified or at least very sensitive. Literally tens of thousands of copies of this fighter pilot's e-mail were read and forwarded to others, including the news media.

The trusting nature of individuals also leaves them open to a hacker technique known as social engineering. Social engineering involves hackers impersonating authorized users, customers, vendors, or others to persuade unwitting authorized employees to divulge critical information such as logons and passwords. Although very "low-tech," this technique continues to reap benefits for hackers. Social engineering exploits the lack of security training and awareness of employees and the emphasis placed on customer service. It is a the computer world's equivalent of the old-style "confidence game."

C. Lack of Security Culture

Another significant vulnerability is the inability of managers who run systems to detected intrusions. Of the DoD systems compromised by the electronic Red Teaming performed by DISA, only 4% of the managers or users of compromised systems actually detected the intrusion. The primary reason systems administrators are not able to detect these types of attacks is the lack of a security culture within government and private industry. Even those entities that take security seriously, though, are hindered by the lack of a dequate tools to assist the systems administrators and computer security professionals to detect these invisible crimes.

Of the 4% of the DoD systems administrators that did detect the electronic intrusion by DISA experts, only 27% of the 4% reported the intrusion to the appropriate security or law enforcement agency. Reasons for not reporting can range from not knowing where or to whom to report to being directed not to report due to embarrassment. Commanders are reluctant to report incidents for fear it may negatively affect their careers. This is also true for systems administrators.

Although these statistics are alarming, DoD is proactively identifying and trying to address their systemic deficiencies. Other agencies have no Red Teaming activity or very limited plans to address their own vulnerabilities.¹⁰ The Staff conducted interviews with the computer security personnel at numerous government agencies. Most of these agencies quoted the DISA statistics, but few agencies conducted their own vulnerability assessments. Many of the computer security personnel interviewed from non-DoD agencies and departments believed Red Teaming was imperative but generally did not have the resources to perform their own vulnerability assessments.

Computer security professionals lack the resources to address the systemic problems of network vulnerability. In many government organizations, senior managers typically do not understand and, therefore, cannot acknowledge the vulnerabilities of their information systems. As the government downsizes and the private sector struggles

¹⁰ The National Institute of Standards and Technology (NIST) recently received an "innovation" grant for \$4 million in order to establish, in the future, an incident response team within non-DoD government that would, as part of its duties, conduct vulnerability assessments of government computers. Unfortunately, the response aspect of the team will be on a "pay as you go" basis, so government agencies will pay for its services out of their budgets. This may serve as a disincentive to government agencies to bring their intrusions to NIST. Further, given the enormous amount of computer systems and networks, it is doubtful that the grant will meaningfully address this problem.

For example, currently in the government there is no Computer Security Specialist Career Field. Personnel are most often assigned the duties of computer security as an additional duty, not as a full-time computer security expert. The additional duty of computer security may be assigned to a non-computer specialist.

Generally, computer security personnel have virtually no computer security experience prior to the assignment and receive very little in the way of computer security training during their tenure. The Staff has found instances of secretaries and administrators being assigned these duties in an office because their computer expertise, although limited, was greater than everyone else's. Often, after two or three years as a computer security specialist, the duty is rotated to another person. This new appointee will normally not have any background in computer security either. The government continues to rotate these additional duties and completely loses the institutional knowledge it has developed.

Our government has created a climate that is not conducive to fostering security. Clearly, in-depth knowledge and understanding of a very technical subject is a requisite for an information security officer. Unfortunately, specializing in a subject that lacks a career path is a disincentive for employees. If a government employee wants to stay in these specialities they must either accept little prospects for promotion or move from the government to the private sector which is willing to reward specialists in this area with much greater monetary compensation. The end result is a brain-drain of experts from the government to the private sector, which then turns around and contracts the same experts back to the government at a far greater price then if the government gave them career progression in the first place.

In the law enforcement arena the Staff has observed that almost all law enforcement agencies recruit criminal investigators from within their agency and then try to teach them computer technology. Generally, criminal investigators are assigned to computer crime investigations for a two to three year assignment and not as a permanent career choice. The result is a constant turnover of personnel with little to no corporate knowledge, and a constant pool of investigators with little "computer" expertise.

Similar to security personnel, if a computer crime investigator is allowed to stay in the speciality, it may have a negative effect on career progression, as law enforcement favors generalists over specialists.

Based on interviews conducted by the Staff with computer security experts from the private sector, the problem is generally the same outside of government as well. Computer security personnel in the private sector generally do not have a strong voice in the corporate and management decisions. In the private sector the computer security experts are usually at odds with the business leaders of their companies. Generally, the computer security function is buried in the administrative computer support area of a business. The pressure to automate and connect systems almost always takes precedence over the need to protect.

- 11 -

D. Examples of Vulnerabilities

The Staff's own review of a number of federal agencies confirmed many of these vulnerabilities. For example, the Staff requested from various agencies the name of the individual or office in charge of computer security. Most agencies responded that they did not know who that individual was; or that they did not know if such a position existed; or that the position was spread over numerous departments.

For example, the Staff found that the Department of Justice, though concerned about the security of their networks, takes a decentralized approach to organizing computer security. Within DOJ each component is responsible for its own security. Very few of the components have a full-time security administrator -- usually this task is assigned as an additional duty to a secretary within the component. This is partially due to resource constraints. Typically, security administrators are slotted in the range of a GS-7 to GS-11. Attracting quality applicants, according to Department officials, therefore becomes a problem. A concern raised by some DOJ officials was that the "pressure to connect" with other networks and the Internet would increase their vulnerabilities.

The lack of clear authority for computer security was particularly acute at the Department of State. A recent Inspector General (IG) audit of the Department's unclassified mainframe security system found that the Department basically had no security plan. As a result, the IG found that the Department was not in a position to even reliably know if information has been compromised. The IG also found that the lack of senior Department management's involvement in addressing authority, responsibility, accountability, and policy for computer security had resulted in incomplete and unreliable security administration.

Inspector General officials also told the Staff that a major threat to the State Department's systems could be from outsourcing computer systems administration to foreign national employees. At foreign posts (with the exception of "critical threat posts"), the Department hires local nationals for computer systems administrators, primarily due to salary constraints. Once hired, these administrators have unlimited access to the post's unclassified computer systems. In Bangkok, for example, the local system administrator designed his own software that embassy employees were using on their computer system. It gave user privileges to everyone regardless of their need for access.

In the Defense Department, the problem of intrusions and attacks into the unclassified but sensitive network is growing with an estimated tens of thousands of successful computer attacks occurring each year.¹¹ While the existence of DISA and its aggressive vulnerability assessment program affirms a level of commitment, a particularly troubling assessment of the Defense Department's treatment of this threat was set forth by the House Committee on National Security in its report on H.R. 3230, the National Defense Authorization Act for FY 1997.

[The] Department is devoting woefully insufficient resources to protecting the Department's information systems.

¹¹ The recent GAO report, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, May 1996, GAO/AIMD-96-84, prepared at the request of Senators Sam Nunn and John Glen, provides an excellent statement of the challenges confronting the Department of Defense.

The problem is a familiar one. Despite widespread recognition of a problem, there are no volunteers to provide funds to correct it. The senior DOD leadership is reluctant to impose a solution to a non-traditional threat, particularly when functional managers and information systems developers present plans that would require funding from outside their own budgets, and therefore entail difficult tradeoffs. In other words, the military services, and the managers of the logistics, medical, personnel, transportation, finance, and other functions within DOD have thus far chosen to maximize capabilities rather than sacrifice capabilities slightly in order to ensure minimum critical requirements are met in wartime conditions.

As a result, over the last two years, the DOD leadership has added only modest resources for information security. The level of funding was not based on a rigorous analysis of requirements, nor were funds limited because advocates failed to make a strong case for additional resources. Rather, the allocation appears to have been determined by the amount of funds that could be easily extracted from the overall budget for command, control, and communications after the normal budget review process.

The potential consequences are that DOD may not be able to generate, deploy, and sustain military forces during a major regional conflict in the event of information warfare attacks on critical support functions controlled by networked computers.

The above language may overstate the extent of neglect in the Defense Department. The Staff would observe that in many ways DoD's <u>self-initiated</u> reviews are the reason for our appreciation of their need to address this issue more meaningfully.

In the Hollywood movie *The Net*, a hacker electronically breaks into the Bethesda Naval Medical Center (BNMC) computer network to access the Secretary of Defense's medical records and change them to reflect that the Secretary was HIV positive. The Staff contacted a senior Bethesda Naval officer to assess BNMC's actual vulnerability. That official indicated that although some management personnel that did not see a great priority in securing the Center's medical files because they could not imagine why anyone would want to break into them, she had conducted her own vulnerability assessment of the computer system of BNMC. She found that she -- and virtually anyone else -- could break into BNMC and access and change the medical records of our government's leaders. Since then, BNMC has aggressively and proactively addressed this vulnerability of their records.

The Staff also interviewed officials with the Federal Aviation Administration (FAA) who stated that they were quite confident their systems were relatively safe from intrusion. This is not, they explained, because they have instituted a healthy security program. Rather, they indicated it is because their aircraft control systems are so antiquated and consist of so many separate and incompatible systems, they are more resistant to modern hacking tools. Further, because the current systems, especially power sources, are unreliable, air traffic controllers are prepared to work without computers. Once the FAA upgrades systems, they will be more vulnerable: first, because their operating systems will be compatible with most other computer systems, including those used by hackers; second, because controllers may become unaccustomed to providing guidance without computer support.

The "pressure" to connect was commonly mentioned by security personnel within government as a great concern and challenge for the future. Various of these professionals were very troubled not by current vulnerabilities, but anticipated - 14 -

III. THE THREAT

Based upon a lack of data collection and analysis by the intelligence community and a failure to report from the business and financial communities, little data has been assembled to provide a reliable assessment of the threat to this nation's information infrastructure.

What is known about the potential threat, however, is extremely disturbing. Technology provides a variety of potential "bad actors" with innumerable methods and opportunities to disrupt our critical information infrastructure and the institutions it supports. These same technologies also offer opportunities to destroy the confidentiality and reliability of the information itself.

Unfortunately, anecdotal incidents provide little assistance in compiling threat assessments and estimates. Most of the documented incidents where bad actors have been identified involved what is considered to be the least competent attacker. A nation state or organized subnational group would likely be more sophisticated, structured and funded -- and difficult to defend against.

A. Lack of Intelligence Collection

In the 150 page Brown Commission Report on the Roles and Capabilities of the United States Intelligence Community (the "Brown Report") the Commission dedicated but one paragraph to the subject of information warfare intelligence collection. This paragraph, however, made the following important observation:

Collecting information about 'information warfare' threats posed by other countries or by non-governmental groups to U.S. systems is, however, a legitimate mission of the Intelligence Community. Indeed it is a mission that has grown and will become increasingly important. It is also a mission which the Commission believes requires better definition. While a great deal of activity is apparent, it does not appear well coordinated or responsive to an overall strategy. (Emphasis added, Brown Report, March 1, 1996, p.27)

A senior member of the intelligence community responsible for collection of such data compared it to "a toddler soccer game, where everyone just runs around trying to kick the ball somewhere."

The Staff did find, however, that collection of data that might provide the nature and extent of the threat posed to our information infrastructure is not presently a priority of our nation's intelligence and enforcement communities. The Staff received numerous briefings from the intelligence components of various agencies, as well as the counter-intelligence community. Each agency agreed that the threat posed to our information infrastructure was substantial; yet when pushed to reveal the level of resources dedicated to assessing the threat, each agency admitted that few personnel were working on developing such an assessment. One agency assembled 10 individuals for the Staff briefing, but ultimately admitted that only one person was actually working "full time" on intelligence collection and threat analysis.

The Central Intelligence Agency (CIA) staffs an "Information Warfare Center"; however, at the time of the Staff briefing, barely a handful of persons were dedicated to

- 15 -

collection and analysis on defensive information warfare. The National Security Agency (NSA), hopes to create a "thousand person" information warfare center that would include both a defensive and offensive infowar focus, as well as a 24 hour response team.

Despite the rhetorical emphasis placed on this issue, at no time was any agency able to present a national threat assessment of the risk posed to our information infrastructure. Usually, briefings, at any level of classification, consisted of extremely limited anecdotal information. The Staff found that, although there is a growing awareness within the intelligence community, there are still very few analysts dedicated to data analysis, and no procedures in place to process intelligence information. Although many agencies had formed "working groups" or incorporated the term "information warfare" into pre-existing offices, there has been very little prioritization of this issue, or re-allocation of resources dedicated to it. Furthermore, there has been minimal retraining of intelligence officers on information warfare or, more importantly, recruitment of intelligence officers with specialized training in information systems technology.

One very senior intelligence officer for science and technology admitted that in order for the intelligence community to focus on the information warfare issue adequately, it would require significant retraining of collectors and analysts. "Don't wait for the intelligence community to provide a threat estimate" he explained, "it will probably take the intelligence community years to break the traditional paradigms, and re-focus resources on this important area."

There have been recent attempts to obtain threat assessments. The "Kyl Amendment" to the Intelligence Authorization Bill for FY 1997 (Sec. 1053) provided:

...the President shall submit to Congress a report setting forth the results of a review of the national policy on protecting the national information infrastructure from strategic attacks. The reports shall include the following:

(1) A description of the national policy and architecture governing the plans for establishing procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions regarding strategic attack for foreign nations, groups, or individuals or any other entity against the national information infrastructure. [Emphasis added.]

Part of the Amendment required that the intelligence community respond to the Congress with a threat estimate within 120 days of the bill's effective date. The timetable was ambitious and the Director of the Central Intelligence Agency requested an extension of time within which to respond. A former high-ranking White House science and technology officer explained the intelligence community's difficulty in responding to the task: "usually they just can pull the information out of the box that holds the data -- as of today, however, the box is just empty!" In the recent House Committee on National Security's report on H.R. 3230, the National Defense Authorization Act for FY 1997, it was observed:

To date, Congress has not received the requested report and overall it is clear that the Administration's response to this statutory requirement has been lackluster at best.

The need for a threat assessment by the intelligence community is great. It is impossible to conduct meaningful risk management absent reliable threat data. How do agencies determine the level of resources to commit to computer security without

- 16 -

knowing the dimension of the threat? The technology of intrusions is changing rapidly. If we do not know what current methods are being employed by hackers, how do we obtain and implement countermeasures. Finally, because much of the threat relates to the compromising of sensitive information, it is difficult, absent reliable threat assessments, to determine what damage has been done. Our nation may be losing critical information advantages and economic advantages without knowing it.

There are numerous explanations for why our intelligence and enforcement assets are unable to collect the requisite data for a national threat assessment.

First, there is no mandatory reporting at the Department of Defense.¹² Yet, Defense installations and assets are a favored target for foreign governments or organized subnational groups. In fact, in the Rome Lab case [see Appendix B] the youthful hacker admitted he penetrated ".mil"¹³ sites because those sites were notoriously easy to penetrate. Due to the lack of reporting, little raw intelligence data is being analyzed by DIA or other intelligence or counter-intelligence components.

Second, from a legal and organizational perspective, intelligence collection is difficult in the virtual world. In the physical world our government assigns intelligence and counter-intelligence responsibility based, in large part, upon the origin of threat. The intelligence community is responsible for foreign threat assessment; the FBI is responsible for domestic threat estimates. There are rules limiting the ability of the CIA, for instance, from collecting information domestically. Similarly, the FBI does not engage in foreign intelligence collection.

The virtual world, however, is borderless and therefore does not fit easily into the organization of the physical world. The technologies employed by hackers permits them to take numerous paths when attacking networks. For instance, it is not uncommon for an attack emanating from a foreign country to take a circuitous route through different nations and different computer networks, both government and private.¹⁴ Thus, when the attack is observed or detected, it may appear to originate from a domestic computer when it actually originated abroad. Because of this, though, the intelligence community would find itself constrained from conducting any original investigation of this matter. The Staff was advised on several occasions that the intelligence community was suffering from their inability to receive raw data that is directed to the law enforcement community.

Finally, and perhaps most importantly, it is simply not yet a high priority within the intelligence community. As long as the intelligence community does not actively and aggressively address the void of threat information, senior leaders and managers will be reluctant to reallocate and re-prioritize resources for their agencies.

¹² Some of the services, such as the Air Force, do make reporting mandatory for computer intrusions. Most, however, do not compel systems administrators to report intrusions in the unclassified but sensitive network upon which 95% of DoD data/voice traffic is transmitted.

¹³ ".mil" refers to the suffix address for all DoD computer addresses. For instance, non-Defense Department addresses within government have a ".gov" suffix.

¹⁴ The practice of "looping and weaving" is extremely common to even the most rudimentary hackers. More structured computer attacks will regularly change the route of attack, and purposely go through institutions or nations where detection is unlikely. At all times the attacker is masquerading as a legitimate user on the coopted system.

- 17 -

'A common theme expressed by many experts was that there is absolutely no clear plan or direction as to how our nation should go about assessing the threat. While many individuals -- including the principals of our intelligence, enforcement and defense agencies -- agree the threat is significant, there is still no blueprint that might guide a national effort.

The counter-intelligence community suffers from similar problems. Since World War II, the common concern in the counter-intelligence community was the Cold War threat of spies and traitors photographing classified documents, or stealing information. Technical Surveillance Countermeasure (TSCM) agents are still looking for physical bugging devices that are planted in homes and offices. Undoubtedly, physical security is still a concern and needs to be a priority. However, it is clear that an equal threat arises in the virtual world where communication and information systems can be compromised remotely.

The law enforcement community has similarly been unable to adequately provide reliable threat assessments. Among non-Defense Department enforcement agencies, the FBI has dedicated the most resources to a computer crime program. However, results by way of arrests or even raw intelligence data have not been realized. Initially, the difficulty may have been linked to the Bureau's insistence that prosecutive or investigative decisions be premised upon quantifiable losses, or other indicia that normally factor into such decisions. Recently, however, the Bureau has begun to recognize that decisions to investigate cannot be premised upon traditional factors.

B. Lack of Detection and Reporting

1. Government

A major obstacle to assessing the threat posed to our information infrastructure is the failure of most government agencies to detect intrusions and, second, to report intrusions that are detected. As stated previously, the Defense Information Systems Agency (DISA) performs proactive vulnerability assessments of Defense Department computer networks. According to 1996 DISA's statistics, of the 18,200 systems they were able to penetrate, only 5% of the systems administrators actually detected the intrusion; and of the 910 system users that detected the intrusion, only 27% (246) reported it to a superior.

These statistics, which are limited to the unclassified but sensitive networks of the Defense Department, reflect how little is known about this problem. In its recent report released at a previous Subcommittee hearing, the GAO estimated that approximately 250,000 computer attacks were occurring each year at the Defense Department. Applying DISA statistics to these estimates, it would translate into 162,500 successful intrusions each year, with only a small portion begin detected and reported.

Having access to such a small sampling of this problem makes it difficult, if not impossible, to assemble reliable threat assessments. Furthermore, virtually every computer investigator interviewed by the Staff declared that they are detecting the least competent and most reckless hackers. As one investigator explained "we are only catching the bottom of the food chain, anyone with half a brain could elude our net with ease." Essentially, we are identifying mostly the unfunded, unstructured attacker.

The major reason computer intrusions are neither detected nor reported is that the Defense Department and most government agencies outside of DoD simply do not mandate that they be reported. If anything, there is a disincentive for systems administrators to report intrusions. Numerous personnel involved in computer security admitted that reporting a break-in, or even raising the issue of a potential security lapse, may "reflect negatively" on their job performance.

In addition, most of the government agency victims do not have the expertise and tools to detect an intrusion or attempted intrusion. The Air Force is in the process of installing intrusion detection tools on all Air Force bases over the next two-three years. The tool, ASIM¹⁵, captures all of the keystrokes of all of the users on the base network and automatically matches them against known hacker keystrokes. The system then analyzes the threat and rates its seriousness. In 1995, ASIM was deployed on 23 Air Force bases and discovered 2,332 incidents. Most agencies, however, appear to lack the resources or commitment to pursue such initiatives.

2. Private Sector

There is very little anecdotal data concerning the threat posed to the private sector. While much of the failure to report intrusions within government is due to an absence of interest, in the private sector it is due primarily to fear of the marketplace and of government. The Staff interviewed several security experts from commercial institutions, as well as various private individuals who provide computer security to commercial institutions that might be targets of computer attacks. The most common theme among those interviewed was that the commercial sector is loathe to report computer intrusions for fear of affecting customer or shareholder confidence. Company insiders confirm to the Staff that they have experienced intrusions on a regular basis, but fear reporting them to the government or other agencies that might ultimately report them into a public record.

One of the premier companies that provide security services, including countermeasures, to private industry explained the extent of this problem. This company informally surveyed a handful of other security firms about known losses from commercial or financial client-companies. This small group of firms was able to account for \$800,000,000 of losses last year alone worldwide. This figure included only actual losses reported by clients to these few firms. Over \$400,000,000.00 was attributed to U.S. companies. These figures do not include losses that might be attributed to damage to data, or temporary lost access to data, and it could not quantify unknown losses from competitive advantage (e.g..industrial espionage).

Despite the likelihood of substantial losses in the U.S., the FBI can only report a single substantial case where a financial institution lost money due to outside intrusion into a network. In the Citibank incident of 1994, Citibank lost \$400,000 to a group of hackers operating out of St. Petersburg, Russia.

The disincentive for an institution not to report a financial loss is obvious. For a financial institution, customer confidence is a staple for commercial viability. Lack of customer confidence in a competitor, similarly, is viewed as a competitive advantage in the marketplace. Publicity that exposes unauthorized intrusions into customer accounts could easily inspire customer insecurity which would have a bottom line effect on business. For instance, the Staff was advised by numerous and reliable sources that, after Citibank received publicity in 1995 for having been attacked, Citibank's top 20 customers were immediately targeted by six of Citibank's competitors. The competitors argued that their banks were more "secure" than Citibank's.

¹⁵ ASIM is a computer program, Automated Security Incident Measurement.

There are legal requirements that, in theory, should result in the reporting of intrusions. For instance, banks have to comply with certain regulations in the Federal Code relating to the suspicious disappearance or unexplained shortages of funds of \$5000 or more (12 C.F.R. 21) and there is a well-defined regulatory structure overseeing our nation's financial infrastructure. The Securities and Exchange Commission (SEC) also has reporting requirements for securities firms and publicly traded corporations. Virtually every bank officer interviewed by the Staff, although agreeing that they would never want to report losses and adamantly opposing more comprehensive mandatory reporting legislation, refused to acknowledge any non-reporting. A representative of the N.Y. Federal Reserve indicated that as part of their oversight of financial institutions, including 40-50 of the country's major banks, they were unaware of any attempted "cover-up" of a break-in.

As of April 1996, financial institutions are required to report suspicious activity to FINCEN (Financial Crime Enforcement Network). Failure to report can result in a \$5,000 fine. FINCEN collects the reports on a database located in Detroit. FINCEN has not yet received any reports relating reports of computer intrusions and is unaware of any fines for nonreporting levied prior to April 1996. A representative of the Federal Reserve Board also indicated he was unaware of any regulatory agency fining an institution for failure to file a criminal referral form. Although an institution might be fined for failure to report, a \$5,000 fine may be of little deterrent value as many companies privately advised the Staff that they will spend much more just to respond to an intrusion so that it does not become public.

The Staff, however, was advised by numerous information security professionals, that banks and financial institutions were not reporting computer intrusions. According to these professionals, commercial institutions may report losses, but not disclose the full nature of the intrusion. As one senior account representative explained, "there's reporting, and then there's reporting." The Staff learned that on many occasions corporate internal investigations of computer intrusions were conducted through the corporation's general counsel office, so as to provide a veil of secrecy that flows from the attorney-client relationship. Another method of avoiding scrutiny is to report an incident among a bulk of other documents such that discovery of the details of the computer attack is nearly impossible.

A related concern expressed by representatives of the private sector was the fear that reporting an intrusion to the FBI, or other law enforcement agency, would mean loss of control over the investigation. While the FBI is primarily interested in proving criminal misconduct and bringing perpetrators to justice, a corporation is more interested in stopping the intrusion with as little publicity as possible. These two goals become inapposite when a public trial is likely to result from a successful investigation. Thus, virtually all corporate representatives interviewed by the Staff expressed great fear of mandatory reporting of intrusions, even if they are criminal law violations.

A recent survey by the San Francisco-based association of information security professionals, Computer Security Institute (CSI), demonstrated the extent of corporate reluctance to report. The CSI, in coordination with the FBI, sent out 4,971 questionnaires to information security practitioners.¹⁶ Although the survey was anonymous, only 8.6% (428) were even willing to respond. Of those that responded, 42% admitted experiencing some form of intrusion within the preceding 12 months. Many of the intrusions were from remote dial-in sources and Internet connections. Over

¹⁶ The survey was sent to U.S. corporations, financial institutions, academic institutions and government agencies.

50% of those suffering intrusions believed they were from competitors in their marketplace.

The damage to the institutions varied. 36% of attacks reported by medical institutions and 21% of attacks report by financial institutions indicated they had data altered through these intrusions. Significantly, 83% of respondents to the survey indicated they would not advise law enforcement if they thought they had been victimized; over 70% cited fear of negative publicity as the primary reason for not reporting.

The Staff cannot overstate the effect under-reporting has on our ability to assemble a reliable threat assessment which would encourage management to re-align and reprioritize resources. Within the business community itself, a lack of reporting has been a barrier to implementing proper security to private networks. A top executive with a global securities firm advised the Staff that "without reliable data it is impossible to prioritize countermeasures."

There have been formal and informal efforts to assemble anecdotal information that might help private industry better equip itself for attacks on its information infrastructure. For instance, the National Security Information Exchange (NSIE) Subcommittee of the National Security Telecommunications Advisory Committee (NSTAC) is a group of company representatives -- mostly from the telecommunications industry - that meets regularly to share threats and vulnerabilities observed within their own companies. The NSIE maintains strict confidentiality agreements with its members¹⁷ in order to prevent exploitation of weaknesses by competitors or other bad actors. Members of the NSIE related to the Staff that it took a great deal of time before the members developed trusted relationships with one another.

C. The Potential Attackers

Is the bad actor a 16 year old cyber-joyrider, a well-funded foreign intelligence service, an anarchist, or an industrial spy? Does the threat come from a foreign or domestic source? Is the attack motivated by espionage, greed or a desire to create terror? Unfortunately, at any given time it can be any one or even a composite of the above. The threat to our information infrastructure is organic, evolving, and elusive.

Furthermore, while much has been reported about the threat posed to our information infrastructure from the outsider, virtually every security expert interviewed by the Staff agreed that, at least in the short term, the greatest threat to our infrastructure will come from the "insider." The insider is defined as the individual already possessing authorized access to a network. The Staff found that the basis of this fear was premised upon the difficulty in defending against the insider, and the great amount of potential damage an insider could accomplish.

The "hacker" has been traditionally perceived as the misguided youthful computer intruder who acts out of a perverse sense of adventure. Perhaps, best illustrated in the 1982 movie *War Games*, this individual has generally been viewed as an inconvenience and not a true threat to national security.

¹⁷ There are two NSIE subcommittees. One has 9 NSIE companies, the other 9 NSIE government agencies. The two NSIE subcommittees meet jointly. NSIE members are chosen by the NSTAC.

- 21 -

The hacker, even if a true generalist, is, nevertheless, a threat in every sense of the word. Misconduct motivated by curiousness or impishness can have a devastating effect on our infrastructure. For instance, the "Morris Worm" in late 1988 caused more than 6,000 computers to shut down. As indicated previously, even the most innocent hackers can become dupes for foreign intelligence services or other bad actors. In the Rome Labs case (see Appendix B) the 16 year old British hacker "Datastream" was actually seizing control of Defense Department computers at the direction of an unknown third party ("Kuji") who was directing him through chat sessions on the Internet. In the virtual world it is much easier for a foreign government to utilize a dupe because of the anonymity inherent on the Internet.

The National Security Agency has acknowledged that potential adversaries throughout the world are developing a body of knowledge about Defense Department and other government computer networks. According to DoD officials, these potential enemies are developing attack methods that include sophisticated computer viruses and automated attack routines which allow adversaries to launch untraceable attacks from anywhere in the world. In some extreme scenarios, studies demonstrate how our adversaries could seize control of Defense information systems and seriously degrade the nation's ability to deploy and sustain military forces.¹⁸ Official estimates reflect that more than 120 countries are developing offensive information warfare capabilities.

Additionally, it is likely that our vulnerability in this regard will only increase and at the current rate, countermeasures will never keep up with technology. Discussions with Defense Department officials indicate that there is a great desire and pressure to further interconnect all our defense components in order to create a seamless mosaic of information networks within our defense infrastructure. Undoubtedly, this will increase the efficiency and effectiveness of all aspects of the DoD mission. Unfortunately, it will also open that same defense infrastructure to foreign intelligence agents, and potentially disruptive forces.

The Staff received several briefings from national security officers who repeatedly expressed concern that the Internet and the easy exploitation of computer networks is providing other nations with opportunities to assemble intelligence information. In the Hanover Hacker case that was the subject of Cliff Stoll's best-selling novel, *The Cuckoo's Egg*, the German hackers were working for the Russian KGB and met regularly on a Bulletin Board System (BBS). Today, many Subcommittee sources have alleged that a certain foreign government sponsored a hacker bulletin board on which hackers exchanged data, including passwords and logon files, of foreign governments. This government apparently monitored the BBS activity obtaining the critical information for its own use. Clearly, if true, this illustrates how the Internet provides foreign nations with virtually risk-free intelligence services for little cost and almost no exposure.

In interviews with senior intelligence and counter-intelligence officers, the Staff has been advised that there is great concern that insiders will gain access to classified networks as well. Previously, in the physical world, our classified intelligence data was maintained in secure locations with physical barriers (doors, walls, guards, file cabinets) that served as a deterrent to loss of information. Even persons with access to a building could not gain access to certain documents, rooms and secure file cabinets. Only presumably trusted persons would have access to these areas and this information. The

¹⁸ The RAND Corporation, at the Direction of the Deputy Secretary of Defense, has sponsored a series of "info war games" designed to enhance our policy-maker appreciation of emerging infrastructure related issues. The series of exercises present mock info attacks and then the counter measures and decisions that must be made.

networking of classified computer systems within agencies, has created new vulnerabilities by giving network-wide access to insiders who previously may have had access to only a single classified system. As one senior intelligence officer explained to the Staff, "anyone on a network, from a clerk, to a guy on the other side of the building can peruse critical information without anyone knowing about it."¹⁹

This will become an even greater concern as the CIA and other intelligence agencies continue to link their internal systems together in order to enhance productivity and efficiency. The Staff recognizes that undoubtedly the advantages posed by increased connectivity will be to great to resist. However, connection without protection is a huge risk, and one that may well be minimized with a proper front-end security investment.

The threat from a subnational group, a terrorist organization, or a disaffected individual must also be considered. Recent incidents support the "softness" of U.S. target to physical attacks. The Oklahoma City and World Trade Center bombings, and the series of attacks by the Unabomber, support the proposition that individuals and small groups can do massive physical damage to our infrastructure. The same is clearly true in the virtual world of cyberspace. The Internet, from its inception, was intended to be robust, open and accommodating, emphasizing trust, and not security.

Perhaps more frightening than any threat we are presently familiar with, is the threat we will face in the future. Although the growth of our information infrastructure has been dramatic, most experts agree it is only the beginning of what will be continued growth and dependency. Technology is advancing and multiplying, as computers become quicker and more versatile. There appears to be no limit on the potential expansion of networks and users.²⁰

Along with increases in technology, will come a maturation of a generation of potential bad actors. Many national security experts advised the Staff that it is likely that foreign nations will view information attacks as a cheaper and relatively risk free alternative to conventional intelligence gathering. Furthermore, given our nation's increasing dependency on information networks, foreign adversaries will find it easier to damage our infrastructure. To what extent our nation will be able to defend against this threat in the future is unknown, but clearly more attention must be paid to it today.

IV. EFFORTS TO PROMOTE INFORMATION SECURITY

The difficult task of promoting the security of our information infrastructure was aptly explained in the recent interim report of the Justice Department-led Critical Information Infrastructure Working Group:²¹

¹⁹ A good example of this enhanced vulnerability is seen in a review of the Aldrich Ames spy case. Ames, though attempting to steal classified information, was a computer illiterate and unable to perform even the most basic "download" functions on a computer. Therefore, he had to take home hard copies of documents and retype them. Had he been able to download onto computer disks, or access files throughout the CIA's database, the damage to our national security would have been even greater.

²⁰ The use of fiber optic cables will provide virtually unlimited room for Internet traffic. Presently only a small percentage of optical capacity is being used.

²¹ The Critical Infrastructure Working Group ("CIWG") was created in the wake of Presidential Decision Directive 39 which clarified U.S. Policy on Counter terrorism. Although classified in its original form, an unclassified version is attached as Appendix C. PDD-39 tasked Cabinet-level officials with reviewing the vulnerability of government facilities and critical

Assuring critical national infrastructures is a difficult problem to solve, not only because of the breadth of the infrastructures, the varied nature of the threats, and the multiplicity of sources of threats, but also because of the differences in perspective among the relevant government agencies and between the government and the private sector. The Defense community naturally is focused on protecting and ensuring the viability of those elements of the infrastructures vital to the defense mission. Law enforcement is responsible for preventing, investigating and prosecuting terrorist and other criminal acts against the infrastructure. The Intelligence Community also has a preventive mission, but is limited to looking at foreign based threats. Yet for cyber attacks in particular, it is often difficult to determine whether the source of an attack is foreign or domestic.

Addressing this threat becomes even more difficult when recognizing that a desire to gain a competitive advantage may give private industry a different, and even opposite, motive to government. Furthermore, our national effort dedicated to securing our information infrastructure is a disjointed mosaic of agencies, private enterprises and individuals each trying to provide services that enhance our infrastructure. To which agency do you task responses to computer attacks when the identity, location and motivation of the attacker is often unknown? What apparatus can be created that will foster confidence in the private sector in lieu of the documented distrust of government involvement in this area? How do you create threat estimates when reporting and collection of data is sparse and hidden throughout government and the private sector?

A. Creation of a National Policy

A substantial obstacle confronting efforts to secure our NII is our nation's failure to adopt a national policy that defines roles and missions of agencies and provides national strategies that are clearly articulated and implemented. Presently, a patchwork approach has evolved that is uneven and lacking direction. In March of 1996, the Justice Department-led Critical Information Working Group ("CIWG") circulated two proposals to address these concerns.

The first proposal was to create a full-time Task Force within the Executive Office of the President to study infrastructure assurance issues and recommend national policy. The CIWG recommends that the Task Force be headed by a presidential appointee from the private sector and be comprised of full-time representatives from affected agencies. The Task Force, as primarily a policy body, may also utilize advisory boards, including pre-existing bodies or created ones. The CIWG estimated the Task Force would need a year to complete its mission.

In the interim, the CIWG recommends establishing a single interagency coordinating group within the Department of Justice, chaired by the FBI, to handle the interim infrastructure assurance mission with regard to both physical and cyber security. The primary purpose of the group is to facilitate a more rapid and coordinated response to threats to our national infrastructure and to facilitate access to the diverse and fragmented resources already dedicated to the mission of securing that infrastructure.

national infrastructure. As a result, Attorney General Janet Reno convened a working group, chaired by Deputy Attorney General Jamie Gorélick and various other officials, to scope out the issue and report back to the Cabinet with policy options. The CIWG's interim report was completed in early February 1996, and has not yet been released.

- 24 -

As a starting point, most experts the Staff consulted, in government and private industry, supported both these concepts in some form. More than a few officials in both the Defense and Intelligence communities, however, expressed concern that assigning leadership of the Task Force to a representative from the private sector was essentially ceding national security to the business community. More than a few commentators also emphasized the need to make sure the group sustained White House interest in this effort.

Regarding the interim coordinating group, experts disagreed. One concern voiced by a senior Defense Department official was that the operational coordinating group was really not operational, but merely a human referral service that lacked all capability to perform "real-time" analysis and response. One former Justice Department official indicated that even if the interim group fails to actually perform any operational response, it will at least serve as "a laboratory" for the policy board to observe the difficult obstacles to meaningful coordination. Finally, some concern from other participating agencies was raised as to whether the FBI would be able to serve in the role of "honest broker" in this effort. The CIWG acknowledged that the FBI "has been criticized for failing to share information with other agencies."

The Staff would further note that how the interim group relates to other efforts must be defined immediately. How will the interim group, which seeks to have an operational, 24 hour response team, work with the NSA's "thousand person" info warfare center that also has its own 24 hour response capability? Furthermore, will the interim group, which is led by the FBI, treat each intrusion as a criminal case and limit the intelligence community's access to critical intelligence data?

Ultimately, there exists a great need to begin examining this issue from differing perspectives and the CIWG proposals serve as a good beginning point. The Attorney General and Deputy Attorney General, as well as the principals and staff working on this project, deserve a great deal of credit for addressing this difficult challenge.

B. Current Law Enforcement Response

Presently, only a handful of law enforcement agencies have committed meaningful resources to computer crime investigative programs. The FBI, the Air Force Office of Special Investigations (AFOSI) and, to some extent, the U.S. Secret Service have made this commitment on the federal level; with the exception of a few local agencies -- Baltimore County Police Department and the Florida Department of Law Enforcement (FDLE) -- the local law enforcement community has not acknowledged any need for specialized computer crime investigators.²² The lack of resources, even in the agencies that have made a commitment, severely limits the operational capability of the law enforcement community. The FBI and AFOSI²³ can only investigate a handful of cases simultaneously.

Part of the reason for the limited commitment of law enforcement resources has to do with the unique nature of the evidence and the technical expertise necessary to

²² Virtually no state or local law enforcement agency has attempted to develop an expertise in computer forensics, and only a handful have the expertise and capability to conduct a computer intrusion investigation.

²³ The FBI has a computer analysis and response team located at FBI headquarters in Washington, D.C. with 51 full time agents and forensic technicians; the AFOSI has 68 full time agents, technical support, and forensic technicians at 12 different Air Force bases worldwide.

- 25 -

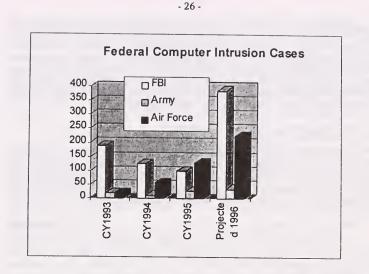
Present law makes it extremely difficult to monitor computer attackers to determine an attackers' origin and identity. Data transmits over electronic communications systems and, therefore, any attempt to monitor the text of transmissions is considered a Title III wiretap.²⁴ Because attackers use "loop and weave" techniques that allow them to transmit over numerous systems in various places, a court ordered wiretap is necessary for each computer system that is being used no matter its location. Computer programs exist that permit you to automatically "hack back" to find the original source of the attack; however, use of this "hot pursuit" technique in cyberspace is difficult if not impossible because current law does not permit government agents to break into unknown computer systems.²⁵

Numerous law enforcement professionals have confirmed to the Staff that these resource constraints limit their ability to respond to the needs of victims. The Staff was advised by a security professional from a major financial institution that there exists a feeling that federal law enforcement is not equipped to respond with the resources and, equally important, the necessary technical expertise. In the Citibank investigation the victim-bank initially took their case to a private security firm and only after the investigation had been completed successfully was it referred to the FBI.

Statistics on the number of criminal investigations of computer intrusion incidents are difficult to assemble because most agencies lack mechanisms to extract that information from their investigative databases. The Staff did obtain from the FBI, Air Force Office of Special Investigations and U.S. Army (Military Intelligence and Criminal Investigative Division) their statistics since 1993. The FBI had shown progressive decline in cases until this year. This may be because the Bureau appears to be more willing to open cases without knowing the actual damage and loss. If true, this would be a dramatic turnaround from just 10 years ago when the Bureau was unwilling to even investigate cases absent substantial and quantifiable loss.

²⁴ Federal law governing wiretaps authorizes the use of Title III wiretap only with the consent of the Deputy Attorney General and only after a complex process that can take up to weeks to complete. Furthermore, wiretaps are usually only permissible on specific communication ports in specific geographical areas.

²⁵ The fact that hackers often traverse national boundaries and use foreign government computer systems to launch their attacks further complicates the use of an electronic "hot pursuit." How would our nation explain to an un-friendly nation why U.S. government agents hacked through a foreign government's computer system?



C. Private Sector Response

The lack of confidence in a government or law enforcement response has created a demand in the private sector for services related to information system security. The Staff has attended numerous meetings of corporate security officers who uniformly explain that when confronted with a computer incident -- even if clearly criminal in nature -- they will not go to the FBI, but rather hire a private security firm. In their estimation, these firms offer a greater likelihood of success than the government, as well as the added advantage of confidentiality.

These "cyber-posses" are growing as computer attacks become more prevalent and the demand for security services increase. Unfortunately, private security firms have more incentive to stop intruders than to catch them and ensure they are prosecuted. A few representatives of security firms mentioned that often their clients merely want them to advise the perpetrator that they have been discovered and that they should go elsewhere. An equal number of corporate security officers explained that it was company policy to simply send the attacker back into the marketplace, hopefully "to attack our competitor down the street." Additionally, these security firms may not feel obliged to conform their conduct to applicable laws. For instance, more than a few firms indicated that they have considered "offensive counter-responses."²⁶

Further, as mentioned earlier, the incidents handled by private firms rarely make it on to the government's "radar screen" or intelligence database. Accordingly, any intelligence advantage that might be gained by having access to known anecdotal data is lost. For instance, there would be great utility in knowing e-mail addresses of would-be hackers or their techniques and the vulnerabilities they exploit.

²⁶ Not only would such conduct likely be illegal as it is an unauthorized intrusion into another system, but given the widespread use by hackers of unknown third-party systems to launch attacks, it is possible the counter-attack would damage or destroy an innocent party's computer network.

- 27 -

Finally, the great success of these security firms reflects a similar failure in our government to create a pool of able professionals dedicated to computer security. It has become commonplace for government agencies involved in information security to lose their best and brightest personnel to private firms engaged in the same type of mission. While there is nothing wrong with a natural migration of civil servants to the private sector, numerous persons within government and in the private sector have acknowledged that the "brain drain" of government experts to private industry seriously hampers our government's ability to respond to computer attacks.

D. Computer Emergency Response Team (CERT)

The CERT program first began in the aftermath of the 1988 Morris worm incident in which a dangerous "worm²⁷" program was released onto the Internet. The incident effected over 6,000 machines across the country. According to the United States General Accounting Office, damage caused by the worm could have reached \$96,000,000 due to lost access to the Internet at each infected host.

In response to this and a seemingly continuous stream of security-related incidents that were affecting thousands of computer systems and networks, in November 1988 DARPA (Defense Advanced Research Program Agency) established the Computer Emergency Response Team, now known as the CERT Coordination Center, located at the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, Pennsylvania.

The CERT Coordination Center is chartered to work with the Internet community to facilitate its response to computer security incidents or events²⁸. The CERT mission is to provide a 24-hour point of contact for emergencies; facilitate communication among experts working to solve a computer security problem; serve as a central point for identifying and resolving vulnerabilities in computer systems; maintain close ties with research activities and conduct research to improve the security of existing computer systems; and to take proactive steps to raise the understanding of information security and computer security issues.

The CERT Coordination Center, according to many experts in the field, is responsible for increased awareness of computer network vulnerabilities. Many government agencies have formed their own version of the CERT to coordinate the handling of security incidents, and to act as a focal point for security related activities inside their agencies.

CERT Coordination Center officials told the Staff that when they respond to an "event," they advise the victim of a few options: simply turn off the system and fix the problem; hire a security contractor in an attempt to identify the intruder; report the incident to an appropriate law enforcement agency; or do nothing. The CERT representatives indicated that very few agencies they respond to have internal policies that guide them in choosing a response. The types of incidents CERT officials respond to include everything from corporate espionage to vandalism to profit-motivated criminal

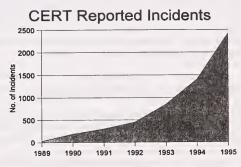
²⁷ A "worm" is a program that is designed to copy itself over a computer network. Unlike a virus, it does not erase files on the computers that it invades, but it creates so many running copies of itself that it overloads and breaks down computers.

²⁸ The CERT Coordination Center defines an incident or event as some form of unauthorized access into a computer system.

conversion. Although the CERT has handled thousands of cases, only a few were actually referred to law enforcement authorities.

Most of the calls, the Staff was told, are from mid-range systems administrators. The callers are usually in a state of panic, resulting from their lack of training. A problem that is observed with great regularity is the inability of systems administrators to even understand security countermeasures and repairs. Clearly, there needs to be better security tools developed that would make systems easier to secure and maintain.

CERT officials told the Staff that the number of computer security incident grows as fast as the number of hosts on the Internet. When the CERT Coordination Center was established, the Internet had approximately 80,000 hosts. Since then, the Internet has grown to more than 9.5 million hosts. Each year the CERT Coordination Center has seen dramatic increases in the number of security incidents. In 1988 there were only 6 reported incidents reported to the CERT Coordination Center. In 1995, there were 2,412 incidents. During the first half of 1996, CERT closed 350 cases and opened 500 new ones.



The CERT Coordination Center coordinates and shares information with 50 other response teams. These teams consist of private security firms, corporate-sponsored teams and teams put together by foreign nations. Additionally, the CERT issues vulnerability reports to the public and most of the vulnerabilities they discover are taken directly to a vendor for a fix.

Ultimately, the CERT program is probably one of the best responses available. Unfortunately, the CERT's impact is constrained by their resource restraints and limited ability to respond as needed. Recently, the Staff learned that the DARPA was, in fact, cutting the CERT's budget by 75% from\$2,000,000 per year for incident response to only \$500,000. The money cut will be redirected to research and development for computer security.

E. Encryption and the NII

There has been much discussion among the computer security industry about the use of encryption technology to secure the confidentiality of data contained in information systems. Encryption, a type of cryptography, is the process of scrambling information to preserve its confidentiality. Through the use of mathematical algorithms, data is scrambled so that its interception is useless to anyone lacking the "key" to decipher it. Encryption has many purposes including the authentication of computer files and the protection of electronic communications. Some encryption may be broken without the decryption key through computer programs or other techniques that decipher the scrambled codes. Unbreakable encryption are scrambled codes that are so complex that they presumably cannot be deciphered and, therefore, preserve the confidentiality of the subject data.

There is uniform agreement between government and the private sector that strong cryptography is critical to protecting our National Information Infrastructure. Much of the data that flows on the NII -- personal communications, financial and commercial transactions, health care -- must necessarily remain confidential. The present debate is not on the need for encryption, but rather who controls the decryption keys.

The private sector almost uniformly demands that there be robust encryption available to the marketplace without government controlling the decryption key (private key escrow). Many parts of our government, including our Executive Branch, conversely believe that making unbreakable encryption available publicly, without government access, will run afoul of public safety concerns by providing organized crime, foreign intelligence agents, terrorists and other bad actors with a confidential method by which to communicate. Some experts have argued unsuccessfully for a standard unbreakable encryption with the government possessing the key in escrow (public key escrow). Though not adopting a public key escrow regime, the U.S. government presently outlaws the export of strong cryptography under arms export laws. Private industry believes export controls disadvantage U.S. companies because unbreakable encryption is already available world-wide despite our government's best efforts.

Recently, a Committee of the National Research Council published a report on encryption standards wherein it recommended that federal policy promote widespread commercial use of encryption technologies. The Committee recognized that such a policy would add to the burden of law enforcement and the intelligence community, but as Committee Chairman Kenneth Dam explained "...the many benefits to society of widespread commercial and private use of cryptography outweigh the disadvantages."

This Subcommittee has a long history of examining both international terrorism and organized crime.²⁹ Undoubtedly, the law enforcement and intelligence communities raise valid questions as recent history has proven that criminals are quick to rely on anonymous, mobile and untraceable methods to communicate. The digital pager and cellular phone industries, for instance, have revolutionized the drug trade, replacing the pay phone as the preferred method of communication. To what extent the use of encryption will become a standard *modus operandi* for criminals, terrorists and other bad actors is a question that must be answered. We are already seeing examples of how encryption can be used to facilitate misconduct.³⁰

Despite our best efforts, however, free encryption is publicly available on the Internet, so everyone now has the capability to encrypt communications in such a manner to thwart current law enforcement or intelligence surveillance court orders.

²⁹ For instance, see Permanent Subcommittee on Investigations hearings, Security in Cyberspace, May 22, 1996; Global Proliferation of Weapons of Mass Destruction: Part 2, March 13, 20, 22 and 27, 1996; Global Proliferation of Weapons of Mass Destruction: Part 1, October 31 and November 1, 1995; and International Organized Crime and Its Impact on the United States, May 25, 1994.

³⁰ Ramzi Yousef, an alleged mastermind of the World Trade Center Bombing, and currently on trial for a plot to destroy U.S. airliners, used encryption to store information about their terrorist plot.

Ultimately, however, the utility of promoting some form of public key encryption regime must be addressed.

F. NIST and NSTAC

1. National Institute of Standards and Technology (NIST)

The 1987 Computer Security Act assigns the Commerce Department through the National Institute of Standards and Technology (NIST) the responsibility for developing security standards and guidelines for sensitive information in government computers. Although NIST's mission specifically exempts classified networks and systems related to national security (such as Defense Department networks), NIST works closely with the National Security Agency (NSA) which is responsible for classified computer security policy and guidance. NIST conducts research and studies to determine the nature and extent of the vulnerabilities of sensitive information in federal computer systems. NIST is also authorized to submit the standards it promulgates to the Commerce Secretary, who can then make them compulsory. NIST has utilized this process to create the Federal Information Processes Standards program or "FEPS" which forwards standards to computer users throughout government.

Although NIST is responsible for establishing standards, NIST advised the Staff that there is no one responsible for enforcing or ensuring that standards are complied with. Furthermore, NIST does not deal with all aspects of computer security.

2. National Security Telecommunications Advisory Committee (NSTAC)

President Reagan created the National Security Telecommunications Advisory Committee (NSTAC) by Executive Order 12382 in September 1982 in order to provide advice and information, from the industry perspective, to the President and the Executive Branch regarding policy and enhancements to national security and emergency preparedness in the telecommunications field.

The NSTAC, working jointly with the Government, is addressing numerous issues relating to the security of various aspects of the telecommunications field, including wireless services, network security, information assurance, and telecommunications legislation.

The NSTAC's committee produces technical reports and recommendations to the President. The NSTAC is an excellent model exhibiting the cooperation between the private sector and the government working together on serious national security and preparedness issues. However, NSTAC only focuses upon the telecommunications industry which is but one part of the NII.

G. International Efforts to Promote Information Security

The vulnerabilities of our NII are greatly enhanced by the international dimension of this threat. By its very nature a computer attack is initially a puzzle: the number and identity of intruders is not knewn; the origin of the attack – whether foreign or domestic -- is impossible to determine; and the motive of the incident is often a mystery. Furthermore, through use of basic methods of "looping and weaving" computer attacks may be extraordinarily difficult to solve. Unfortunately, the international community has been very slow to respond to this situation.

- 31 -

Computer "crime" laws are only now beginning to emerge in other nations. Whether as privacy offenses (data protection), or economic crimes (computer manipulations, sabotage, hacking, espionage and piracy), few countries are developing comprehensive legal codes to address this new type of misconduct. Furthermore, there is no global consensus on what constitutes computer crime. The United Nations Manual on Computer Crime, states:

Laws, criminal justice systems and international cooperation have not kept pace with technological change. Only a few countries have adequate laws to address the problem, and of these, not one has resolved all of the legal, enforcement and prevention problems.

This vacuum, internationally, has made it easier for bad actors to attack our National Information Infrastructure.

For instance, in March of 1996, the Justice Department issued a 23-page press packet announcing "Federal Cybersleuthers Armed with First-Ever Computer Wiretap Order Net International Hacker." The hacker the Justice Department was referring to was 21-year old Julio Cesar Ardita of Buenos Aires, Argentina. Mr. Ardita was indicted for breaking into Harvard University's computers from Argentina, which he then used as a staging point to crack into numerous computer sites, including Defense Department and NASA computer systems. This case was noteworthy because it was the first time the Justice Department had used court-authorized nonconsensual monitoring on a computer network.

Despite the commendable investigation done by the Navy and the FBI, there is virtually no chance that Mr. Ardita will ever see the inside of a U.S. court because our extradition treaty with Argentina does not recognize the computer crime he has allegedly committed.³¹ Even more discouraging is the fact that his alleged conduct, though clearly victimizing the U.S., is likely not even a crime under Argentinean law. Essentially, even after his indictment in the U.S., Mr. Ardita could continue committing the same offenses with little chance of prosecution or punishment.

In addition to extradition conventions, there is little harmony internationally in the area of computer crime and investigation. Substantive law that might set forth generally accepted computer crimes is undeveloped in many nations, and even the act of unauthorized access to computers is not a crime in all nations. Procedural laws, such as extradition, letters rogatory and other transnational tools, are similarly of little help.

Furthermore, the current organizations established to provide for transnational assistance -- such as Interpol -- have been unable to adequately keep up with the rapid advances of potential bad actors. A high ranking official with British law enforcement advised the Staff that calling Interpol for assistance in other countries is "hit or miss, with more misses than hits."

There are a few nations, mostly in Europe, that are attempting to organize the community of nations to address this problem. Great Britain, Germany, Denmark and the Netherlands have all recognized the need for a global response. Furthermore, the need to form global alliances in combating this problem has recently become apparent to some international organizations.

³¹ A "lookout" has been placed for him with Interpol should he travel to the U.S. or a country outside of Argentina that permits extradition.

- 32 -

The Organization for Economic Co-operation and Development (OECD) adopted guidelines for information systems security in late 1992. The OECD is comprised of 24 countries in North America, Europe and the Pacific. The OECD recommended the harmonization of rules on extraterritorial jurisdiction as well as the review of domestic law to determine the ability of member countries to adequately address trans-border offenses.

Interpol sponsored its first computer crime investigative working group meeting in Lyon, France, in May 1996. Other efforts include NATO's *Lathe Gambit* which brings together European computer crime investigators, military investigators and intelligence communities. The International Association of Chiefs of Police has also recently become interested in transnational computer crimes. Although the advances made in the international community are commendable, much more is needed.

V. STAFF RECOMMENDATIONS

The need to establish a comprehensive plan within which to address the vulnerabilities of our National Information Infrastructure (NII) is paramount. Whether through a White House-led Task Force or some similar mechanism, the interdisciplinary nature of this threat requires a government-wide response that also addresses the exposure of the private sector.

The U.S. must formulate national policy to promote the security of its information infrastructure.

Presently, agencies are greatly limited by pre-existing missions and jurisdictional assignments. Unfortunately, the threat ignores national boundaries and often remains a mystery until it is fully investigated. Based upon the multidimensional nature of the threat posed to our information infrastructure, there exists a need to establish a freestanding entity that can conduct operational responses to computer attacks, and task different agencies within our government.

The Staff recommends the creation of a National Information Infrastructure Threat Center that will include representatives from the law enforcement, intelligence and the Defense communities, as well as liaison with the private sector. This center should have "real time" 24 hour operational capabilities as well as serve as a clearinghouse for intrusion reports.

No intelligence, counter-intelligence or law enforcement agency has yet produced an NII threat assessment. More importantly, the intelligence community is having difficulty collecting the data necessary to even prepare such an estimate. Collection of data must become a high priority within the intelligence community.

The Staff recommends that the Director of Central Intelligence complete an NII threat estimate. The estimate should have an unclassified version that can be made available to private industry.

The uneven response in the international community to the threat posed to information infrastructures has created difficulties enforcing anti-intrusion legislation. Only a handful of countries presently have meaningful computer crime investigative capability, and the absence of uniformity has given would-be attackers refuge from detection or prosecution.

- 33 -

The Staff recommends that the U.S. promote the creation of an international computer crime bureau with emergency response capability. This Bureau may be assigned to Interpol and would provide education and awareness training to foreign law enforcement agencies in order to promote the creation of dedicated computer crime units or similar capability as well as uniform investigative and computer forensic practices. This Bureau would also have operational response, like a CERT, in support of computer crime incidents. The Bureau would also collect data on vulnerabilities and disseminate countermeasures as well as serve as an international clearinghouse for intrusion incidents.

Our government must foster a security culture that appreciates the vulnerabilities of our National Information Infrastructure (NII). We need to maintain a better pool of security professionals and, generally, improve the security consciousness of our users and our managers. There are several specialties in the computer career field for government employees including computer operators, computer technicians, computer programmers and computer analysts. There is no specialty in the computer career fields for network administrators, computer security personnel, nor in the criminal investigative career field for computer crime investigators.

> In order to ensure that computer security positions are filled with personnel that possess the requisite experience and training the Staff recommends the creation of a Government Computer Security Specialist Career Field that will include potential for career progression and incorporate specialized computer security training.

> In order to promote a stable pool of information security managers within the U.S. government, the Staff recommends the creation of a Government Computer Systems Administrator Career Field that will include potential for career progression and incorporate specialized computer security training.

In order to promote and improve our government's computer crime investigative potential, the Staff recommends the creation of a Government Computer Crime Investigators Career Field that will include the potential for career progression and specialized computer crime investigation training.

Vulnerability testing and assessment of government and government interest computer systems is the best method of enhancing awareness of the vulnerabilities of our information infrastructure. Presently, only the Defense Department has an aggressive vulnerability program.

The Staff recommends that the federal government promote regular vulnerability assessments, or "red teaming," of government agencies, especially agencies outside of the Department of Defense. The Staff further recommends that an agency be designated to perform such vulnerability assessments in the same manner that the Defense Information Systems Agency (DISA) perform such assessments for the armed services.

One of the most significant voids in computer security is the lack of reporting of attempted and even successful penetrations of government systems as well as other systems of national interest. Mandating the reporting of intrusions in government systems will foster a greater security culture with the NII. Further, it is important to give private industry a mechanism within which it can report intrusions without fear of inciting customer insecurity.

259

The Staff recommends that the U.S. government mandate the reporting of intrusions and attempted intrusions in all government and government interest systems. The Staff further recommends that federal agencies develop protocols and procedures for reporting computer intrusions, and subsequent referral of same to proper criminal or other appropriate agencies like the proposed National Information Infrastructure Threat Center.

The Staff further recommends that the federal government encourage private industry and the private sector to report intrusions into private information systems. The Staff would further recommend that the government promote private industry reporting through creation of anonymous clearinghouses or similar methods.

Logon warning banners that advise users of government computers that there is <u>no</u> expectation of privacy, though recommended by the Department of Justice, are not mandatory on government computer networks. The logon banners put users on notice that they have no reasonable expectation of privacy on government systems and the use of the system constitutes consent to monitoring. Presently, when intrusions occur on government systems, lack of such a logon banner hampers investigative efforts and response.

The Staff recommends logon warning banners become mandatory for all government and government interest systems. (See Appendix D for example of logon banner.)

#

Computer Terms and Definitions

"Attack". The act of trying to bypass security controls on a computer system, resulting in an attempted penetration or an actual penetration. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on a vulnerability of the system or activity and the effectiveness of existing countermeasures.

"<u>Audit trail</u>" is a chronological record of computer system activities which saved to a file on the system. The file can later be reviewed by the system administrator to identify users actions on the system or processes which occurred on the system. Because audit trails take up valuable disk space and can slow the computer system down, many system administrators do not use them or use only limited ones.

"<u>Bulletin Board System</u>" or "<u>BBS</u>" is a computer set up by individuals or companies that can be connected to by using a modem and dialing the telephone number of the BBS. There are thousands bulletin board systems in the United States offering a wealth of information to its users. Some and public domain software than can be downloaded.

<u>Crash.</u> A computer system or program is said to "crash" when it has become inoperable because of a malfunction in the equipment or the software. Causes include power loss, bad software code, or a computer process that conflicts with the system or other processes and causes the system to "lock-up." Hackers can cause systems to crash either by accident or on purpose by initiating certain commands or by installing incompatible programs to the system.

"<u>Cyberspace</u>" is the virtual world of computer networks that can be explored by anyone who has a computer and modem. Individuals can "go" to computer systems all over the world and communicate with other computer users.

"<u>Daemon</u>" (pronounced demon), is a program that maintains or performs certain computer tasks or functions such as the printing of files, monitoring of incoming traffic, or outbound communication services.

<u>DISA</u>. Defense Information Systems Agency (DISA), previously called the Defense Communications Agency (DCA), provides communications and computer services, guidance, policy and direction for DOD. In 1991, the Assistant Secretary of Defense for Command, Control Communications and Intelligence tasked DISA to establish and manage a unified, fully integrated information systems security program for the Defense Information Infrastructure (DII). The Defense Information Systems Security Program (DISSP) was then established as a joint effort of DISA and the National Security Agency.

<u>CISS</u>, The Center for Information Systems Security, which executes the DISSP's missions and functions, has the responsibility to provide a unified information systems security policy and architecture.

Within the CISS is the Information Systems Security (INFOSEC) Countermeasures Directorate. This directorate is charged with several programs, one of which is the Automated Systems Security Incident Support Team known as <u>ASSIST</u>.

DISA's <u>ASSIST</u> is an integrated DoD operational response capability for handling information systems security incidents, attacks and threats to DoD-interest automated telecommunications systems. ASSIST provides telephonic, on-line, and on-site support 24 hours a day, 7 days a week, 52 weeks a year. ASSIST activities include assessing the nature and extent of any damage to systems, helping site systems administrators faced with an incident faced with an incident contact

APPENDIX A

other key technical resources (when appropriate), coordinating (with both DoD community and vendor) technical efforts to develop and collect software patches, providing a source of verification for information pertaining to incidents and also for "patches", and advising site personnel on how to perform damage control and recovery procedures. ASSIST creates a single reporting point to reduce redundant reporting and encourage reporting through training programs, awareness newsletters, and a state-of-the-art electronic bulletin board system. ASSIST, staffed by computer security engineers, scientists and specialist, provide a level of technical assistance sufficient to address the technical problems created by almost any incident that a DoD site could encounter and then restores the site to secure operation in as short as time as absolutely possible. ASSIST is the primary technical tool supporting the DoD and Federal law enforcement communities. Recognized expert witnesses, ASSIST provides the technical perspective to investigations involving DoD-interest automated information systems.

"Denial of Service" is action or actions that result in the inability of an automated information system or any essential part to perform its designated mission, either by loss or degradation of operational capability. Denial of service can impact productivity. Costs associated with it are based on the length and time of day the denial of service occurs.

"Finger" is a computer network command which allows the user of the computer system A to identify a user from computer system B who is logged onto computer system A. The command can be "turned off" or disabled by the user of the computer system B so that if anyone executes the "finger" command to identify them, they are invisible to it and cannot be identified.

Firewall is hardware or software systems that protect an internal network from unauthorized intrusions from the outsider or to prevent insiders from exceeding their authorization.

<u>Hacker</u>. The dictionary defines "hacker" as a slang term describing a person who carries out or manages something successful. A hacker is someone who spends many hours with the computer often successfully operating it by trial and error without first referring to the manual. A hacker is often a technical person in the computer field, such as assembly language programmer or systems programmer. Today the term hacker has taken on a negative meaning. The news media has often used the term hacker in a derogatory manner to refer to people that use their technical knowledge to gain unauthorized access and perform mischievous or destructive activity in computer systems and data banks.

Internet. The "Information Superhighway" or its formal name of the "Internet" is a worldwide entity that cannot be easily defined. The beginnings of the Internet date back to 1969, when DoD's Advanced Research Projects Agency (ARPA), formed the ARPANet. This early network was limited to military entities, military contractors and educational users with UNIX computers linked by leased telephone lines. A main aim of ARPANet was to maintain military communications during disruption of telephone service during nuclear attack. This accounts for the Internet's high degree of redundancy and low degree of centralization. If one communication link between two sites was unavailable, the computers would try other routes to see if an alternate way could be found to deliver a message. Due to the number of different routes between computer centers and how duties are spread among them, there is no "center" or "top" of the Internet. Each computer site is an independent entity, but follows guidelines established by national and international committees. With the exploding growth in personal computers and commercial bulletin boards offering Internet access for a small monthly fee, anyone who has even the most basic computer and a modem can use it. In 1988 the Internet consisted of approximately 33,000 host computers and by the end of 1993 has expanded to over 1.8 million. There are approximately 20 million computer users worldwide who can communicate via the Internet, and one million new users hook up each month.

"Logic Bomb" is a computer program that lies dormant for a period of time in a systems and is triggered by an event, such as a date.

"Logon Warning Banner". As a means of legal warning, immediately after all users enter a logon and password the very first thing a computer system will often present is a paragraph of information known as a Logon Warning Banner. Generally, the banner will contain information

2.

APPENDIX A

which tells the user what computer system they have logged into and who owns it, any restrictions on the use of the system, and whether or not users and the information they process on the system are monitored. By regulation, all DoD and DoD interest computer systems are required to have a "logon warning banner" which advises the user at logon that they have logged into a U.S. government computer system, that use constitutes consent to monitoring of the user and their activities, use is limited to official purposes only, and what level of information may be processed on the system. Additionally, the warning banners often admonish that violation of the system by either an authorized or unauthorized user (hacker) subjects the violator to criminal prosecution. Although required, the warning banners were not present on all of the DoD and DoD interest computer systems SUBJECTS entered.

"Looping" is a method in which hackers try to conceal their point of origin. Using this technique, hackers "leap frog" or loop through several computer systems before finally going into the system they actually intend to attack. The technique serves to mask the hackers actual origin from the system that is being attacked as well as those pursuing them. Additionally, hackers will often ensure the routing their looping takes them crosses them across international and state borders. Any time a border is crossed electronically by hacker they have as good as crossed it physically, and has involved another country's or state's laws and law enforcement agencies. This further complicates and slows down efforts to pursue the hacker.

"NII", National Information Infrastructure The NII refers to that system of advanced computer systems, databases, and telecommunications networks throughout the United States that make electronic information widely available and accessible.

"<u>Password</u>" is a protected word or string of characters that identifies or authenticates a user for access to a computer system, or a specific resource such as data set, file, or record.

"<u>Phreaking</u>" is the hacking of the telecommunication systems. Phreaking is a specialized subset of hacking. It is spelled with PH for PHONE.

"Root" or "System Administrator Privileges" are terms used to describe a particular degree of trust and privilege on an operating computer system. When logged in to a computer system as "root" or "system administrator," the computer regards the user as "God," allowing them to do absolutely anything they desire. The privileges granted extend from simply looking at any file the computer system controls or has access to, moving any of its files anywhere desired, loading other data or executable program files on the system, to destroying and all files under it's control including it's own operating system. Needless to say, "root" or "system administrator" privileges are reserved for a very select few system users who are responsible for the configuration, maintenance, and upgrade of the computer system and it's file structure.

"Security Class C-2" In layman terms, C-2 requires the installation of certain security tools, audit trails and the implementation of procedural security practices which improves computer security and limits the vulnerability of the system to external attack and limits use to only authorized users. A technical definition would include a security testing standard established under The National Computer Security Center's (NCSC) Trusted Computer System Evaluation Criteria (TCSEC). The TCSEC was created as a metric against which computer systems could be evaluated. Security Level C-2 is basically comprised of system documentation defining a system protection philosophy, mechanism and system interface operations. Security level is basically defined as the combination of hierarchical classification and a set of non hierarchical categories that represents the sensitivity of information.

"Sniffer" is a software program that is installed to monitor network traffic. Sniffers typically collect a certain number of characters at the beginning of a new users session

APPENDIX A

to compromise their logon and password.

"<u>Social Engineering</u>" is the gaining of priviledged information about a computer system by an unauthorized person masquarading as a legitimate user. The high-tech version of the old "confidence game"

"<u>Spoofing</u>" is an attempt to gain access to a system by posing as an authorized user. Synonymous with impersonating, masquerading or mimicking.

"<u>TCP Wrapper</u>" Transmission Control Protocol (TCP): Access control mechanism which allows/disallows and records access to TCP daemon. The wrapper sits between the inbound connection and daemon on the system which controls access to the system. The wrapper reads the incoming traffic and originating site and compares the IP address to an access list which the sysop configures. The access list contains sites which are authorized to connect to the system. The wrapper records the time, date, and originating IP address of the inbound connection before it allows access to the system.

"Telnet" is a program that allows you to log on to a computer at another location. Once logged on, you can look at files and run programs. When you run telnet, your local system:

- Opens a connection to the specified remote system

- "Pretends" to this remote systems that it is a terminal, rather than a computer

- Acts to you as a terminal

- Forwards your input as its output to the remote system, which takes it as terminal input

- Forwards the remote system's output back to you

A "*Trojan Horse*," as its name implies, allows an unsuspecting gatekeeper to invite an invading army into his midst. It is a program which performs, or appears to perform a valid function. As the apparently valid program executes in the foreground, a malicious code or set of instructions initiates other processes in the background which are invisible to the user.

"Trusted Host Table" is a listing technically known as "host.equiv file" which defines what other computer systems or networks that will allow remote access without having to login and use a password a second time. In turn, access can be gained to other computer systems who are on the trusted host table of the second system. This allows uninterrupted access to authorized users, however, once a hacker enters one system and cracks the password files, gains what appears to be legitimate access, the hacker can then gain what appears to be legitimate access to any other computer system listed on the trusted host table. If a system which contains a trusted host table has been compromised, all of the systems contained within the trusted host table can be considered compromised as well and appropriate action should be taken to secure them.

THE CASE STUDY: ROME LABORATORY, GRIFFISS AIR FORCE BASE, NY INTRUSION

The following case study is a good illustration of the type of threat facing our Department of Defense information infrastructure. Although the incident has been fully investigated by the Air Force Office of Special Investigations (OSI) numerous questions remain unanswered.

* * *

On March 28, 1994, computer systems administrators at Rome Air Development Center, Griffiss Air Force Base, New York, ("Rome Labs") discovered their network had been penetrated and compromised by an illegal wiretap computer program called a "sniffer"¹ that had been covertly installed on one of the systems connected to Rome Labs network. Rome Labs is the Air Force's premier command and control research facility. Its projects include artificial intelligence system, radar guidance systems, and target detection and tracking systems. Rome Labs works with academic institutions, commercial research facilities, and Defense contractors.

Upon detecting the password sniffer, the Rome Labs systems administrators immediately notified the Defense Information Systems Agency (DISA) that several computers at the Rome Labs had been penetrated electronically by unknown intruder(s). The Defense Information Systems Agency has a Computer Emergency Response Team (CERT) of computer security experts that assist Department of Defense systems administrators when they have a computer security incident.

The DISA CERT team, recognizing the severity of the incident, notified the Air Force Office of Special Investigations (AFOSI) of the intrusion. Agents from AFOSI notified the Air Force computer security experts at the Air Force Information Warfare Center, San Antonio, Texas.²

The team of security experts and Computer Crime Investigators traveled to Rome Labs and proceeded to review audit trails and interview systems administrators and witnesses. Their preliminary investigation revealed that two unknown individuals had: electronically penetrated seven of the computer systems at Rome Labs and gained

¹ A sniffer is covertly installed on computer networks by hackers to illegally collect user logons of authorized users. Generally sniffers collect the first 128 characters of each new user's logon. The first 128 characters of a user session usually contain the network address information of the computer system the user wants to log onto and then their private logon and password. These sniffers will capture this sensitive information in a file that is hidden from most systems administrator making it very difficult to find even when an expert knows what to look for. The hacker periodically comes back (electronically) and reads the sniffer file of captured user logons. The hacker can then masquerade as any of those authorized users that had their logon and password captured.

² The Air Force Information Warfare Center has the Air Force's Computer Emergency Response Team (AFCERT) which receives all AF computer security incidents reports. The Air Force responded by sending multi-disciplined teams from the Air Force Information Warfare Center (AFIWC), Air Intelligence Agency, and a team of AFOSI Computer Crime Investigators. The computer security experts from AFCERT performed three functions at Rome Labs; 1) assist in the assessment and extent of compromise of the Rome Lab's systems 2) secure systems, and 3) provide computer surveillance support for AFOSI's Computer Crime Investigators.

2.

<u>complete</u> access to all of the information residing on the systems; downloaded (copied) data files; and installed sniffer software programs on each of the seven systems.

These seven sniffer programs compromised a total of 30 of Rome Labs's systems. These systems contain sensitive research and development data. The computer system security logs revealed that Rome Labs systems had initially been penetrated on March 23, 1994, but were not discovered until five days later (March 28).

The investigation further revealed that the seven sniffer programs compromised over 100 additional user accounts by capturing user logons and passwords. User's e-mail were read, copied and deleted. Sensitive unclassified battlefield simulation program data was read and copied.

After the attackers had compromised all of the 30 systems at Rome Labs the intruders used Rome Labs systems as a Internet launching platform to attack other military, government, commercial, and academic systems world-wide, compromising user accounts, installing sniffer programs, and downloading large volumes of data from penetrated systems.

The investigative team assembled briefed the Rome Labs Commander who was given the option of securing all of the systems that had been penetrated by the attackers, or leaving one or more of the compromised systems open to attack so the agents could attempt to trace the path of the attacks back to their origin and identify the attackers. The commander opted to leave some of the systems open for the agents but the majority of the 30 compromised computer systems were secured.

Using standard software and computer systems commands the attacks were initially traced back one leg of their path. The majority of the attacks were traced back to two commercial Internet providers,³ cyberspace.com, in Seattle, Washington and *mindvox.phantom.com*, in New York. Newspaper articles indicated that *mindvox.phantom.com*'s computer security was provided by individuals that described themselves as "two former East-Coast Legion of Doom members". The Legion of Doom is a loose-knit computer hacker group which had several members convicted for intrusions into corporate telephone switches in 1990 and 1991.

Because the agents did not know whether the owners of the New York Internet provider were willing participants or merely a transit point for the break-ins at Rome Labs, they decided to surveil the victim computer systems to find out the extent of the access of the intruders and identify all of the victims. Following legal coordination and approval with Headquarters AFOSI's legal counsel, the Air Force General Counsel's Office and Department of Justice, Computer Crime Unit, real time content monitoring was established on one of the Rome Labs's networks. Real time content monitoring is analogous to performing a Title III wiretap as it allows you to eavesdrop on communications, or in this case text. The investigative team also began full "keystroke monitoring"⁴ at Rome. A sophisticated sniffer program was installed by the team to

³ An Internet provider is a subscription service provided by a commercial company. In this case, the company had computers that were connected to the Internet and a bank of telephone lines connected to their computer system that can be accessed from a home or office computer via modem. Once a subscriber accesses the company's computer system he or she can store data on their systems, utilize their reference library or use programs that reside on their system. In addition the service provider gives you connectivity to the Internet.

⁴ Keystroke monitoring is the capturing of predetermined data typed by a user that is logged into a system. Keystroke monitoring usually captures every keystroke typed by every user logged into the system. Keystroke monitoring is an electronic surveillance equivalent to a

capture every keystroke of any intruder who entered the Rome Labs's system.⁵ Additionally limited context monitoring of the commercial Internet providers was also performed remotely. This limited context monitoring consisted of subscribing to the commercial Internet providers service and utilizing only software commands and utilities the Internet provider authorized every subscriber to use.

The path of the intruders could only be traced back one leg. To determine the next leg of the intruders path required access to the next system along the hacker's route. If the attacker was utilizing telephone systems to access the Internet provider a court ordered "trap and trace" of telephone lines was required. Due to the time constraints involved in obtaining such an order, it was not a viable option. Furthermore, if the attacker changed their path the trap and trace would not be fruitful.

During the course of the intrusions, the Investigative team monitored the hackers as they intruded on the system attempting to trace the intruders back to their origin. They found the intruders were using the Internet and making fraudulent use of the telephone systems, or "phone phreaking."⁶ Because the intruders used multiple paths to launch their attacks, the investigative team was unable to trace back to the origin in real time due to the difficulty in tracing back multiple systems in multiple countries. Subsequent reviews of the surveillance logs revealed that on March 30, 1994, that systems of the Army Corps of Engineers, Vicksburg, Mississippi were attacked from Rome Lab's systems. Additionally, from the monitoring, the investigators were able to determine the hackers used the nicknames *Datastream* and *Kuji*.

AFOSI Computer Crime Investigators turned to their human intelligence network of informants that "surf the Internet". The investigators levied their informants to identify the two hackers using the handles Datastream and Kuji. On April 5, 1994, an informant told the investigators he had a conversation with a hacker that identified themselves as Datastream Cowboy. The conversation was via E-Mail and the individual stated that he was from the United Kingdom. The on line conversation had occurred three months prior. In the E-Mail provided by the informant, Datastream indicated he was a 16 year old from the United Kingdom who liked to attack ".MIL"⁷ sites because they were so insecure. Datastream even provided the informant with his home telephone number for his own hacker bulletin board systems he had established.⁸

The Air Force Agents had previously established liaison with New Scotland Yard who were able to identify the individuals residing at the residence associated with Datastream's telephone numbers. New Scotland Yard had British Telecom initiate monitoring (pen registers) of the individual's telephone lines. A pen register recorded

wiretap.

⁶ Phone phreaking is a subset of computer hacking and involves hacking of the telephone systems to make fraudulent phone calls, or manipulate the telephone systems. Phone phreakers can install calling features like caller-id, call waiting, make conference calls, zero out billing records, etc.

⁷ ".MIL" is a suffix attached to many military Internet addresses.

⁸ Hackers commonly set up bulletin boards that serve as open access repositories of information they wish to disseminate to the Internet community.

⁵ Since the Rome Lab had previously installed a logon warning banner putting all users on notice that the system was for "Official Use Only", was monitored for security purposes, and "Use of the system constituted consent to monitoring", a court order was not required. The surveillance could commence with only the approval of the AF's General Counsel's office.

all of the numbers dialed by the individuals at the residence. Almost immediately that monitoring disclosed that someone from the residence was phone phreaking through British Telecom, which is also illegal in the United Kingdom.

4.

New Scotland Yard found that every time there was an intrusion at Rome Labs, the individual in the UK was phone phreaking the telephone lines to make free telephone calls out of the UK. Originating from the UK, his path of attack was through systems in multiple countries in South America, multiple countries in Europe, and also through Mexico and Hawaii and occasionally end up at Rome Labs. From Rome Labs he was able to attack systems via the Internet at NASA's, Jet Propulsion Laboratory in California and their Goddard Space Flight Center in Greenbelt, MD.

Continued monitoring by the UK and U.S. authorities disclosed on April 10, 1994, Datastream successfully penetrated an aerospace contractor's home system that had been compromised at Rome Labs by the installation of the sniffers. The attackers captured the logon of the contractors at Rome Labs with their sniffer programs when the contractor would log onto their home systems in California and Texas. The sniffer would capture the address of their home system, plus that contractor's logon and password for that home system. Once the logon and password was compromised the attackers could masquerade as that authorized user on the contractor's home system. Four of the contractor's systems were compromised in California and a fifth in Texas.

Datastream also utilized an Internet Scanning Software attack on multiple systems of this aerospace contractor. The Internet Scanning Software is a hacker tool developed to gain intelligence about a system. It will attempt to collect information on the type of operating system the computer is running and any other available information that could be used to assist the attacker in determining what attack tool might successfully break into that particular system. The software also tries to locate the password file for the system being scanned and then tries to make a copy of that password file. The significance of the theft of a password file, is that even though password files are usually stored encrypted, they are easily decrypted. There are several hacker "password cracker" programs available on the Internet. If a password file is stoler/copied and cracked, the attacker can then log onto that system as what the systems perceives is a legitimate user.

Monitoring activity disclosed, on April 12, that Datastream initiated an Internet Scanning Software attack from Rome Labs against Brookhaven National Labs, Department of Energy, New York. Datastream also had a two hour connection with the aerospace contractors system previously compromised.

On April 14, remote monitoring activity of the Seattle Internet provider, cyberspace.com, by the Air Force, indicated Kuji connected to the Goddard Space Flight Center, Greenbelt, Maryland, through the Internet provider and from Latvia. The monitoring disclosed data was being transferred from Goddard Space Flight Center to the Internet provider. In order to prevent the loss of sensitive data, the monitoring team broke the connection. It is still unknown if the data being transferred from the National Aeronautics and Space Administration (NASA) system was destined for Latvia.

Further remote monitoring activity of the Seattle Internet provider, *cyberspace.com*, disclosed Datastream accessing the National Aero-Space Plane Joint Program Office, a joint project headed by the NASA and the Air Force at Wright-Patterson, AFB, Ohio. Monitoring disclosed a transfer of data from Wright-Patterson AFB traversing through *cyberspace.com* to Latvia. Apparently, Datastream attacked and compromised a system in Latvia which was just being used as conduit to prevent identification.

Kuji also initiated an Internet Scanning Software attack against Wright-Patterson AFB, from the Internet provider in Seattle, Washington, the same day. The theft of a password file from a computer system at Wright-Patterson AFB was also attempted.

On April 15, real time monitoring disclosed Kuji executing the Internet Scanning Software, against NATO Headquarters in Brussels, Belgium and Wright-Patterson AFB, OH, from Rome Labs. Kuji did not appear to gain access to any NATO systems from this particular attack. However, a systems administrator from SHAPE Technical Center (NATO Headquarters), The Hague, Netherlands was interviewed, on April 19, by AFOSI and disclosed Datastream had successfully attacked one of SHAPE's computer systems from the Internet provider in New York, *mindvox.phantom.com*,

Once they confirmed the hacker's identity, and developed probable cause, New Scotland Yard requested and was authorized a search warrant for the residence of Datastream. The plan was to wait until the individual was on line, at Rome Labs, and then execute the search warrant. The investigators wanted to catch Datastream on line so they could identify all of the victims in the path between his residence and Rome Labs. Once Datastream got on-line at Rome Labs, they found that he suddenly accessed a system in Korea and logically⁹ obtained up all of data stored on the Korean Atomic Research Institute system and deposited it on Rome Lab's system. Initially it was unclear whether the Korean systems belonged to North Korea or South Korea. The concern was that if it was North Korea, the North Koreans would think the logical transfer of the storage space was an intrusion by the US Air Force, which could be perceived as an aggressive act of war. During this time frame, the U.S. was in sensitive negotiations with the North Koreans regarding their nuclear weapons program. Within hours, it was determined that Datastream had hacked into the South Korean Atomic Research Institute. At this point, New Scotland Yard decided to expand their investigation and requested the Air Force to continue to monitor and collect evidence in support of their investigation and postponed execution of the search warrant.

On May 12, New Scotland Yard executed their search warrant on Datastream's residence. The search disclosed Datastream had launched his attacks with only a 25 MHz, 486 SX desktop computer with only an 170 Megabyte hard drive. This is a very modest system that is very slow with very limited storage capacity.¹⁰ Datastream had numerous documents which contained references to Internet addresses, including six NASA systems, US Army and US Navy systems with instructions on how to loop through multiple systems to avoid detection.

At the time of the search, Datastream was arrested and interviewed by New Scotland Yard detectives. Detectives stated Datastream had just logged out of a computer systems when they entered his room. Datastream admitted to breaking into Rome Labs numerous times as well as multiple other Air Force systems (Hanscom AFB, Massachusetts, and Wright-Patterson AFB, Ohio). Datastream admitted to stealing a sensitive document containing research regarding Air Force artificial intelligence. He added he searched for the word "missile", not to find missile data but to find information specifically about artificial intelligence. He further explained that one of the files he stole was a 3-4 megabyte file (3-4 million characters in size) and he stored it at the Internet provider's system in New York (*mindvox.phantom.com*). He stored it at the Internet provider's system because it was too large to fit on his home system. This file was an

⁹ When a user logically picks up data, he or she is adding remote disk storage that will be accessed by their own system as if it were physically located inside their own system.

¹⁰ Computers sold off the shelf today, just 2 years later, are significantly more powerful with over 100 Mhz Pentium processors and well over 1 Gigabytes of disk storage capacity.

artificial intelligence program that dealt with Air Order of Battle. Datastream explained he paid for the Internet provider's service with a fraudulent credit card number which was generated by a hacker program he had found on the Internet. Datastream was released on bail following the interview.

The investigation never revealed the identity of Kuji. From conduct observed through the investigators monitoring, Kuji was a far more sophisticated hacker than the 16 year old Datastream. Air Force investigators were able to observe that Kuji would only stay on a telephone line a short time, not long enough to be traced successfully. There was no informant information available except that Computer Crime Investigators from the Victorian Police Department in Australia had seen the name Kuji on some of the hacker Bulletin Board Systems in Australia. Unfortunately, Datastream provided a great deal of the information he stole to Kuji electronically.

Furthermore, Kuji appears to have tutored Datastream on how to break into networks and on what information to obtain. During the monitoring, the investigative team could observe Datastream attack a system and fail to break in. Datastream would then get into an on-line "chat sessions"¹¹ with Kuji which the investigative team could not see due to the limited context monitoring at the Internet providers. These chat sessions would last 20-40 minutes. Following the on-line conversation the investigative team would then watch Datastream attack the same system he had previously failed to penetrate, but this time he would be successful. Apparently Kuji assisted and mentored Datastream and, in return, received from Datastream stolen information. Datastream, when interviewed by New Scotland Yard's Computer Crime Investigators, told them had never physically met Kuji and only communicated with him through the Internet or on the telephone. Nobody knows what Kuji did with this information or why it was being collected. In addition it is not known where Kuji resides. During the 26 day period of attacks, there were over 150 known intrusions by the two hackers, Datastream Cowboy and Kuji.

A damage assessment of the intrusions into the Rome Lab's systems was conducted on October 31, 1994. The assessment indicated a total loss to the United States Air Force of \$211,722. This cost did not include the costs of the investigative effort or the recovery and monitoring team. No other federal agencies that were victims of the hackers, including NASA and the Bureau of Reclamation, conducted damage assessments. The General Accounting Office conducted an additional damage assessment at the request of Senator Sam Nunn. (See GAO Report, *Information Security, Computer Attacks at Department of Defense Pose Increasing Risks.*)

Datastream is pending prosecution in the UK. Numerous aspects of this investigation remain unsolved:

- The identity and motivation of Kuji. Thought investigators believe he was technically
 more sophisticated than Datastream, he has not been identified, and his motivation
 is presently unknown. Furthermore, it is unknown whether Datastream was his only
 agent, or whether he utilized others in the same manner.
- The extent of the attack. The investigators believe they only uncovered a portion of the attack. It is not still not known (1) whether the hackers attacked Rome Labs at previous times before the sniffer was discovered; (2) whether the hackers attacked other systems where they were not detected.

¹¹ Chat sessions are text conversations that occur between users on the Internet who type their conversations in real time versus talking of voice telephone lines.

The extent of the damage. Some costs can be attributed to the incident such as the
cost of repair, and the cost of the investigative effort. The investigation, however,
was unable to reveal what was downloaded from the networks, or whether any data
was tampered with. Given the sensitive information contained on the various
computer networks -- Rome Labs, at Goddard Space Flight Center, Jet Propulsion
Laboratory at Wright-Patterson AFB, or National Aero-Space Plane Program -- it is
very difficult to quantify the loss from a national security perspective.

APPENDIX C

NATIONAL SECURITY COUNCIL WASHINGTON, D.C. 20504

271

March 8, 1996

MEMORANDUM FOR MR. JOHN F. SOPKO Minority Deputy Chief Counsel Permanent Subcommittee on Investigations Senate Governmental Affairs Committee

SUBJECT:

Senator Nunn's Request for Copy of FEMA Abstract on PDD-39

Pursuant to Senator Nunn's request, enclosed for your information is a copy of the NSC approved unclassified FEMA abstract on PDD-39.

All requests for copies of, access to or information about Presidential Decision Directives (PDD) should be sent directly to the National Security Council.

rdrew D. Sens

Executive Secretary

Attachment Tab A

Unclassified FEMA Abstract on PDD-39

cc: Ms. Catherine H. Light Director Office of National Security Coordination Federal Emergency Management Agency

APPENDIX C

U.S. POLICY ON COUNTERRORISM

1. <u>General</u>. Terrorism is both a threat to our national security as well as a criminal act. The Administration has stated that it is the policy of the United States to use all appropriate means to deter, defeat and respond to all terrorist attacks on our territory and resources, both people and facilities, wherever they occur. In support of these efforts, the United States will:

- Employ efforts to deter, preempt, apprehend and prosecute terrorists.
- Work closely with other governments to carry out our counterterrorism policy and combat terrorist threats against them.
- Identify sponsors of terrorists, isolate them, and ensure they pay for their actions.
- Make no concessions to terrorists.

2. <u>Measures to Combat Terrorism</u>. To ensure that the United States is prepared to combat terrorism in all its forms, a number of measures have been directed. These include reducing vulnerabilities to terrorism, deterring and responding to terrorist acts, and having capabilities to prevent and manage the consequences of terrorist use of nuclear, biological, and chemical (NBC) weapons, including those of mass destruction.

a. <u>Reduce Vulnerabilities</u>. In order to reduce our vulnerabilities to terrorism, both at home and abroad, all department/agency heads have been directed to ensure that their personnel and facilities are fully protected against terrorism. Specific efforts that will be conducted to ensure our security against terrorist acts include the following:

- Review the vulnerability of government facilities and critical national infrastructure.
- o Expand the program of counterterrorism.
- Reduce vulnerabilities affecting civilian personnel/facilities abroad and military personnel/facilities.
- Reduce vulnerabilities affecting U.S. airports, aircraft/passengers and shipping, and provide appropriate security measures for other modes of transportation.
- o Exclude/deport persons who pose a terrorist threat.

APPENDIX C

- Prevent unlawful traffic in firearms and explosives, and protect the President and other officials against terrorist attack.
- Reduce U.S. vulnerabilities to international terrorism through intelligence collection/analysis, counterintelligence and covert action.

b. Deter. To deter terrorism, it is necessary to provide a clear public position that our policies will not be affected by terrorist acts and we will vigorously deal with terrorist/sponsors to reduce terrorist capabilities and support. In this regard, we must make it clear that we will not allow terrorism to succeed and that the pursuit, arrest, and prosecution of terrorists is of the highest priority. Our goals include the disruption of terrorist-sponsored activity including termination of financial support, arrest and punishment of terrorists as criminals, application of U.S. laws and new legislation to prevent terrorist groups from operating in the United States, and application of extraterritorial statutes to counter acts of terrorism and apprehend terrorists outside of the United States. Return of terrorists overseas, who are wanted for violation of U.S. law, is of the highest priority and a central issue in bilateral relations with any state that harbors or assists them.

c. Respond. To respond to terrorism, we must have a rapid and decisive capability to protect Americans, defeat or arrest terrorists, respond against terrorist sponsors, and provide relief to the victims of terrorists. The goal during the immediate response phase of an incident is to terminate terrorist attacks so that the terrorists do not accomplish their objectives or maintain their freedom, while seeking to minimize damage and loss of life and provide emergency assistance. After an incident has occurred, a rapidly deployable interagency Emergency Support Team (EST) will provide required capabilities on scene: a Foreign Emergency Support Team (FEST) for foreign incidents and a Domestic Emergency Support Team (DEST) for domestic incidents. DEST membership will be limited to those agencies required to respond to the specific incident. Both teams will include elements for specific types of incidents such as nuclear, biological or chemical threats.

The Director, FEMA, will ensure that the Federal Response Plan is adequate for consequence management activities in response to terrorist attacks against large U.S. populations, including those where weapons of mass destruction are involved. FEMA will also ensure that State response plans and capabilities are adequate and tested. FEMA, supported by all Federal Response Plan signatories, will assume the Lead Agency role for consequence management in Washington, D.C. and on scene. If large scale casualties and infrastructure damage occur, the President may appoint a Personal Representative for consequence management as the on scene Federal authority during recovery. A roster of senior and former government officials willing to perform these functions will be created and the rostered individuals will be provided training and information necessary to allow them to be called upon on short notice.

Agencies will bear the costs of their participation in terrorist incidents and counterterrorist operations, unless otherwise directed.

d. NBC Consequence Management. The development of effective capabilities for preventing and managing the consequences of terrorist use of nuclear, biological or chemical (NBC) materials or weapons is of the highest priority. Terrorist acquisition of weapons of mass destruction is not acceptable and there is no higher priority than preventing the acquisition of such materials/weapons or removing this capability from terrorist groups. FEMA will review the Federal Response plan on an urgent basis, in coordination with supporting agencies, to determine its adequacy in responding to an NBC-related terrorist incident; identify and remedy any shortfalls in stockpiles, capabilities or training; and report on the status of these efforts in 180 days.

SAMPLE COMPUTER LOGON BANNER

This is a U.S. Government computer system. Government computer systems are provided for the processing of Official U. S. Government information only. All data contained on Government computer systems is owned by the U.S. Government, and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. Systems personnel may give to law enforcement officials any potential evidence of crime found on this U.S. Government system. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, or CAPTURING and DISCLOSURE.

IF YOU DO NOT CONSENT, LOG OFF NOW.

<u>NOTE</u>: A BANNER SUCH AS THIS ONLY AUTHORIZES GENERAL MONITORING FOR ADMINISTRATIVE PURPOSES. IF THE MONITORING SHOULD GO BEYOND SUCH PURPOSES AND TAKES ON THE NATURE OF A CRIMINAL INVESTIGATION, THEN MONITORING SHOULD BE CONDUCTED ONLY PURSUANT TO THE PROCEDURES SPECIFIED IN FEDERAL LAW AND REGULATIONS.



GAO

For Release on Delivery Expected at 9:30 a.m. Wednesday June 5, 1996

United States General Accounting Office

Testimony

Before the Permanent Subcommittee on Investigations, Committee on Govenmental Affairs, United States Senate

INFORMATION SECURITY

Computer Hacker Information Available on the Internet

Statement for the Record of Jack L. Brock, Jr. Director, Defense Information and Financial Management Systems

and Keith A. Rhodes, Technical Assistant Director,

Office of the Chief Scientist, Accounting and Information Management Division



GAO/T-AIMD-96-108

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to again participate in the Subcommittee's continuing hearings on the security of our nation's information systems. As you know, on May 22, 1996, the first day of the Subcommittee's hearings, we testified and released our report¹ about the increasing risks computer hackers² pose to computer systems and information at the Department of Defense. Our purpose today is to reiterate the importance of computer security to Defense and other federal agencies, and to provide an introduction to hacker techniques and information available on the Internet.

COMPUTER ATTACKS ARE AN INCREASING THREAT

The Department of Defense, like the rest of government and the private sector, relies on technology. The Department depends increasingly on computers linked together in a vast collection of networks, many of which are connected to the worldwide Internet.³ The Internet provides tremendous benefits; it can streamline business operations and put a vast array of information at the fingertips of millions of users. Over the last several years, we have seen a rush to connect to the Internet, and today there are over 40 million users worldwide.

However, with these benefits come risks. Hackers have been exploiting security weaknesses of systems connected to the Internet for years. The number of people with access to the Internet, any one of which is a potential hacker, coupled with the rapid growth and reliance on interconnected computers, has made the cyberspace frontier a dangerous place. Hackers have more tools and techniques than ever before, and the number of attacks is growing every day. The need for secure information systems and networks has never been greater.

The Department of Defense's computer systems are being attacked every day. Although the exact number of attacks cannot be readily determined because only a small portion are actually detected and reported, Defense Information Systems Agency (DISA) data

¹Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

²The term hacker refers to unauthorized individuals who attempt to penetrate information systems; browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way.

³The Internet is a global network interconnecting thousands of dissimilar computer networks and millions of computers worldwide. Over the past 20 years, its role has evolved from relatively obscure use by scientists and researchers to a popular, userfriendly means of information exchange for millions of users.

1

suggest that Defense may have experienced as many as 250,000 attacks last year, and that the number of attacks is doubling each year. DISA information also shows that attacks are successful 65 percent of the time.

Not all attacks result in actual intrusions; some are attempts to obtain information on systems in preparation for future attacks, while others are made by the curious or those who wish to challenge the Department's computer defenses. Many attacks, however, have been very serious, resulting in stolen and destroyed sensitive data and software. By installing *backdoors*, guessing passwords, or other techniques, hackers have surreptitiously gained illegal entry into sensitive Defense systems, many of which support critical functions, such as weapons systems research and development, supply, personnel, contract management, and finance. They have caused entire systems and networks to crash, denying computer service to authorized users and preventing Defense personnel from performing their duties. Although Defense has not computed the cost of these attacks, unofficial estimates place the cost at millions of dollars in lost productivity and damage to systems.

Even more critical than the cost and disruption caused by these attacks is the potential threat to national security. Many Defense and computer systems experts believe that computer attackers can disrupt communications, steal sensitive information, and threaten our ability to execute military operations. The National Security Agency and other experts have acknowledged that potential adversaries are attempting to obtain sensitive information by hacking into military computer systems. They believe that over 120 countries either have or are developing information warfare capabilities. Countries today do not have to be military superpowers with large standing armies, fleets of battleships, or squadrons of fighters to gain a competitive edge. Instead, all they need to steal sensitive data or shut down military computers is a \$2,000 computer, a modem, and a connection to the Internet.

The Internet was spawned from ARPANET, a network designed by the Advanced Research Projects Agency in the 1960s to provide a means of electronically exchanging military research information. The main goals of ARPANET were to provide a network that would continue to function even if sections of the network were lost, to allow computers of many different types to communicate with each other, and to enable inexpensive, convenient addition or removal of nodes (Internet hookups). In the 1980s, ARPANET became the Internet. Because of this history, the Department of Defense has been using the Internet longer and more widely than other government agencies. As a result, the Department, despite its problems, probably has one of the strongest computer security programs in government. Its experience suggests, however, that other agencies will increasingly be at risk of computer attacks as they expand their use of the Internet.

HOW COMPUTER SYSTEMS ARE ATTACKED A variety of weaknesses can leave computer systems vulnerable to attack. For example, they are vulnerable when (1) inexperienced or untrained users accidentally violate good security practices by inadvertently publicizing their passwords, (2) weak passwords are chosen which can be easily guessed, or (3) identified system or network security weaknesses go uncorrected. Malicious threats can be intentionally designed to unleash computer viruses,⁴ trigger future attacks, or install software programs that compromise or damage information and systems.

Attackers use a variety of methods to exploit numerous computer system vulnerabilities. Examples, include (1) <u>sendmail</u> - a common type of attack in which the attacker installs malicious code in an electronic mail message that adds a password into the system's password file thereby giving the attacker total system privileges, (2) <u>password cracking</u> - a technique in which attackers try to guess or steal passwords to obtain access to computer systems, and (3) <u>packet sniffing</u> - a technique in which attackers surreptitiously insert a software program that captures the passwords and user identifications contained in the first 128 key strokes of a connection.

Once they have gained access, hackers use the computer systems as though they were legitimate users. They use a variety of techniques to cover their tracks and avoid detection. Hackers can steal information, both from the systems compromised as well as systems connected to them.

HACKER INFORMATION AVAILABLE ON THE INTERNET

Computer attacks have also become easier to carry out due to the proliferation of readily available hacker information, tools, and techniques on the Internet. Behind this proliferation are informal hacker groups, such as 2600, the Legion of Doom, and Phrack, Inc., which openly share information on things such as how to break into computer systems and how to obtain free telephone service. The information posted on the electronic bulletin boards at the web sites⁵ such groups sponsor allows virtually any of the more than 40 million Internet users who wants to be a hacker to become one.

⁴A virus is a code fragment that reproduces by inserting copies of itself to other programs. In may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users.

⁵The worldwide web (www), started by Tim Berners-Lee while at the European Laboratory for Particle Physics, is a "distributed hypermedia system." In practice, the web is a vast collection of interconnected information, spanning the world. A web site is any computer on the Internet running a World-Wide Web server process. A particular web site is identified by the hostname part of the uniform resource locator.

The potential hacker can learn about these groups from any computer with an Internet connection by using any one of a number of search programs available to Internet users. These programs, or search "engines," which include *lycos, alta vista, yahoo, web crawler, excite, magellan,* all can be used as a starting point to help a potential hacker pinpoint web sites containing information for conducting computer attacks. For example, we tried a simple single-word and dual-word query using the *alta vista* program. Using the word "hacking", we got more than 20,000 responses showing Internet sites or files where information on hacking is available. Similarly, using the words "password cracking", we got an additional 20,000 responses. The two examples below are typical of the responses we came across.

• alt.2600/#hack FAQ at www.(site).edu/alt2600/FAQ.html

• alt.2600 Survival Guide_ at www.(site).edu/alt2600/survive.html

These two responses are from *alt.2600*, the file name of a web site on the Internet that supports the readers of *2600 Magazine*, a hacker quarterly. The purpose of the *alt.2600* survival guide is to provide information on the hacker news group, as well as information on how to avoid being caught by the people and organizations under attack. To get to the web site containing the files, one need only click on the file name. In this case, we were sent to a web site called the *Internet Underground*. The *Internet Underground* site provides a typical disclaimer

"This WWW (world-wide web) page is provided for informational sake to those like me who are interested in computer and telephone security. In no way do I encourage you to do anything illegal (emphasis added). Far from it. Think of this as a guide of what not to do."

This disclaimer is like openly providing the recipe for baking a cake, but telling you not to bake it. Despite this disclaimer, people will use the information to hack into computer systems.

At this *Internet Underground* site, one can examine the frequently asked questions, or take a look at the survival guide itself. The survival guide begins, "Welcome to *alt.2600*, the Internet news group for readers of *2600 Magazine*. On *alt.2600* we discuss telephone (phreaking), computer (hacking), and related topics. . . . *alt.2600* readers pride themselves on being hackers. A hacker seeks out information by every available means (emphasis added)."

If you proceed further into this site, you can locate additional information files. For example, "info philes" (spelled with a "ph" because the file mostly contains information on how to break into a telephone system) contains information on how to build devices known as boxes that allow you to break into cable/video boxes, pay telephones, or telephone circuits. For example, one home page⁶ we visited containing information on these devices was John's Boxing Page. Again we came across a disclaimer that read "... my intention is not to defraud or encourage people to defraud the phone company. . ." and then proceeded to describe how to build 26 different kinds of boxes. One of the files linked to this home page gave the following directions for building a red box.

- 1. Buy Radio Shack part number 43-146.
- 2. Unscrew all of the screws.
- 3. Desolder the crystal which says 3579 on it.
- 4. Replace it with a 6.5536 MHz crystal.
- 5. Replace the cover.
- 6. You now have a red box.

Although this information is claimed to be outdated and no longer valid, a red box is typically used to generate a digital or tonal signal that emulates the sound of coins being dropped into a public telephone, thus allowing hackers to make telephone calls for free.

There are many other hacker publications on the Internet. For example, *Phrack* is a very popular phone cracking association. When you go to this web site, you find several directories; one being the Phrack Magazine Underground Archives. The maintainers of the archives have collected a variety of documents from various phreaking, cracking, and hacking sources. These publications include information on hacker conferences and how to break into computer and telephone systems. It also contains links to other web sites. Following is just a partial list of groups in the archives.

- 40 Hex Magazine
- Activist Times, Inc.
- The BIOC Files
- Chalisti
- Freakers Bureau Inc.
- Freedom
- The Legion of Doom
- Misc. Underground Files
- National Security Anarchists
 Network Information Access
- The New Fone Express
- PHUN Magazine
- United Phreakers Inc.

- The Art of Technology Digest
- Anarchy 'N' Explosives
- The Cult of the Dead Cow
- Chaos Digest
- Digital Free Press
- Informatik
- Legions of Lucifer
- N.A.R.C. Newsletter
- Phantasy Magazine
- Pirate Magazine
- Vindicator Publications

⁶A home page is typically the top-level introduction to an individual's or institution's Internet site. It often includes a uniform resource locator, a draft standard for specifying an object on the Internet, such as a file or newsgroup, e.g. http://www.ncsa.uiuc.edu/. All other pages on a server are usually accessible by following links from the home page.

For example, some of these groups openly share information on how to go from one's home into a public telephone switch without paying for it, and then go from there into another telephone switch (possibly in another country), and then from there to the desired destination. This use of multiple telephone switches makes it more difficult for the authorities to trace the hacker.

Also available on the Internet are user-friendly hacker tools. For example, SATAN (Security Administrator Tool for Analyzing Networks) is one such tool that was designed to identify computer system and network security weaknesses, but which is also being used by hackers to break into systems. Similarly, a tool called *rootkit* is available on the Internet. *Rootkit* is actually a series of "trojan horses." A trojan horse is a software program that replaces and mimics an existing function, but also performs unauthorized functions, often usurping the privileges of authorized users. For example, a hacker can install rootkit on a targeted system administrator, but would enable the hacker to obtain a list of the files on that system, monitor disk usage, and see what processes are running.

We also found hacker tools at an Internet bulletin board called the *Computer* Underground Digest. It contains nearly 70 directories, each containing information on how to undertake acts of destruction and mayhem such as how to break into systems and how to create and plant viruses. For example, the directory called 40hex/ publishes *Spotlight on Viruses* which actually includes some of the source code⁷ for viruses that one can use to disrupt somebody else's computer system. Some of the virus information in 40hex/ includes

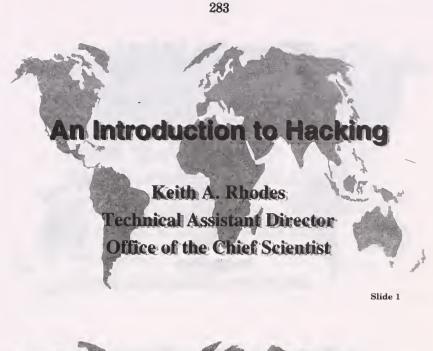
- Virus Spotlight, The Tiny virus
- Sub-Zero virus
- Leprosy-B
- USA Virus News
- The Sunday Virus
- The Typo COM Virus
- How to modify viruses to avoid SCAN
- Simple encryption techniques
- 1992 virus
- The Bob Ross Virus
- The Terror Virus

In conclusion, these bulletin boards and sites clearly show that any marginally computer literate individual can use the Internet itself to quickly obtain basic information on the tools and techniques needed to become a computer hacker. They also demonstrate that the Subcommittee's concerns about unauthorized access to sensitive information in computer systems is well-founded. The Department of Defense has already experienced thousands of computer attacks originating from network connections, many of which have resulted in considerable disruption and damage. Other government agencies and the private sector will undoubtedly be at increasing risk of attack as their reliance on the Internet increases, as the number of worldwide Internet users multiplies, and as information on hacker tools and techniques becomes even more readily available.

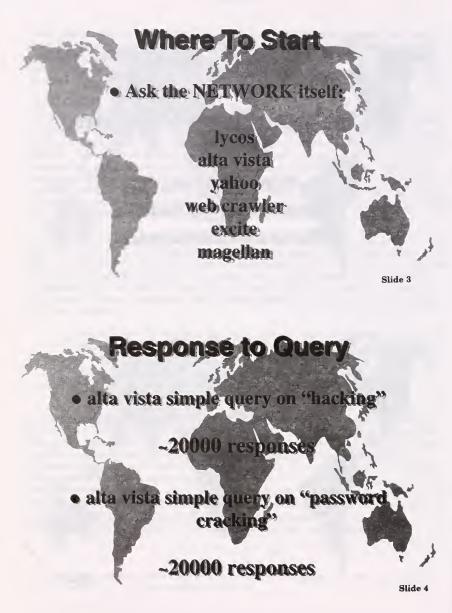
.

Mr. Chairman, that completes our testimony. We will be happy to answer any questions you or Members of the Subcommittee may have.

⁷Source code is the software program written in human readable form by the programmer, as opposed to object code which is derived from source code and is machine executable.







Example respo alt.2600/#hack FA 0.-- alt.2600 is the usenet newsgroup comprised of readers of 2600 Magazine .. www.site.edu/alt2600/FAO.html • alt.2600 Survival Guide -- The purpose of this guide is to help you fit into the newsgroup... www.site.edu/alt2600/survive.html Slide 5 The Internet Underground

Slide 6

Home

The Internet Underground

"Disclaimer: This WWW page is provided for informational sake to those like me who are interested in computer and telephone security. In no way do I encourage you to do anything illegal. Far from it. Think of this as a guide of what not to do."

Slide 7

The Internet Underground

The FAQ's

alt.2600/#hack FAQ

alt.2600 Survival Guide

alt.cyberpunk FAQ

alt.2600 Survival Guide

"Welcome to alt.2600, the Internet newsgroup for readers of 2600 Magazine. On alt.2600 we discuss telephony (phreaking), computers (hacking), and related topics. The purpose of this guide is to help you fit into the newsgroup, and avoid being flamed (insulted and abused) by the other users of this newsgroup...alt.2600 readers pride themselves on being hackers. A hackers seeks out information by every available means."

Slide 9

The Internet Underground

Info "Philes" Boxing Page How to be a Hacker - A satirical look at "traditional"-hacking Free Service from AOL PGP in a Nutshell Modifying a Radio Shack Memory Dialer

John's Boxing Page

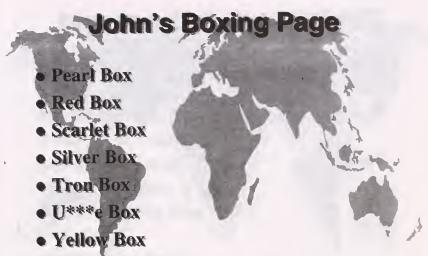
"Most if not all of this information is horribly out-of-date. My primary motivation for putting this online was a way to look back at the history of phone fraud. Again, my intention is not to defraud or encourage people to defraud the phone company. Even if one of these articles opens up that possibility for you, which I highly doubt, don't do it!"

Slide 11

John's Boxing Page

- Aqua Box
- Beige Box
- Black Box
- Blotto Box
- Brown Box
- Bud Box
- Bug Detector
- Busy Box
- Chartreuse Box

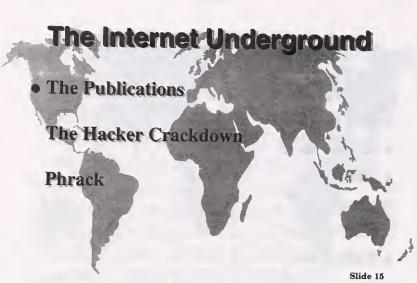
- Cheese Box
- Clear Box
- Crimson Box
- DLOC Box
- Gold Box
- Jack Box
- Neon Box
- Paisley Box
- Pandora's Box



Slide 13

Radio Shack Dialer Modification

- Buy Radio Shack part number 43-146. Unscrew all of the screws.
- Desolder the crystal which says 3579 on it.
- Replace it with a 6.5536 MHz crystal.
- Replace the cover.
- You have now have a red box.





PHRACK MAGAZINE UNDERGROUND ARCHIVES

- 40 Hex Magazine/
- Anarchy 'N' Explosives/
- The Art of Technology Digest
- Activist Times Inc./
- The BIOC Files/
- The Cult of the Dead Cow/
- Chalisti/
- Digital Free Press/
- Freakers Bureau Incorporated/

Slide 17

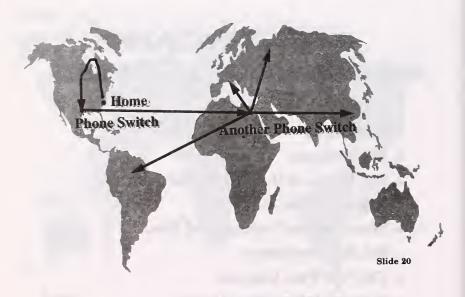
PHRACK MAGAZINE

Freedom/

- T. Formatik
- Informatik/
- Chaos Digest/
- The Legion of Doom Technical Journals
- Legions of Lucifer/
- Miscellaneous Underground Files/
- N.A.R.C Newsletter/
- The New Fone Express/
- Network Information Access/

PHRACK MAGAZINE UNDERGROUND ARCHIVES

- National Security Anarchists/
- Phantasy Magzine/
- PHUN Magazine/
- Pirate Magazine/
- The Syndicate Report/
- United Phreakers Incorporated Newsletter/
- Vindicator Publications/
- The WorldView/





SATAN was designed to have a very "user friendly" user interface. Since it is extremely difficult to create a good user interface from scratch, we stole everyone else's.

SATAN

Subsections in the User Interface section

The Basics Data Management **Gathering Data** Looking at and understanding the results Hints, Further tricky security implications, or Getting The Big Picture (tm) The Command-line Interface



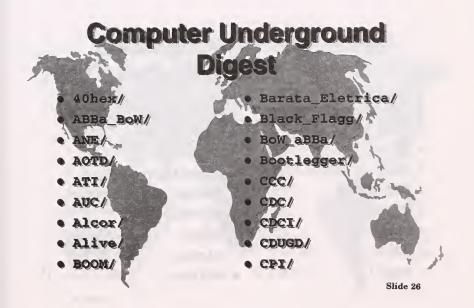
Directory listing of /~/System/rootkit

- ps.c
- revarp.c
- rootkit.README
- route.c
- e sl.c
- unix.c
- z2.c

Slide 24



Slide 25





MoT/

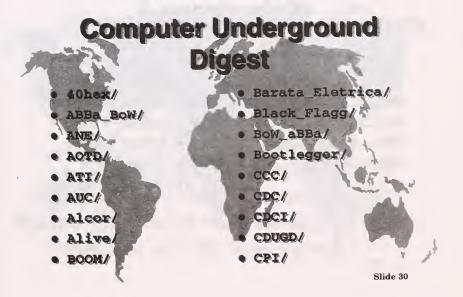
• InfoPol/

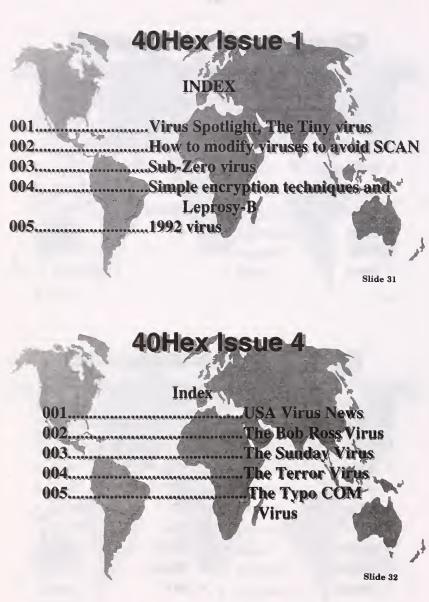
Slide 27

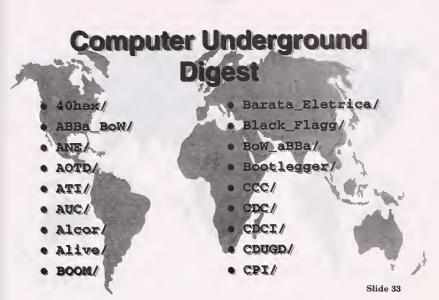


Slide 28





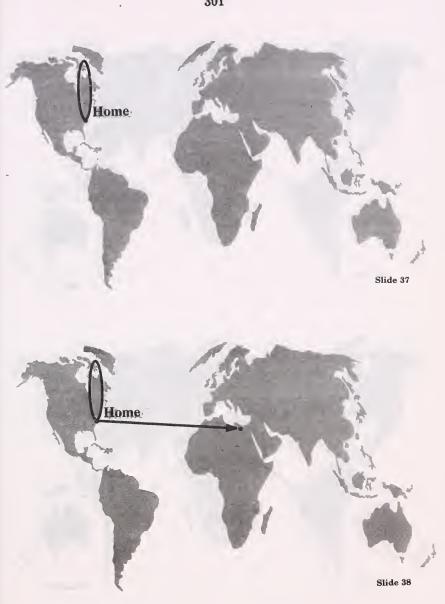


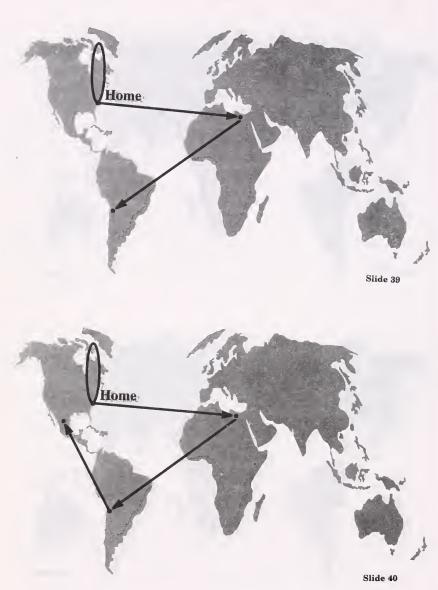


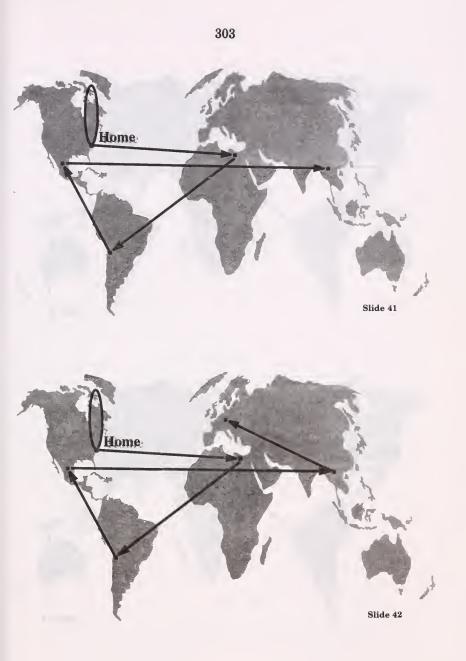
Contents of BOOM #5 In this issue we will be explaining how to make simple explosives and projectiles. 1. Gas[oline] bomb. 2. Small rocket projectile. 3. The Amazing Fireball Shooting Rod. "Dazzle your friends while burning off their eyelashes with this amazing rod."

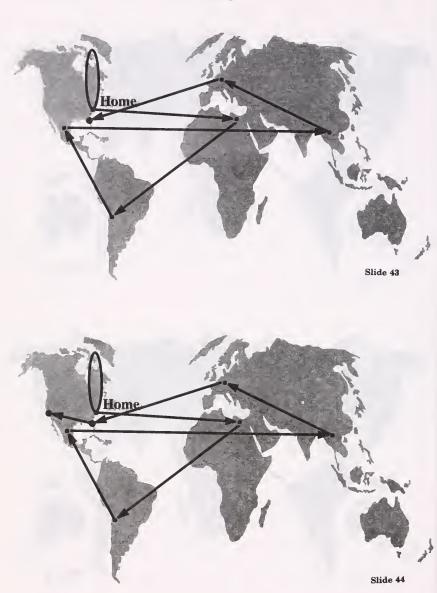
Slide 34















Carnegie Mellon University Software Engineering Institute

Testimony of Richard Pethia

Manager, Trustworthy Systems Program and CERT Coordination Center Software Engineering Institute Carnegie Mellon University

Before the

Permanent Subcommittee on Investigations

U.S. Senate Committee on Governmental Affairs

June 5, 1996

Cernegie Mellon University Pittsburgh, Pennsylvania 15213-3890 (412) 268-7700 FAX: (412) 268-5758

- - *

Introduction

Mr. Chairman and Members of the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs:

My name is Richard Pethia. I manage the Trustworthy Systems Program and the CERT SM Coordination Center (CERT/CC) at the Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania.

Thank you for the opportunity to testify on the role of the CERT Coordination Center in addressing the security of computer information systems and networks. Today I will give you some background on the CERT/CC, describe the trends we have observed while responding to computer security incidents on the Internet, discuss near term steps that I believe can be taken to address today's problems, and consider what the future holds.

Background

The CERT Coordination Center is located at the Carnegie Mellon University Software Engineering Institute in Pittsburgh, Pennsylvania.

The SEI was established in 1984 as a federally funded research and development center in response to the "software crisis." We were established through a competitive procurement process, initiated by the Department of Defense with the approval of Congress. Operated by Carnegie Mellon and sponsored by the Defense Advanced Research Projects Agency (DAR-PA), the SEI concentrates on technology transition to improve software engineering practice.

Nearly a decade ago, DARPA recognized the growing danger of automated and human-driven attacks on the Internet. Following the Internet Worm incident in November 1988, DARPA charged the SEI with setting up a center to coordinate communications among experts during security emergencies and to help prevent future incidents like the worm. In particular, the CERT/CC mission is to

- Operate a 24-hour point of contact to respond to security emergencies on the Internet
- · Facilitate communications among experts working to solve security problems
- Provide a central point for identifying vulnerabilities in computer systems and for working with technology producers to resolve those vulnerabilities
- Serve as a model for, and facilitate the creation of, other computer security incident response teams
- Take steps to increase awareness of information security and computer security issues
- Maintain close ties to the research community and conduct research and development to produce methods and tools that improve the security of networked computer systems

1

June 5, 1996

Since the inception of its response team, the SEI has responded to over 7,600 security incidents affecting tens of thousands of Internet-connected sites. In this role, the SEI helps sites identify and correct specific problems in their systems and policies, notifying and working with law enforcement agencies, notifying and working with the vendor community to correct deficiencies in their products, and coordinating incident response activities with other sites affected by the same incident. In addition to incident response, the SEI warns the community of vulnerabilities and widespread attacks through its advisory service. The CERT/CC at the SEI has issued 119 advisories with direct distribution to over 100,000 sites and secondary distribution to millions of others.

The CERT/CC plays both response and prevention roles. Like a fire department, the response efforts are most widely visible; but, also like a fire department, the prevention efforts have the greatest long-term impact. While my comments today focus on the security incidents and trends we have seen, the plans we are developing for the future, with guidance from DARPA, place increased emphasis on CERT/CC research and development activities.

Security Incident Handling Activities

In its response role, the CERT/CC assists computer system administrators within the Internet who report security problems to us. We help the administrators of the affected sites to identify and correct the vulnerabilities that allowed the incident to occur, and we coordinate the response with other sites affected by the same problem. Our staff also works closely with computer vendors to identify and correct vulnerabilities in their products.

The CERT/CC operates in an environment where intruders form a well-connected community and use network services to quickly distribute information on how to maliciously exploit vulnerabilities in systems. Intruders dedicate time to developing programs that exploit vulnerabilities and to sharing information. They have developed their own publications and they regularly hold conferences that deal specifically with tools and techniques for defeating security measures in networked computer systems.

In contrast, the legitimate, often over-worked, system administrators on the network frequently find it difficult to take the time and energy from their normal activities to stay current with security and vulnerability information, much less design patches, workarounds (mediation techniques), tools, policies, and procedures to protect the computer systems they administer.

In helping the legitimate Internet community work together, we face policy and management issues that are perhaps even more difficult than the technical issues. For example, one challenge we routinely face concerns the dissemination of information about security vulnerabilities. Our experience suggests that the best way to help the community to improve the security

June 5, 1996

of their systems is to work with a group of technology producers and vendors to develop workarounds and repairs for security vulnerabilities disclosed to the CERT/CC. To this end, in the absence of a major threat, we do not publicly disclose vulnerabilities until a repair or workaround has been developed, along with directions on how to install it.

Once those conditions have been met, the CERT/CC issues an advisory to the entire Internet community, explaining the problem and detailing the corrective action to be taken. Appendix A lists the advisories we have released to date.

Forum of Incident Response and Security Teams (FIRST)

From the beginning, DARPA recognized that the scale of emerging networks and the diversity of user communities would make it impractical for a single organization to provide universal computer security response support. The CERT model, therefore, presumed the creation of multiple incident response organizations, each serving a particular user group. The challenge was to develop prevention and response capabilities that are sensitive to the cultural differences among communities, that account for the different nature of vulnerabilities encountered, and that provide solutions to problems that can be effectively adopted by the different communities.

The CERT/CC worked closely with a number of other organizations and agencies to help them create their own incident response teams. DARPA collaborated with the National Institute of Standards and Technology (NIST) to create a facility for interaction between these incident response organizations. That initiative resulted in the Forum of Incident Response and Security Teams (FIRST). Within FIRST, the individual response teams focus on specific constituencies (organizations from government, from industry, and from academe) reflecting the international scope of the Internet. Each response team builds trust within its constituent community by establishing contacts and working relationships with members of that community. These relationships enable response teams to be sensitive to the distinct needs, technologies, and policies. FIRST members collaborate on incidents that cross boundaries, and they crosspost alerts and advisories on problems relevant to their constituents.

More than 50 organizations make up the membership of FIRST. For a full list of current FIRST members, see Appendix B.

Incident Trends

The CERT Coordination Center received its first computer security incident report on its first day of operation and has responded to a continuous stream of incidents ever since.

Some incidents are best characterized as pranks or minor vandalism, but others have more serious consequences. For example:

- Two organizations discovered that several individuals had established a
 pirated software archive at their sites. The responsible individuals were
 eventually identified and apparently confessed. The copyrighted material
 involved in the incident was estimated to be worth about two million US
 dollars.
- A large, scientific and engineering organization in the US experienced an incident in which a significant number of their systems were severely compromised. As a result, they were forced to disconnect their entire network from the Internet for a week while rebuilding their systems. The costs involved included the time to rebuild systems, and loss of productivity of 1500 employees, as well as the disruption of information flow caused by the weeklong disconnection.
- A major US high-tech manufacturing organization had 40 systems compromised by an intruder. Although the intruder appeared to be simply using their systems as a base from which to attack other sites, they spent significant amounts of time recovering the compromised systems at their site and on investigative activities associated with the incident. In total, the incident resulted in more than 15,000 hours of lost productivity for the organization.
- Source code for two operating systems copyrighted by two major US vendors was reportedly stolen from compromised computer systems by an intruder. The intruder was later reported trying to trade the stolen source code, via electronic means, in exchange for other intruder programs and tools that could be used to break into systems.

Computer security events occasionally capture public attention and command headlines, such as "High-tech crooks crack Internet security" (USA Today, January 1995); "America Online admits hackers harassing network" (Boston Globe, September 1995); "Hacking theft of \$10 million from Citibank revealed" (Los Angeles Times, August 1995); "Hacking away at the Internet's Web" (Washington Post, November 1995); and "Stop! Cyberthief!" (Newsweek, February 1995).

A

June 5, 1996

However, these sensational events represent only a small fraction of the events that are reported to the CERT/CC and other incident response teams. In 1989, its first full year of operation, the CERT/CC responded to 132 reported security incidents. By calendar year 1995, the number of incidents reported annually had risen to over 2,400. In addition to the increase in incident reports, we are also seeing the following trends.

Intruders demonstrate increased technical knowledge.

In 1988, intruders most often exploited widely known system vulnerabilities, default passwords, and easy-to-guess passwords. These activities continue in 1996. However, more sophisticated intrusions are now common; for example, intruders examine source code looking for new ways to exploit flaws in programs such as those used for electronic mail.

Intruders are abusing poorly assembled or configured systems to exchange pirated software, information on credit card numbers, and information on sites that have been compromised. Among the site information they share are the identities of compromised hosts, accounts, and passwords.

 Intruders demonstrate increased understanding of network topology and operations. They are becoming more sophisticated and presenting new and increasingly complex methods of attack.

Intruders monitor the Internet looking for new hosts or sites connecting to the Internet. These hosts/sites are often not fully configured before connecting, and are therefore vulnerable to attacks.

Intruders install packet spiffers, programs that capture data (such as user identifications and passwords) from information packets as they travel over the network.

Most recently, intruders have been exploiting vulnerabilities associated with the World Wide Web to gain unauthorized access to systems that have not installed corrections to the vulnerabilities.

They also "spoof" computer addresses, resulting in allowed connections that would not otherwise be permitted.

Of the 346 incidents closed during the first quarter of 1996, 7.5 percent involved these new, sophisticated methods, including packet sniffers, spoofing, and infrastructure attacks (and 20 percent resulted in total compromises of systems, in which intruders gain "super-user" privileges). This represents a significant increase in such attacks.

Attacks on the network infrastructure are increasing.

With their sophisticated technical knowledge and understanding of the network, intruders are increasingly exploiting network interconnections. They move easily through the infrastructure, attacking it all. The intruders have targeted for attack network name servers, network service providers, and major archive sites.

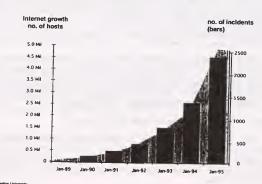
Infrastructure attacks are even more threatening because legitimate network managers and administrators typically think about protecting systems and parts of the infrastructure rather than the infrastructure as a whole. Not only do automated tools make it easier for sophisticated intruders to find and exploit vulnerabilities, but these tools also enable the less knowledgeable to do the same thing. For example, even technically naive, would-be intruders can scan the Internet looking for new hosts/sites and for particular vulnerabilities. By sharing easy-to-use tools, successful intruders increase their population and their impact.

 Intruders are increasingly cloaking their behavior through use of Trojan horses and cryptography.

The intruders hide their existence on hosts through the use of Trojan horse programs, programs that have been altered so that they do more than what is expected. For example, the intruders have altered the login program so that the program still allows users to login to a system, but also allows an intruder lo in without the activity showing up in the system logs.

Intruders also encrypt output from their intrusions. For example, they have encrypted packet sniffer output logs. This makes it difficult or impossible to determine what information has been captured. Site information and passwords thus remain compromised.

Carnege Meton University Software Engineering Institute



Increased Number of Incidents

June 5, 1996

Other Significant Trends

While the intruders are becoming more proficient at their work, other trends that exacerbate the problem are also evident.

 There is a continuing movement to distributed, client-server, and heterogeneous configurations.

As the technology is being distributed, the management of the technology is often distributed as well. In these cases, system administration and mangement often falls upon people who do not have the skill needed to operate their systems securely.

- There is no evidence of improvement in the security features of most products. We routinely receive reports of new vulnerabilities. In fact, in 1995 the CERT/CC received an average of 35 new reports each quarter. In the last two quarters, that number has increased to 65 and 92 reports respectively.
- Engineering for ease of use is not being matched by engineering for ease of secure administration.

Today's software products, workstations and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, many of these products are still difficult to configure and operate securely. This gap will lead to increasing numbers of vulnerable systems.

 Increases in the use of computers and networks are ongoing and dramatic. The technology has become an integral part of most organizations' operations.

Computers have become such an integral part of American business and government that computer-related risks cannot be separated from general business risks. In addition, the widespread use of databases leaves the privacy of individuals at risk. New, valuable government and business assets are now at risk over the Internet.

Customer and personnel information may be exposed to intruders. Financial data, intellectual property, and strategic plans may be at risk.

Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives.

 Information infrastructures are increasingly complex and dynamic. At the same time, there is a lack of adequate knowledge about the network and about security.

The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, anonymous FTP servers, or Web sites result in vulnerabilities that intruders can exploit. Even one naive user with an easy-to-guess password increases the organization's risk.

When vendors release patches or upgrades to solve security problems, organizations' systems are not necessarily upgraded. The job may be too time-consuming or complex for the system administration staff to handle.

Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply. Training will solve only part of this problem.

· Comprehensive solutions are lacking.

Security audits and evaluations often only skim the surface of the technology, missing major vulnerabilities. Among security-conscious organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. As these solutions are not foolproof, the organizations are lulled into a false sense of security and become less vigilant.

At the development level, vendors are not seeking comprehensive solutions either. Technology evolves so rapidly that vendors concentrate on time-to-market. Until their customers demand products that are more secure, the situation is unlikely to change.

What Can be Done Today

While the security problem is complex and growing, there are steps that can be taken to mitigate the risks.

 Support the growth and use of global detection mechanisms; use incident response teams to identify new threats and vulnerabilities.

The CERT/CC and other response teams have demonstrated effectiveness at discovering and dealing with vulnerabilities and incidents. Ongoing operation and expansion of open, wide area networks will benefit from stronger response teams and response infrastructures.

 Encourage development of security improvement services by network service and infrastructure providers.

Many network service providers are well positioned to offer security services to their clients. These services should include helping clients install and operate secure network connections as well as mechanisms to disseminate vulnerability information and corrections rapidly.

 Build programs to increase awareness of security issues and share lessons learned among government agencies and industry.

Organizations often are vulnerable because they are not aware of the risks. Organizations that have suffered attacks often are unwilling to discuss their problems for fear of loss of confidence by their customers. Mechanisms should be established to support the sanitizing and disseminating of data on security problems, data that helps the networked community understand the scope and cost of the overall problem.

 Support the development of techniques for comprehensive, continuous risk identification and mitigation programs.

Network operators need guidance in the form of secure network management models, security assessment techniques, and techniques needed to establish ongoing security improvement programs. These programs must keep pace with rapidly changing threats and technology, must strongly emphasize technology, and must become part of routine practice rather than simple, periodic audits against a static policy.

Invest in security training for users and system administrators.

Building, operating, and maintaining secure networks are difficult tasks and there are few educational and training programs that prepare people to perform these tasks. Ongoing operation of secure networks will require higher levels of skill than are evident today.

 Use available technology for configuration management, network management, auditing, intrusion detection, firewalls, guards, wrappers, and cryptography.

Acquisition and operations organizations must recognize the need for, and be encouraged to invest in, technology that is effective at dealing with the security threat.

June 5, 1996

Develop comprehensive system/security administrators' toolkits.

Acquisition and operations organizations should drive the market for comprehensive security toolkits that support network administrators efforts to operate secure systems. While many tools are available today, these tools do not provide comprehensive solutions to the security problem. Comprehensive toolkits will only be developed when technology users demand them from computer vendors.

Steps for the Future

Today, there is rapid movement toward increased use of interconnected networks for commerce, research and development, entertainment, education, operation of government, industry, and academic organizations; and support of delivery of health and other human services. While this trend promises many benefits, it also comes with many risks. Techniques for securing systems that have worked in the past will not be effective in the world of unbounded networks, mobile computing, distributed applications, and dynamic computing that we are beginning to see with languages such as JAVA.

To reap the promise of these emerging networks, ongoing research is needed in the areas of security architectures and models for unbounded domains; techniques that allow development and operation of systems that are robust enough to detect and recover from attacks; techniques and mechanisms to identify, repair and deploy corrections to flawed software in operational systems; and operational models and mechanisms that allow detection of wide-spread, distributed attacks, diagnosis of attack techniques, and rapid development and deployment of preventive measures.

Maintaining a long-term view and investing in research toward systems and operational technqiues that yield networks capable of surviving attacks while protecting sensitive data, is critical.

Appendix A: CERT(sm) Advisories

The following advisories have been issued to date. Complete text of the advisories and other security information can be found at

http://www.cert.org

- CA-88:01.ftpd.hole
- · CA-89:01.passwd.hole
- CA-89:02.sun.restore.hole
- CA-89:03.telnet.breakin.warning
- CA-89:04.decnet.wank.worm
- CA-89:05.ultrix3.0.hole
- CA-89:06.ultrix3.0.update
- CA-89:07.sun.rcp.vulnerability
- CA-90:01.sun.sendmail.vulnerability
- CA-90:02.intruder.warning
- CA-90:03.unisys.warning
- CA-90:04.apollosuid.vulnerability
- CA-90:05.sunselection.vulnerability
- CA-90:06a.NeXT.vulnerability
- CA-90:07.VMS.ANALYZE.vulnerability
- CA-90:08.irix.mail
- CA-90:09.vms.breakins.warning
- CA-90:10.attack.rumour.warning
- CA-90:11.Security.Probes
- CA-90:12.SunOS.TIOCCONS.vulnerability
- CA-91:01a.SunOS.mail.vulnerability
- CA-91:02a.SunOS.telnetd.vulnerability
- CA-91:03.unauthorized.password.change.request

- CA-91:04.social.engineering
- CA-91:05.Ultrix.chroot.vulnerability

- CA-91:06.NeXTstep.vulnerability
- CA-91:07.SunOS.source.tape.vulnerability
- CA-91:08.systemV.login.vulnerability
- CA-91:09.SunOS.rpc.mountd.vulnerability
- CA-91:10.SunOS.lpd.vulnerability
- CA-91:10a.SunOS.lpd.vulnerability
- CA-91:11.Ultrix.LAT-Telnet.gateway.vulnerability
- CA-91:12.Trusted.Hosts.Configuration.vulnerability
- CA-91:13.Ultrix.mail.vulnerability
- CA-91:14.IRIX.mail.vulnerability
- CA-91:15.NCSA.Telnet.vulnerability
- CA-91:16.SunOS.SPARC.Integer_Division.vulnerability
- CA-91:17.DECnet-Internet.Gateway.vulnerability
- CA-91:18.Active.Internet.tftp.Attacks
- CA-91:19.AIX.TFTP.Daemon.vulnerability
- CA-91:20.rdist.vulnerability
- CA-91:21.SunOS.NFS.Jumbo.and.fsirand
- CA-91:22.SunOS.OpenWindows.vulnerability
- CA-91:23.Apollo.crp.vulnerability
- CA-92:01.NeXTstep.configuration.vulnerability
- CA-92:02.Michelangelo.PC.virus.warning
- CA-92:03.Internet.Intruder.Activity
- CA-92:04.ATT.rexecd.vulnerability
- CA-92:05.AIX.REXD.Daemon.vulnerability
- CA-92:06.AIX.uucp.vulnerability
- CA-92:07.AIX.passwd.vulnerability
- CA-92:08.SGI.lp.vulnerability
- CA-92:09.AIX.anonymous.ftp.vulnerability
- CA-92:10:AIX.crontab.vulnerability
- CA-92:11:SunOS.Environment.vulnerability
- CA-92:12.REVISED.SunOS.rpc.mountd.vulnerability
- CA-92:13.SunOS.NIS.vulnerability
- CA-92:14.Altered.System.Binaries.Incident
- CA-92:15.Multiple.SunOS.vulnerabilities.patched

- CA-92:16.VMS.Monitor.vulnerability
- CA-92:17.HP.NIS.ypbind.vulnerability
- CA-92:18.VMS.Monitor.vulnerability.update
- CA-92:19.Keystroke.Logging.Banner.Notice
- CA-92:20.Cisco.Access.List.vulnerability
- CA-92:21.ConvexOS.vulnerabilities
- CA-93:01.REVISED.HP.NIS.ypbind.vulnerability
- CA-93:02a.NeXT.NetInfo._writers.vulnerabilities
- CA-93:03.SunOS.Permissions.vulnerability
- CA-93:04a.Amiga.finger.vulnerability
- CA-93:05.OpenVMS.AXP.vulnerability
- CA-93:06.wuarchive.ftpd.vulnerability
- CA-93:07.Cisco.Router.Packet.Handling.Vulnerability
- CA-93:08.SCO.passwd.Vulnerability
- CA-93:09.SunOS.expreserve.vulnerability
- CA-93:09a.SunOS.expreserve.vulnerability
- CA-93:10.anonymous.FTP.activity
- CA-93:11.UMN.UNIX.gopher.vulnerability
- CA-93:12.Novell.LOGIN.EXE.vulnerability
- CA-93:13.SCO.Home.Directory.Vulnerability
- CA-93:14.Internet.Security.Scanner
- CA-93:15.SunOS.and.Solaris.vulnerabilities
- CA-93:16.sendmail.vulnerability
- CA-93:16a.sendmail.vulnerability.supplement
- CA-93:17.xterm.logging.vulnerability
- CA-93:18.SunOS.Solbourne.loadmodule.modload.vulnerability
- CA-94:01.ongoing.network.monitoring.attacks
- CA-94:02.Revised.Patch.for.SunOS.mountd.vulnerability
- CA-94:03.AIX.performance.tools
- CA-94:04.SunOS.rdist.vulnerability
- CA-94:05.MD5.checksums
- CA-94:06.utmp.vulnerability

- CA-94:07.wuarchive.ftpd.trojan.horse
- CA-94:08.ftpd.vulnerabilities
- CA-94:09.bin.login.vulnerability
- CA-94:10.IBM.AIX.bsh.vulnerability
- CA-94:11.majordomo.vulnerabilities
- CA-94:12.sendmail.vulnerabilities
- CA-94:13.SGI.IRIX.Help.Vulnerability
- CA-94:14.trojan.horse.in.IRC.client.for.UNIX
- CA-94:15.NFS.Vulnerabilities
- CA-95:01.IP.spoofing.attacks.and.hijacked.terminal.connections
- CA-95:02.binmail.vulnerabilities
- CA-95:03.telnet.encryption.vulnerability
- CA-95:03a.telnet.encryption.vulnerability
- CA-95:04.NCSA.http.daemon.for.unix.vulnerability
- CA-95:05.sendmail.vulnerabilities
- CA-95:06.satan
- CA-95:07.vulnerability.in.satan.
- CA-95:07a.REVISED.satan.vul
- CA-95:08.sendmail.v.5.vulnerability
- CA-95:09.Solaris.ps.vul
- CA-95:10.ghostscript
- CA-95:11.sun.sendmail-oR.vul
- CA-95:12.sun.loadmodule.vul
- CA-95:13.syslog.vul
- CA-95:14.Telnetd_Environment_Vulnerability
- CA-95:15.SGI.!p.vul
- CA-95:16.wu-ftpd.vul
- CA-95:17.rpc.ypupdated.vul
- CA-95:18.widespread.attacks
- CA-96.01.UDP_service_denial
- CA-96.02.bind
- CA-96.03.kerberos_4_key_server

14

June 5, 1996

- CA-96.04.corrupt_info_from_servers
- CA-96.05.java_applet_security_mgr
- CA-96.06.cgi_example_code
- CA-96.07.java_bytecode_verifier
- · CA-96.08.pcnfsd
- CA-96.09.rpc.statd
- CA-96.10.nis+_configuration
- CA-96.11.interpreters_in_cgi_bin_dir

Appendix B: FIRST Membership

Current FIRST members include the following organizations:

- 1. AFCERT (US Air Force)
- 2. ANS
- 3. Apple Computer
- 4. ASSIST (US Dept. of Defense)
- 5. AUSCERT (Australia)
- 6. Bellcore
- 7. Boeing CERT
- 8. BSI/GISA (German government)
- 9. CCTA (United Kingdom)
- 10. CERT(sm) Coordination Center
- 11. CERT-IT (Italy)
- 12. CERT-NL (SURFnet-connected sites)
- 13. CIAC (US Dept. of Energy)
- 14. Cisco Systems
- 15. DFN-CERT (Germany)
- 16. DISA (MILNET)
- 17. Digital Equipment
- 18. DOW USA
- 19. EDS
- 20. General Electric Company
- 21. Goddard Space Flight Center
- 22. Goldman, Sachs and Company
- 23. Hewlett-Packard
- 24. IBM-ers
- 25. ILAN (Israeli academic)
- 26. JANET CERT (United Kingdom academic)
- 27. JP Morgan
- 28. MCI
- 29. Micro-BIT Virus Center (Germany)

June 5, 1996

- 30. Motorola
- 31. NASA
- 32. NASIRC (NASA)
- 33. NAVCIRT (US Navy)
- 34. NIST/CSRC
- 35. NORDUnet (connected sites)
- 36. Northwestern University
- 37. Purdue University
- 38. Penn State University
- 39. RENATER (France)
- 40. Security Emergency REsponse Center (SAIC)
- 41. Silicon Graphics
- 42. Small Business Administration
- 43. Stanford University
- 44. Sun Microsystems, Inc.
- 45. SWITCH-CERT (Swiss academic and research)
- 46. TRW Inc.
- 47. Unisys Corp.
- 48. U.S. Sprint
- 49. Veteran's Health Administration
- 50. Westinghouse Electric Corporation
- 51. UK Defense Research Agency

TESTIMONY OF RICHARD G. POWER, EDITOR, COMPUTER SECURITY INSTITUTE BEFORE THE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, U.S. SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS

Wednesday,

June 5, 1996

Mr. Chairman and Members of the Subcommittee,

The "1996 CSI/FBI Computer Crime and Security Survey" was conducted by CSI and composed of questions submitted by the Federal Bureau of Investigation (FBI) International Computer Crime Squad's San Francisco office. Both CSI and the FBI hope that the results of this survey will be used to better understand the threat of computer crime and provide law enforcement with some basic information that can be used to address this problem more effectively.

CSI, established in 1974, is a San Francisco-based association of information security professionals. It has thousands of members worldwide and provides a wide variety of information and education programs to assist practitioners in protecting the information assets of corporations and governmental organizations.

The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, has established International Computer Crime Squads in selected offices throughout the United States. The mission of these squads is to investigate violations of Computer Fraud and Abuse Act of 1986, including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes where the computer is a major factor in committing the criminal offense.

THE NATURE OF THE THREAT

There is a serious problem.

The *1996 CSI/FBI Computer Crime and Security Survey" offers some evidence. For example, 42% of respondents acknowledged that they had experienced unauthorized use of computer systems within the last 12 months. And we're not talking about users playing solitaire on company time—respondents reported a diverse array of attacks from brute force password guessing (13.9% of attacks) and scanning (15% of attacks) to denial of service (16.2% of attacks) and data diddling (15.5% attacks).

The figures concerning data diddling in financial institutions (21% of attacks) and medical institutions (36.8% of attacks) were higher than both the averages for other specific industry segments and the overall average. This data is disturbing. Private medical records, financial transactions and credit histories are at risk.

Respondents reported that their networks were being probed with frequency from several access points. Over 50% reported incidents on their internal networks and almost 40% reported frequent incidents through both remote dial-in and Internet connections. These results tear at the "conventional wisdom" that 80% of the information security problem is due to insiders (i.e. disgruntled or dishonest employees, contractors, etc.)

Over 50% of respondents said that the information sought in probes would be of use to U.S.-owned corporate competitors. Over 50% also said that they considered U.S.-owned corporate competitors likely sources for eavesdropping, system penetration and other forms of attack. Foreign competitors and foreign government intelligence services also drew double-digit numbers as likely sources of attack. These results indicate that another bit of "conventional wisdom"—i.e., that "hackers" from the electronic underground and disgruntled or dishonest employees are the biggest problems—may be ill-founded.

Other studies corroborate CSI's findings in different ways.

According to "Trends in Intellectual Property Loss," a study from American Society for Industrial Security (ASIS), potential losses from intellectual property theft for U.S.-based companies are estimated to be \$24 billion annually. The ASIS study also ranked hacking second only to pre-text phone calls (i.e., social engineering) as a means of acquisition.

According to the 1996 Ernst & Young/Information Week survey, 80% of respondents considered employees a threat to information security, 70% considered competitors a threat to information security, and almost 50% had experienced financial losses due to an information security incident.

According to a 1995 study from East Michigan State University, over 40% of respondents had been the targets of computer crimes at least 25 times. The study also indicated dramatic increases in many types of computer crime (e.g., a 77% increase in theft of trade secrets and a 95% increase in unauthorized access to computer files).

According to the General Accounting Office, the U.S. Defense Department may have suffered as many as 250,000 attacks on its computer systems last year and the number of such attacks may be doubling each year.

But even if you are skeptical of the data yielded in such studies, a glance at recent newspaper headlines should give you a feel for the scope of the problem.

In 1994, IBM, General Electric and NBC were hacked over Thanksgiving Day weekend. The alleged perpetrators, a mysterious group dubbing itself "The Internet Liberation Front" caused major disruptions. In 1995, Citibank was hit by Russian hackers who illegally transferred over \$10 million to separate accounts around the world, using a laptop PC.

Recently, a former software engineer for Intel Corporation pled guilty to charges that he stole Pentium chip production secrets, worth millions of dollars, and gave them to a rival computer company. Also, in recent weeks, it was revealed that several employees of the Social Security Administration allegedly passed information on 11,000 people (including their Social Security numbers and mothers' maiden names) to a credit card fraud ring.

In another widely reported incident, FBI investigators armed with a court-ordered wiretap and a sophisticated program called Intruder Watch (I-Watch), tracked down an alleged hacker who had compromised computer networks at many sensitive sites including Harvard University, NASA and the Los Alamos Naval Laboratory.

These incidents weren't reported because they were exceptional, they were exceptional because they were reported. Less than 17% of respondents to the CSI/FBI survey reported incidents to law enforcement; over 70% cited negative publicity as the reason.

MANY ORGANIZATIONS ARE UNPREPARED

Perhaps the most disturbing data relates to the level of preparedness within organizations.

Over 50% of respondents don't have a written policy on how to deal with network intrusions.

Over 60% of respondents don't have a policy for preserving evidence for criminal or civil proceedings.

Over 70% of respondents don't have a "Warning" banner stating that computing activities may be monitored. (Absence of "Warning" banners hampers investigations and exposes an organization to liability.)

Over 20% of respondents don't even know if they've been attacked. And as already mentioned, less than 17% of respondents who experienced intrusion(s) indicated that they reported it to law enforcement, and over 70% cited fear of negative publicity as the primary reason for not reporting.

WHAT NEEDS TO BE DONE

It is our view that the preponderance of evidence indicates that the problem of computer crime is only getting worse. And although the heated debate over the U.S. export restrictions on cryptography would seem to suggest otherwise, encryption is not a panacea. All organizations (whether public sector or private sector) must develop a comprehensive information security plan. Encryption is a vital component, but it is not a complete solution.

There is an insufficient level of commitment to information security.

A serious commitment to information security translates into budget items for building information security staffs as well as providing them with training to keep abreast of emerging trends and empowering them with sophisticated technologies.

A serious commitment to information security also means conducting in-depth, periodic risk analysis in order to understand the nature of the threat as it relates to the particulars of a specific organization as well as developing strong, enforceable policies on a broad range of information security issues.

Security awareness for users is also essential. Organizations that don't already have such a program in place must implement one immediately. Those that already have a program in place must augment, update and intensify its scope.

Even physical security is often overlooked as well.

There is also a great need for an emphasis on information security in computer science curriculum and on computer ethics as a critical aspect of good citizenship.

The high-tech vendors of operating systems, applications and hardware must begin to pay more than lip service to information security. Since the dawn of the desktop PC, the emphasis has been on ease of use, speed and connectivity. This attitude must change. Security can no longer be ignored. And although there are many excellent third-party security products from firewalls to Fortezza cards, until the underlying information systems architectures are developed with a greater respect for security issues, serious vulnerabilities will continue to be exploited.

Finally, there is a need for greater cooperation between the private sector, academia and the government. There is much to be done and too little time to do it. There are many excellent champions who have been working tirelessly—e.g., Scott Chamey of the U.S. Justice Department, Professor Eugene Spafford of Computers, Operation, Audit, Security and Technology (COAST) at Purdue University, and CSI's own members in Fortune 500 corporations, government agencies and universities. But is imperative that common ground be found in order to meet the "current and future danger."

ADDENDUMS

For your perusal, I have also submitted a list of additional materials that outline the scope of threats, risks, vulnerabilities and counter-measures, these include: CSI/FBI 1996 Computer Crime & Security Survey Current & Future Danger: CSI Primer on Computer Crime and Information Warfare CSI Special Report on Information Warfare CSI Special Report on Electronic Commerce CSI 1995 Internet Security Survey CSI 1995 Crypto Survey

ruch

Statement for the Record

329

"Foreign Information Warfare Programs and Capabilities"

John M. Deutch Director of Central Intelligence

25 June 1996

Good morning Mr. Chairman and members of the Subcommittee.

I wish to thank you for inviting me to appear before you this morning and speak about foreign information warfare activities against the United States. Protecting our critical information systems and information-based infrastructures is a subject that is worthy of considerable attention and is an issue that I am deeply concerned about.

Over the past 20 years, our nation has witnessed and contributed greatly to a technology revolution. As a result, our government, business, and citizens have become increasingly dependent on an interconnected network of telecommunications and computer-based information systems. These systems, such as the ones comprising the public switched telephone network, serve as a critical backbone for the entire U.S. public and private sectors. U.S. military logistic and operational elements increasingly rely on computer databases and the public telephone network for their classified, as well as unclassified, activities. In addition, the U.S. civil sector also increasingly depends on the uninterrupted and trusted flow of digital information. Day-to-day operations of U.S. banking, energy distribution, air traffic control, emergency medical services, transportation, and many other industries all depend on

reliable telecommunications and an increasingly complex network of computers, information databases, and computerdriven control systems. The Internet has created a global information network that will be an enabler for an exciting new opportunity for digital commerce. This connectivity will create a seemingly seamless world of commerce without borders.

I, like many others in this room, am concerned that this connectivity and dependency make us vulnerable to a variety of information warfare attacks. While attention is focused on computer-based "cyber" attacks, we should not forget that key nodes and facilities that house critical systems and handle the flow of digital data can also be attacked with conventional, high-explosives. These information attacks, in whatever form, could not only disrupt our daily lives, but also seriously jeopardize our national or economic security. Without sufficient planning as we build these systems, I am also concerned that the potential for damage could grow in the years ahead.

I welcome the efforts of this Subcommittee to increase public awareness about these important issues. I believe steps need to be taken to address information system vulnerabilities and efforts to exploit them. We must think carefully about the kinds of attackers that might use information warfare techniques, their targets, objectives, and methods.

There has been much discussion in the press and testimony before this Subcommittee about computer-based intrusions into banks and other financial institutions. We are keenly aware of the several, well-publicized incidents

where computers were used to divert funds by false bank wires, embezzlement, and credit card fraud. To date, these incidents appear to be isolated and the goal limited to theft; that is, high-technology bank robbery. If so, they do not yet pose a serious national security threat to the United States. However, the number and size of these intrusions may grow to the point where they begin to threaten our economic well-being. In addition, we do not fully understand the real source and purpose of these events. Some may be sponsored by foreign adversaries in support of broader political, economic, or military goals.

My greatest concern is that hackers, terrorist organizations, or other nations might use information warfare techniques as part of a coordinated attack designed to seriously disrupt:

- infrastructures such as electric power distribution, air traffic control, or financial sectors;
- international commerce; and
- deployed military forces in time of peace or war.

Virtually any "bad actor" can acquire the hardware and software needed to attack some of our critical informationbased infrastructures. Hacker tools are readily available on the Internet, and hackers themselves are a source of expertise for any nation or foreign terrorist organization that is interested in developing an information warfare capability. In fact, hackers, with or without their full knowledge, may be supplying advice and expertise to rogue states such as Iran and Libya.

It is important to keep in mind, however, that computer-based tools are only one part of an information warfare capability. An adversary also needs highly detailed information about the target and its vulnerabilities, access to the target, and some way to judge how effective the attack will be. While some key U.S. infrastructure targets may be vulnerable to both physical destruction and "cyber" attacks, others are more secure.

Last summer, the National Intelligence Council, with help from a number of Intelligence Community agencies, produced a classified report compiling our knowledge of foreign information warfare plans and programs. Produced at the request of the Pentagon, it focused on foreign efforts to attack the U.S. public switched telephone network and socalled Supervisory Control and Data Acquisition (or SCADA) systems--the computers that control electric power distribution, oil refineries, and other similar utilities. This Intelligence Community publication was the first of its kind on this topic and served as a vehicle for organizing the Intelligence Community's collection and analysis on this subject.

While the details are classified and cannot be discussed here, we have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks. At present, most of these efforts are limited to information dominance on the battlefield; that is, crippling an enemy's military command and control centers, or disabling an air defense network prior to launching an air attack. However, I am convinced that there is a growing awareness around the world that advanced societies, especially the U.S., are increasingly

332

dependent on open, and potentially vulnerable information systems.

333

The Intelligence Community is on the look-out for information that would indicate whether any of the "rogue" states have plans and programs underway to develop an offensive information warfare capability. These countries are very difficult intelligence targets and such programs, by their nature, are almost certainly highly covert and difficult to uncover. In virtually all of them we see advances in computer connectivity and information systems technology that would contribute to an offensive capability. We are alert for any evidence that these technologies are being applied to offensive information warfare programs, as well as information that suggests they may be sponsoring hacker activities.

International terrorist groups clearly have the capability to attack the information infrastructure of the United States, even if they use relatively simple means. Since the possibilities for attacks are not difficult to imagine, I am concerned about the potential for such attacks in the future. The methods used could range from such traditional terrorist methods as a vehicle-delivered bomb-directed in this instance against, say, a telephone switching center or other communications node--to electronic means of attack. The latter methods could rely on paid The ability to launch an attack, however, are hackers. likely to be within the capabilities of a number of terrorist groups, which themselves have increasingly used the Internet and other modern means for their own communications. The groups concerned include such wellknown, long-established organizations as the Lebanese

Hizballah, as well as nameless and less well-known cells of international terrorists such as those who attacked the World Trade Center.

As I noted earlier, many of the tools and technologies needed to penetrate computer systems and launch information warfare attacks are readily available to foreign adversaries. However, we need to remember that a threat is comprised not only of a <u>capability</u>, but also the <u>intent</u> to conduct an attack.

There are a number of activities underway designed to improve our ability to quantify the information system threat to our critical information systems.

- First, we have initiated new collection activities designed to uncover evidence of foreign intent to attack our systems. Some of these initiatives involve traditional intelligence resources such as HUMINT and SIGINT. Unfortunately, obtaining additional information on foreign information warfare plans and programs will take some time.
- Second, we are working closely with the FBI and Department of Justice on this issue. I recognize that information warfare threat analysis is a non-traditional intelligence problem requiring non-traditional sources of data. One effort looks for foreign sponsorship of U.S.based computer hacking activities as well as for evidence of organized crime involvement.
- Third, both the law enforcement and Intelligence Communities are attempting to forge working relationships with the private sector, including U.S. corporations and academic institutions. As we all know, the private

sector is being "hit" every day by hackers. I believe that foreign organized crime is behind some of these events and we are eliciting the private sector's help in looking for evidence of foreign involvement and sponsorship. However, obtaining computer intrusion data from U.S. banks, telecommunications companies, and other institutions has been difficult. Although the situation is improving, many of these firms are still reluctant to share information on intrusions for fear of losing consumer confidence. I know the Subcommittee witnessed this problem first-hand several weeks ago at your last hearing. We are working hard to develop a relationship with industry based on trust and confidentiality.

- Fourth, the intelligence agencies are devoting additional resources to information system threat analysis. For example, analysts at CIA are developing methods to assess the status of foreign information warfare programs. At DIA, analysts are working on ways to understand the warning indicators signaling that a major information warfare attack against the United States is planned or imminent.
- Fifth, in order to provide an increased Intelligence Community information warfare focus, the Deputy Secretary of Defense and I are looking to reorganize existing efforts and create a new center at the National Security Agency.
- Finally, the National Intelligence Council is preparing a National Intelligence Estimate on this subject. This NIE will build on their report produced last summer and cover many of the topics I have discussed this morning. Participants include not only the various intelligence agencies, but also the FBI, DISA, the military services computer crime units, and government representatives with

7

liaison responsibility to the major telecommunications providers. I have directed the National Intelligence Council to complete this effort by 1 December.

I am convinced that organized information warfare threat from both state and non-state actors will grow over the next decade as the technology proliferates. I am encouraged by the steps we have taken over the past year to improve our collection and analytic posture on this issue.

However, intelligence and threat analysis are only part of the infrastructure protection process. We also need to determine which systems are most important for the functioning of our society and which are most vulnerable to attack. The steps outlined by Attorney General Reno in the Critical Infrastructure Security study, in which the Intelligence Community participated, is an excellent starting point for government action. Much more needs to be done. I look forward to working with this Subcommittee and others on this issue in the months ahead.

TESTIMONY

RAND

Strategic Information Warfare

Roger C. Molander

Based on: Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare" RAND MR-661-OSD, 1996.

June 1996

National Security Research Division

RAND is a nonprofit institution that seeks to improve public policy through research and analysis. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

Outline of Presentation 1. "Strategic Information Warfare" - What is it? 2. Perspectives on the Issue • Peter Neumann - SRI • Robert Anderson - RAND 3. "The Day After...in Cyberspace" - The Challenge to Crisis Decision-making 4. Unresolved Issues

1. This slide provides an Outline of what we will be going through in this session.

2. I will first provide a brief presentation on the subject of strategic information warfare - explaining why we think this is the appropriate term for the problem that we will be addressing.

I will also describe to you the character and objectives of the strategic information warfare exercises that we have been conducting at RAND for the last sixteen months.

3. Peter Neumann of SRI and Robert Anderson of RAND will then give you additional perspective on the strategic information warfare problem, drawing on their lengthy experience in dealing with both the technological aspects of the information revolution and the issue of information security or, if you prefer, information assurance.

4. We will then present for your consideration an example of the kinds of strategic crises that we employ in the RAND exercises. We will describe the decision-making challenges that a President - or a Congress - might face in dealing with a real strategic crisis in which there is a strong strategic information warfare component - and give you an opportunity to place yourself in an agenda-setting or decision-making role in such a crisis.

5. Finally I will walk through some perspectives obtained from our work to date in this area and present a menu of key unresolved issues related to the strategic information warfare problem - from which an action agenda related to this problem might be constructed.



1. Strategic information warfare can best be thought of as the interesection of two possible revolutions.

2. The first is that ascribed to information.

Few would dispute that advances in information technologies - in particular in computers and communications - are bringing changes to our country and our civilization that are worthy of the name revolution, a word not to be used lightly.

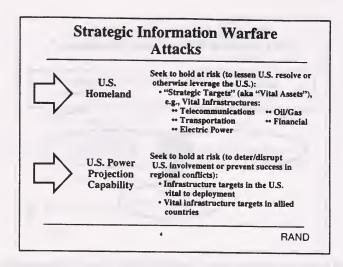
3. At virtually the same time that the information revolution is washing over us, there is taking place in the world of international politics and the derivative realm of warfare (recalling Clausewitz's description of warfare as politics by other means) a change of possibly comparable revolutionary magnitude - in what is called <u>strategic warfare</u>.

In the period of the Cold War strategic warfare came to be synonymous with nuclear warfare.

But then the end of the Cold War came very fast and very unexpectedly. No one had thought much at all about what strategic warfare would be like after the Cold War.

We have a highly developed framework, language, and catechism to deal with strategic nuclear warfare in a bipolar world. But no one had thought much about what strategic wafare would be like in a multi-polar world where our adversaries might have regional rather than global strategic objectives - where they might choose to use nuclear weapons, and possibly other so-called weapons of mass destruction, in a creative fashion to serve regional strategic objectives. And possibly choose to use information warfare tools and techniques for this purpose as well.

4. It is that intersection in these two ongoing revolutions - call it strategic information warfare - that we are addressing here.



1. If you were in the strategic warfare business in the Cold War - them or us - you were principally in the business of holding at risk to nuclear attack key strategic targets (also sometimes called vital assets) and in particular, key infrastructure targets. This "holding key targets in one's nuclear gunsights" was the principal means by which the deterrence of the Cold War was achieved.

2. When we look at the prospect of strategic information warfare, it is again the holding at risk of key infrastructure targets that is the chief concern.

3. There are two principal generic categories of strategic information warfare attacks that appear to warrant careful attention.

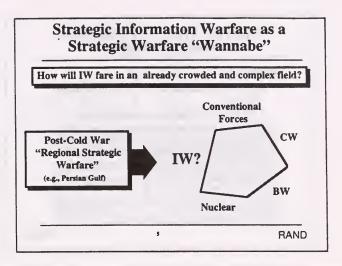
4. The first is a more direct carry over from the Cold war - a direct threat against the U.S. homeland - the posssibility that the same infrastructure targets that were held at risk to <u>destruction</u> by nuclear weapons might be held at risk to <u>disruption</u> by information warfare tools and techniques.

Our chief concern in this regard is probably a peer competitor - a Russia or a China that might successfully develop the capability to exert leverage on the U.S. through an ability to wreak massive disruption in the United States through cyberspace warfare.

5. A second concern is the possibility that an adversary with regional ambitions would attempt to use information warfare tools and techniques to deter or disrupt U.S. involvement - or prevent U.S. success - in regional conflicts in areas such as the Persian Gulf where we have clear vital interests.

One concern in this regard is that an adversary might successfully disrupt U.S. deployment to such a region through attacks on U.S. infrastructure targets key to that deployment - to the point where the forces arrive too late to avert a vital strategic loss, or maybe not at all.

Alternatively the target might be a key regional ally or coalition member who under strategic information warfare attack might refuse to join a coalition, or quit one in the middle of a war.



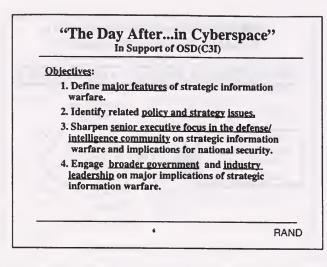
1. But would an adversary choose to use strategic information tools and techniques from among the many other strategic weapons that he might have in his armory? Would attack via cyberspace appear attractive - as potential future adversaries think about various situations in strategic warfare terms?

2. As indicated in this graphic, regional strategic warfare is already a crowded and complex field.

3. When we try to think about how a future regional adversary would conduct a strategic campaign against the United States, we immediately face formidable issues in terms of envisioning the possible strategic objectives that such an adversary might have in, say, the Persian Gulf or East Asia, and the risks and tactics that he might undertake to achieve those abjectives.

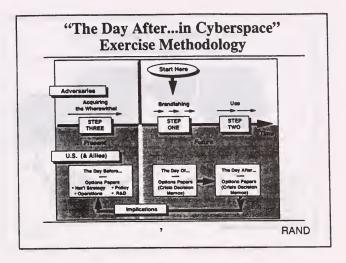
4. Would he risk using chemical or biological weapons - knowing that the first use of any such weapons would almost certainly be judged in strategic warfare terms? Would cyberspace attack be more attractive, say, at the beginning of a strategic campaign? Would an adversary see particular value in the possibility of launching an anonymous cyberspace attack? Would he target current U.S. regional allies or coalition members early? Would the prospect of overwhelming U.S. conventional capability (sustained by the envisioned revolution in military affairs) deter cyberspace attack or attack by weapons of mass destruction?

5. These are the kinds of issues that render thinking about strategic information warfare both challenging and relevant.



1. In December of 1994 OSD(C3I) asked RAND to take a methodology that we had been using to examine the counter-nuclear proliferation problem - that goes by the name "The Day After..." - and apply it to the strategic information warfare problem with the objectives shown here.

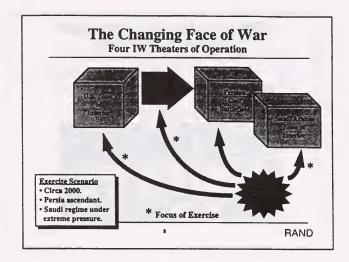
2. [Read through list of Objectives]



1. This chart summarizes the methodology of these exercises.

2. The first two steps in the exercises are set in a future crisis context. The challenge to the participants is to decide which issues and options should go forward to the President in the crisis.

3. In the third and final step in the exercises participants return to the present and consider the challenge of deciding which issues in this area might be ripe for Presidential decision-making in the relatively near future.



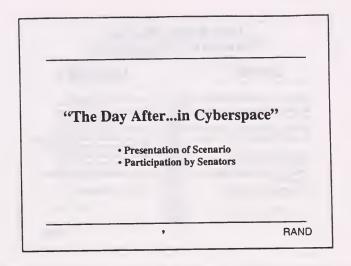
1. The exercise that we are about to go through, set in the year 2000, is brought on by both an internal and external threat to the Saudi monarchy. Another problem is anti-interventionist political groups in the United States. We envision a situation in which all of these parties employ strategic information tools and techniques against the United States and its allies.

2. As a consequence, in contrast to the situation in the past where we thought in terms of a single overseas theater of operations, we are now looking at the possibility of four theaters of operation in which information warfare issues will be of concern. [Go through four theaters.]

3. We would now like to place you into this future context and get your perspectives on what might be done in such a crisis.

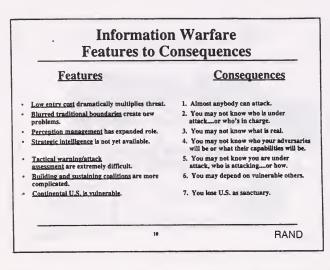
4. We would ask you to envision that you have been invited to attend a pre-meeting of principals minus the President in advance of an NSC Meeting where the task is to prepare an issues an options papaer for the President. You might envision yourself there as a majority or minority leader, as a trusted friend and advisor to the President, or as a cabinet secretary who would naturally attend such a meeting. Most importantly, you're at the meeting.

5. I would now like to introduce Andy Riddile of National Security Research, Inc. who along with Peter Wilson, Bob Anderson and others at RAND were part of the the design team that produced the original version of this exercise.



Reference: Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare" RAND MR-661-OSD, 1996.





1. Stepping back from our experience in working on this problem, we see the following key features as essential to understanding strategic information warfare.

• Low Entry Cost. Because of the low cost of microcomputing and computer networking, we have to accept the possibility that almost anyone can launch an attack using these techniques.

• <u>Blurred Boundaries</u>. Geographical, bureaucratic, and jurisdictional boundarties are all blurred in this realm of warfare. So are other distiunctions such as foreign/domestic, public/ private, military/commercial, war/crime, and even war/peace. This will result in increased ambiguities, disputes, and vulnerabilities.

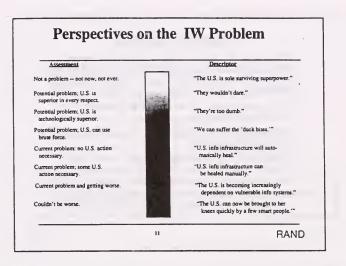
• <u>Perception Management</u>. There will be increased capability for nonstate and state actors to manipulate information key to perceptions in competition with authoritative sources. This will decrease capability to build and sustain domestic support for controversial actions.

 <u>Strategic Warning</u>. Classical intelligence collection and analysis methods are not readily adapted to this intelligence challenge. Collection targets are difficult to identify. The rapidly changing nature of the threat makes intelligence resource allocation much more difficult. Vulnerabilities and target sets are not well understood.

• <u>Tactical Warning and Attack Assessment</u>. There is currently no adequate tactical warning system for distinguishing between strategic IW attacks and other kinds of cyberspace activities, nor is there any organized means of attack assessment.

• <u>Coalitions</u>. Forming and sustaining coalitions will be more difficult as allies and coalition partners face and experience strategic information warfare attack.

• <u>Vulnerable Homeland</u>. Finally, there is the phenomenon of a potentially vulnerable homeland. This almost unprecedented loss of sanctuary will have a profound impact on the future course of this problem.



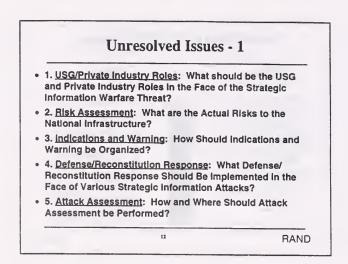
1. Participants in the exercise expressed a wide and telling range of perspectives on the gravity of the IW threa as depicted in this graphic.

2. As you can infer from previous testimony on this problem, it is very difficult at this point in time to provide any kind of summary assessment of just how bad this problem might be today or how bad it might become in the future.

3. Will IW be a new but subordinate facet of warfare in which the United States and its allies readily overcome their own potential cyberspace vulnerabilities and gain and sustain whatever tactical and strategic military advantages that might be available in this arena?

4. Or will the changes in conflict wrought by the ongoing information revolution be so rapid and profound that the net result is a new and grave threat to traditional military operations and U.S. society that fundamentally changes the future character of warfare?

5. In terms of our experience with this basic question, we have observed that as the participants progressed through the exercise, their perspective on the IW threat almost invariably tended to move downward along this graphic.



1. Considering the early stage of development of this overall issue, there is a wide spectrum of areas in which issues arise and in which possible actions might be undertaken.

2. Based on our exercise experience and analysis, we see several areas as potential strong candidates for early action:

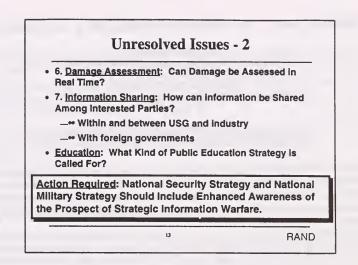
• <u>USG/Private Industry Role</u>. A badly needed first step is the assignment of a focal point for federal government leadership in support of a coordinated U.S. response to the strategic IW threat. Most participants believed that this focal point should be located in the Executive Office of the President to achieve the necessary interagency coordination - and carry out the necessary interactions with the Congress and industry on this problem.

• <u>Risk Assessment</u>. There is a need for an immediate risk assessment to determine, to the degree possible, the extent of the vulnerability of key elements of current U.S. national security and national military strategy to strategic information warfare. There is no sound basis for presidential decisionmaking on strategic IW matters without such a risk assessment.

• Indications and Warning. There is a needto establish a formal means of pooling information related to indications and warning in order to increase our ability to determine whether the country is under cyberspace attack.

• <u>Defense/Reconstitution Response</u>. Procedures for responding to a strategic information warfare attack need to be established. There is a particular need for key infrastructures to be prepared to implement reconstitution measures.

 <u>Attack Assessment</u>. Beyond the provision of warning and the implementation of defensive measures, there is a need to be able to assess who is attacking, what has been attacked, and the prospect of additional future attacks.



1. Here are several additional areas that are potential strong candidates for early action:

• <u>Damage Assessment</u>. There is a need to be able to assess as soon as possible the extent of damage from a strategic information warfare attack in order to fashion an appropriate strategic response.

• Information Sharing. There is a need for a more effective means of exchanging information within the government at all levels, within industry, and between government and industry. Information sharing between the intelligence and law enforcement communities constitutes a particularly challenging issue.

2. It is clear from the spectrum of problems cited that strategic information warfare could have a strong impact on National Security Strategy and National Military Strategy:

• <u>National Security Strategy</u>. Once an initial risk assessment has been completed, preparedness for the threat as identified needs to be appropriately addressed in U.S. national security strategy.

• <u>National Military Strategy</u>. Planning assumptions relating to current national military strategy - with its emphasis on maintaining U.S. capability to project power into key regions of Europe and Asia - are obsolescent. Consideration of the possibility of cyberspace attack outside the primary theater of operations need to be accounted for.

Security Risks in the Computer-Communication Infrastructure

Peter G. Neumann Computer Science Laboratory, SRI International Menlo Park, California 94025-3493 Telephone: 1-415-859-2375 Neumann@CSL.SRI.com (Peter G. Neumann) 25 June 1996

Written testimony for the U.S. Senate Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs

Thank you for the invitation to appear before you today. It is a very special privilege for me. (For the record, I have included some of my personal background at the end of this testimony.)

My written statement addresses some of the fundamental risks facing us in our present uses of computer-communications technology, and assess how those risks might change as we depend increasingly on that technology.

These written comments address issues that I understand to be at the heart of the intended scope of these hearings: an assessment of security vulnerabilities and risks in computer-communication systems within the Department of Defense, non-DoD U.S. Government, and private sector (including the NII and its future evolution). I include a few recommendations that might contribute to improved security. In the present context, security implies techniques for the prevention of intentional and – to some extent – accidental misuse in computer-communication systems.

Brief Summary

To give an idea of the scope of this testimony, here are a few talking points.

- We are becoming massively interconnected. Whether we like it or not, we must coexist with people and systems of unknown and unidentifiable trustworthiness (including unidentifiable hostile parties), within the U.S. and elsewhere. Our problems have become international as well as national.
- There are fundamental vulnerabilities in the existing computer-communication infrastructure, and serious risks that those vulnerabilities will be exploited – with possibly very severe effects. Our national infrastructure depends not only on our interconnected information systems and networks, but also the public switched network, the air-traffic control systems, the power grids, and many associated control systems – which themselves depend heavily on computers and communications.
- There are many past cases of security misuse worthy of your attention, such as the 1988 Internet Worm, the Citibank penetration, and the Rome Lab case (Reference 8). (See the attached Reference 3 for a summary of other cases as well.) However, there are many serious security vulnerabilities that have been discovered by friendly parties and fixed before they could exploited. In addition, there have been various cases of misuse of government databases,

Peter G. Neumann

Security Risks in the Infrastructure

including IRS data and law-enforcement data (Reference 9). In general, we have been lucky, but should not count on that in the future as the stakes and risks increase.

- Global problems can result from seemingly isolated events, as exhibited by the early powergrid collapses, the 1980 ARPANET collapse, and the 1990 long-distance collapse – all of which began with single-point failures.
- Our defenses against isolated attacks and unanticipated events are inadequate. Risks include not just penetrations and insider misuse, but also insidious Trojan horse attacks that can lie dormant until triggered.
- Our defenses against large-scale coordinated attacks are even more inadequate. The unintended effects of the nonmalicious 1988 Internet Worm must be interpreted properly – hinting at the devastating effects that could have resulted if that case had been carried out maliciously.
- Reliability and system survivability are closely interrelated with security.
- Attaining dependable security and reliability is a very difficult problem that has not been adequately understood by most people. It is essentially impossible to have any guarantees whatsoever that a system will work properly when and where it is needed. Security and reliability are both weak-link phenomena, and there are far too many weak links.
- Cryptography is an absolutely essential ingredient in achieving confidentiality, user authentication, system authentication, information integrity, and nonrepudiability. U.S. cryptographic policy has generally not been sufficiently oriented toward improving the infrastructure, in that it has been more concerned with limiting the use of good cryptography. U.S. crypto policy has instead acted as a deterrent to better security. (See Reference 6 for an elaboration of that point.)
- In general, efforts to develop and operate complex computer-based systems and networks that must meet critical requirements have been monumentally unsuccessful particularly with respect to security, reliability, and survivability. This is a widespread problem, and is not limited to either government or private-sector systems. (References 3 and 4 provide numerous examples of development fiascos.)

My testimony amplifies all of these points, addressing a few questions that have been suggested to me as being of particular interest to you.

RISKS

What Are the Intrinsic Risks in Our Information Infrastructure?

• Vulnerabilities. Our infrastructure depends on the adequate functioning of many computercommunication systems, including (for example) the public switched network, power distribution, air-traffic control, nuclear-power systems, and - increasingly - the Internet itself. We focus here on the security vulnerabilities, although we observe a relationship with reliability failures and system survivability issues in the presence of adverse conditions. Many of these systems have serious potential security vulnerabilities, exploitation of which could cause massive disruptions. Peter G. Neumann

Security Risks in the Infrastructure

These problems must be properly addressed in the emerging global information infrastructure, particularly as more systems become interconnected. One of the biggest risks is that typically not enough effort is expended on prevention until after a disaster has occurred.

• Security requirements are typically not being met with sufficient assurance in the computer systems and networks that are commercially available today. Most systems are flawed in one way or another, and some of those flaws are potentially very serious. Furthermore, in general, adequate security cannot be attained unless there is adequate reliability – namely, that a system will do what it is expected to do, when it is expected, with some suitably high probability. The converse is also true: a system is not likely to be reliable unless it is adequately secure – for example, because of maliciously caused deviations from expected behavior. (Reference 4 exhibits examples of each type.) Security and reliability are both required for system survivability and may also be required for assuring system safety – although they are not enough by themselves. It is essential that a complete set of requirements be understood in advance, encompassing (for example) security, reliability, safety, and survivability (as needed) and the interactions among them. If these requirements are not clearly defined, the risks are much greater that systems will not do what they ought to do.

• Software development is a labor-intensive effort. Very few large development efforts are developed on time, on budget, and with acceptable functionality. Development of complex systems and complex software requires intelligent, well-trained, experienced individuals, especially when critical requirements are involved. Those individuals typically must have a range of abilities and specialties spanning expertise in technology, systems, hardware, software, management, human factors, and other system aspects. The absence of any particular expertise can and often does reflect adversely in the resulting systems. Each system development has its own characteristics: air-traffic control systems, law-enforcement database systems, medical systems, and nuclear-power plants share some common infrastructure such as operating systems, database management systems, networking, cryptographic techniques and other common security solutions, but each type of system presents special problems of its own. (These problems ar considered further in the section beginning on Page 9.) People who have both system development skills and security expertise are quite rare.

• Crises can have widespread consequences, nationally and even globally. However, responding to crises is difficult. The cause of a problem cannot always be quickly determined. Disseminating remedial actions can be complicated – especially if the infrastructure used for remediation has itself been impaired. The year-2000 problem (discussed below) and the ongoing personal-computer virus problem illustrate the point that there are no quick fixes.

Do Past Incidents Suggest Perils That We May Face in the Future?

• Case histories. Cases experienced in the past span an enormous range, including losses of human lives (particularly in aviation and medical care – see Reference 3), serious injuries, long-term effects on human well-being, and financial integrity and stability of individuals, organizations, and governments. The attached list of cases (Illustrative Risks to the Public in the Use of Computer Systems and Related Technology) (Reference 3) summarizes many cases that I have collected over the past many years. The security-related cases include many serious security flaws, insider misuse, system breakins and penetrations (including one reported case involving the computer system of Senator John McCain, who at the time was a Congressman), trapdoors that can be used to gain surreptitious access, and pest programs such as Trojan horses, viruses, programmed logic bombs

Security Risks in the Infrastructure

and time bombs that can be used to create arbitrary havoc because they are able to operate with all of the permissions normally attributed to the users and systems they have invaded. There are also financial frauds, election irregularities and possible frauds, many cases of accidental and intentional denials of service, satellite television channel spoofs, electromagnetic and other interference (including effects on pacemakers, with renewed warnings concerning microwaves and digital cell-phones), electronic eavesdropping and jamming, and numerous problems related to violations of privacy and proprietary rights. In addition, there are many complicating factors: information-based fraud is becoming increasingly prevalent (San Francisco police report that well over half of the fraud cases are so attributable); the international software theft problem is intensifying, whereby something on the order of one-half of the market value of all software worldwide is attributable to unauthorized copies, according to the Software Publishers Association; electronic attackers may be located anywhere in the world, and are typically very hard to track; international laws are not sufficiently helpful.

• Global implications. Several widespread power blackouts in our now distant memories, the ARPANET collapse of 1980 in which the precursor of the Internet was incapacitated for four hours, and the 11-hour collapse of AT&T's long-distance service of 1990 attributed to a software flaw illustrate one high-risk type of problem in distributed systems – namely, that a fault in a single node can seriously effect every other node in the system. It is significant to note that each of these problems could alternatively have been triggered maliciously by relatively small individual actions. Similarly, in many supposedly secure systems, a single ponetration can often be parlayed into widespread adverse consequences.

• Controls. We are inevitably embarked on a course toward a worldwide information infrastructure that can potentially permit access to computer systems from anywhere, but that will require controls over who has access to what sensitive information and who has the ability to modify or delete data and programs. Existing controls are not adequate. Recent incidents such as a Russian remotely breaking into Citibank computers and the continual discovery of serious security flaws in popular computer systems demonstrate just a few of the security risks in our infrastructure.

• Risks of anecdotal evidence. Anecdotal evidence is by itself generally not convincing enough. However, in computer-communication systems, there is a serious absence of systematic data that is really definitive. Thus, it is very important to examine the enormous existing body of evidence and understand its implications. In addition, it is important to understand that a considerable portion of the evidence is hidden from public scrutiny.

Are Things Happening That We Just Don't Know About?

One of the biggest problems relating to security incidents is that many incidents are hever reported officially, including cases of financial fraud and computer security violations. Furthermore, many exploitations are very difficult to detect and trace – such as interception of unencrypted communications via cell-phone, remote phones, and microwave links, and in some cases even financial losses.

Above all, it is important to keep an overall view on security in the emerging information infrastructure. Security will always be a problem, and it is a problem that cannot be addressed effectively in the small and that cannot be retrofitted onto systems that were not originally designed to be secure. As a consequence, there are many risks. See Reference 3 for a broad examination of vulnerabilities and risks and what can be done to minimize them. Another recent view is provided by Teresa Lunt

Peter G. Neumann

of DARPA (Reference 2).

THE FUTURE

Where Are We Going in the Next 10 Years? Is the concept of an "electronic Pearl Harbor" or a "Global Chernobyl" on the Internet something that the country must take seriously and prepare for? Or are these terms just euphemisms for an ill-defined uneasiness that we feel about the security of our information systems? What threats really exist? What form might a widespread security disaster take? What needs to be done? And over what time period? Are we thinking adequately about the security ramifications in our rush to become Internetted?

• Actually, I do not like to use such popular metaphors, because they tend to trivialize some very difficult problems. However, they do convey the message of the urgent need for a realistic assessment of the risks and what can be done to minimize those risks.

• We will be massively interconnected. Major functions of Government will be automated or semiautomated. Security will always be a major problem, because it is difficult to assure – for technological, operational, and managerial reasons. There is a threat of attacks by outside intruders and misuse by insiders, as well as risks that Trojan horses planted long ago may finally become activated and that backup mechanisms have themselves long since been contaminated. Security has typically been considered only as an afterthought. It must become a fundamental part of our thinking, beforehand, and not after the crises have occurred. In addition, we must address reliability and survivability issues as well, to prevent repetitions of the types of large-scale outages noted above. We would be very foolish not to be proactive with respect to these risks, with short-term measures to shore up the existing infrastructure and long-term measures to plan for the future.

· Desires for privacy and anonymity are generally incompatible with the desire for accountability - that is, the ability to know the identity of participants and what they are doing (for billing purposes in the case of commercial transactions, for scheduling and resource management, and many other purposes). Attempts to create completely anonymous services such as anonymous cash tend to run counter to practical notions of accountability, authenticity, integrity, revocability, nonforgeability and nonrepudiability, and would seriously impair law enforcement when confronted with massive fraud. There are also privacy risks relating to monitoring and surveillance activities - whether those activities are done clandestinely or with full knowledge of system users. Such risks include the misuse of the information that is thus obtained for other than the intended purposes, and harmful effects that can result from dependence on incorrect, misinterpreted, or maliciously falsified information. As discussed in the National Research Council crypto report (Reference 6), escrowing cryptographic keys presents some enormous potential risks that must be considered very carefully in advance. Ideally, a balance must be struck between privacy and accountability, and that balance must be carefully guarded. Therefore, it is desirable to minimize the information that is monitored and to control strictly who has access to it, and also to ensure the correct identity of all individuals engaged in potentially risky activities - whether arising because of monitoring activities or because of being monitored. Otherwise, slight deviations from the desired balance can result in extensive compromise of privacy or accountability (or possibly both!).

 Digital commerce. It would be prudent to tiptoe into the era of digital commerce, beginning with small transactions, until confidence is attained that the infrastructure is ready. Eventually,

25 June 1996.

Security Risks in the Infrastructure

electronic commerce will be commonplace (irrespective of how secure it is), simply because of marketplace factors. However, there must be suitable controls and oversight on the electronic distribution of financial assets and intellectual property, including software and other content.

• There are no easy answers, although everyone always seems preoccupied looking for them. Great care is required to avoid global problems such as in 1980 ARPAnet outage and the 1990 AT&T outage. The oncoming year 2000 is likely to cause surprising reliability problems, resulting from programming languages and operating systems that do calendar arithmetic using two-digit years – for example, with software believing that the year 99 comes *after* the year 00 because 99 is obviously larger than 00! The efforts to fix this problem are decidedly nontrivial, particularly because many computer systems are expected to be affected, some of which were implemented many years ago and are already very difficult to maintain. It is not yet clear whether the year-2000 problem is overhyped, although the estimates of the cost to fix it within Government computers alone are astoundingly high.

• Simple solutions and draconian solutions are both risky. Simplistic solutions such as the V-chip, indecency filters, and other efforts to censor our communications media are at best likely to have little or no positive impact, and at the same time present many negative and counterproductive effects. Similarly, the concept of mandatory crypto-key escrow found in the Escrowed Encryption Initiative is full of potential risks; it would require an extensive infrastructure to make it work securely, and that infrastructure would itself be vulnerable to attack. Furthermore, even if the infrastructure could be made feasible (for example, through nonmandatory commercial key escrow), there are still serious problems that must be overcome - such as the almost total lack of business incentives for escrowing communication keys (whereas there is a business incentive for escrowing storage keys). No matter how many safeguards are in place, there are always risks. Similar comments apply to the socalled Clipper III, whereby certain private keys would have to be escrowed, exposing the concept of public-key cryptography to abuse. In general, systems that require complex operational and administrative procedures are often vulnerable to people who ignore those procedures. In another direction, outlawing computer misuse would not be likely to succeed if the infrastructure still permits fraud, privacy violations, and unethical behavior to occur - and worse yet, to remain undetected. Similarly, outlawing certain forms of cryptography is not likely to succeed, partly because cryptography is already available worldwide, and partly because of the ability to hide information undetectably (through steganographic techniques) without using cryptography. Above all, security is an overall system problem, and requires that there be no significant weak links. Thus, attaining adequate security usually requires much greater effort than people are used to investing. Furthermore, in the absence of colossal losses, people find few incentives to invest in defensive measures. The evolution of U.S. crypto policy is also highly relevant to your Subcommittee, and is reviewed extensively in the just-released National Research Council report (Reference 6).

Another simplistic solution would be to cut the United States off from the Global Information Infrastructure, relying instead on a totally isolated National Information Infrastructure. That seems draconian. The most intelligent solution would be to significantly improve the infrastructure! In that way, the potential benefits could be realized and the risks dramatically reduced.

Security Risks in the Infrastructure

THE ROLES OF GOVERNMENT

What Roles Should Government Play? What Roles Should It Not Play?

• The Government should strive to increase public awareness of the risks, and to work actively toward reducing those risks. The various branches of Government need to work more closely together, both proactively and reactively with respect to crises. Above all, the Government should actively promote steps that improve the security of the infrastructure. I hope that these hearings will help in those directions.

• Government-set standards are not likely to be effective unless they are closely aligned with commercial and consumer interests. The Government must encourage the development of commercially viable systems that can adequately satisfy stringent requirements for security, reliability, survivability, performance, etc. It can do so by encouraging the development of critical system and network components and the establishment of effective criteria for combining those components into complete systems that are strongly secure. It is not enough to merely have a bunch of components; those components must be capable of rapid integration, with high assurance that the overall systems will function securely.

• The Government must take a strong position relating to the protection of personal and corporate privacy. Privacy is something that you often never realized you had until after you have lost it. Defending it requires special care, and a keen awareness of the risks involved. H.R.3011, Security and Freedom Through Encryption (Representative Goodlatte), S.1726, Promotion of Commerce On-Line in the Digital Era (Senator Burns), and S.1587, Encrypted Communications Privacy Act of 1996 (Senator Leahy) all have significant merit.

• The Government must also take a strong position relating to nontrivial individual authentication and system-to-system authentication in computer-related activities. Good system security and good encryption properly implemented are essential for authentication as well as for ensuring privacy. Fixed passwords for user authentication are inherently dangerous, especially when they traverse unencrypted links or reside in system memory, and can be easily captured; some sort of cryptographically or biometrically based authentication is desirable for cases in which penetrations and masquerading represent serious threats.

• The Government must review in great depth the critical role of cryptography in the emerging infrastructure as it relates to need for national well-being in the context of the international evolution of the infrastructure. Good cryptography is absolutely essential for ensuring confidentiality of sensitive information in the private and public sectors, and is also absolutely essential for achieving much greater information integrity and user authentication. It also presents new problems for intelligence-gathering and law-enforcement communities. I sincerely hope that the just completed National Research Council study of U.S. cryptographic policy (Reference 6) will be helpful in your review. (See also Reference 11.)

• The Government must defend itself against anarchy, oligarchy, and other unhealthy forms, and diligently avoid the pitfalls such as those found in Orwell's "1984". There are dangers in underreacting to the security risks discussed here, as well as dangers in overreacting (such as might occur with censorship, outlawing or limiting free speech, outlawing or blocking access to domestic use of good encryption, undermining privacy rights, and microcontrolling media content). There are also corresponding dangers of negative impacts that can result from attempts to overcontrol domestic business in a global marketplace. In general, national security must be understood to

Security Risks in the Infrastructure

include national economic survivability and political stability, as well as military and intelligence strength. The so-called equities should not be pitted against one another as adversaries. Once again, improving the infrastructure would be a major step forward.

• The Government has gotten some useful mileage out of past studies such as those conducted by the National Research Council. (For example, see References 5 and 7.) Even though the concept of "another study" may seem boring, here are a few topics that could benefit from some incisive thinking:

- What should be the research and development priorities relating to the emerging infrastructure? How can we develop meaningfully secure components out of which much more secure systems can be readily configured? What fundamental gaps must be filled – for example, with respect to authentication and proper use of cryptography.
- 2. What can be done to foster the effective development of complex systems, especially those that have critical requirements for security?
- 3. It is time to revisit and broaden the "Computers at Risk" report from 1991 (Reference 5). There has been some significant progress since that report was written (for example, toward the establishment of a comprehensive set of generally accepted security principles, taking certain recommended short-term measures to improve the infrastructure, establishing incident repositories to help promote public awareness, and reevaluating cryptographic export control policies. However, one particular recommendation of that report has still not been adequately addressed how best to represent end-user interests and needs, particularly in the private sector (which NSA and NIST cannot represent). Unless commercial systems are adequate for critical applications, U.S.Government systems will not be adequate for national needs.
- 4. Recognizing the overall system perspective required to achieve adequate security in the infrastructure, it might be desirable to establish a representative working group that cuts across a broad range of fields and interests, including computer and communication technologists, lawyers, and people deeply involved in private-sector applications such as medical information systems and critical control systems, to act as a standing advisory group relating to the evolution of the infrastructure and able to focus on issues such as security and system survivability.
- 5. What can be done to ensure that computer system and software professionals perform in ways that more closely approach engineering disciplines in which there is substantial enforcement of licensing, accreditation, responsibility, ethical behavior, and legal liability, both individually and corporately, and well established incentives for risk management? I am not comfortable with professional societies policing themselves, and I am also not comfortable with state and Federal governments attempting to legislate or micromanage software quality or professional standards. What works for conventional engineering does not seem to work for software, where a single bit in error can have disastrous results. However, I do believe that a thorough study should be made of how best to achieve a level of professionalism in software development that should be absolutely essential when developing very-high-risk systems and particularly, systems with stringent security requirements. Achieving a true professionalism among software personnel is a very difficult task, but certainly worthy of study.

Security Risks in the Infrastructure

All in all, the U.S. Government must be a leader in addressing the difficult problems noted here.

Security is an International Problem

National boundaries are disappearing in the on-line world. The so-called National Information Infrastructure must be viewed as part of a Global Information Infrastructure. The problems are increasingly international, and require international solutions. Transborder data flows run afoul of differing national laws. Cryptography presents its own problems worldwide. Access is now possible economically from anywhere in the world, which is both a wonderful opportunity and a serious risk – because of the much greater need for system security to prevent misuse.

Bob Morris, former Chief Scientist of the National Computer Security Center and NSA employee, addressed the Computer Science and Technology Board of the National Research Council on Sept 19, 1988, relating to computer security risks. He observed that

To a first approximation, every computer in the world is connected with every other computer.

This is even truer now than it was then, because of the recent surge of Internet activity, with browsers over the worldwide web. The vulnerabilities and risks of our technocratic era are ubiquitous.

FURTHER OBSERVATIONS ON SYSTEM DEVELOPMENT

Although there has been significant progress in recent years, there are still some major problems and major risks relating to the development of large and complex systems – and particularly so in accommodating critical security requirements.

The U.S. Government (and almost everyone else) has experienced repeated difficulties in developing large systems, which are increasingly dominated by software. Significant problems have arisen in air-traffic control systems, law-enforcement systems, the IRS Tax Systems Modernization effort (see Reference 10), and procurements for military and commercial aviation and defense systems. We desperately need the ability to develop complex systems – within budget, on schedule, and with high assurance compliant with their stated requirements. The shuttle is one successful example of a large and very complex system development in which software goals were met adequately, although the costs of that effort were not insignificant and the risks understood somewhat better than in other systems.

The U.S. Government is increasingly dependent on commercial systems. Except for a few special cases, it is no longer feasible to develop custom-designed systems – the costs are prohibitive, the time schedules are awful, and the risks of system failures are considerable. As a consequence, we must encourage system developers to produce systems that are at the same time truly useful for Government needs and for commercial markets as well – and especially when it comes to attaining adequate security. If we ignore security, it seems that the technology has advanced to the point where the required functionality can be configured out of off-the-shelf products. However, when we insist on meaningfully secure systems that are resistant to all sorts of attacks and insider misuse, we discover that it is still very difficult to configure such systems from off-the-shelf products.

The serious difficulties experienced in the past in attempting to develop large systems are amplified when those systems have critical security requirements. Being able to configure secure system

environments readily from commercially available components is one of our biggest challenges.

Here are a few of the many factors that have slowed progress in the security of commercially available high-security products – above and beyond the many reasons why complex systems are inherently difficult to develop and operate in the first place.

- The vulnerabilities in the existing infrastructure are poorly understood. The risks that can
 result from those vulnerabilities tend to be seriously underestimated. This lack of awareness
 pervades Government, developers, vendors, users, and even bystanders who would like to
 believe that their lives are independent of the technology.
- 2. Another factor that has slowed progress in security is that, despite the very considerable vulnerabilities and risks in today's telecommunications infrastructures, digital commerce, and national security systems, serious disasters have not yet struck critical systems. Major security-related events have not yet occurred that in their effects on public awareness might be considered to correspond in scope to a Chernobyl, Bhopal, or Exxon Valdez. The security-related cases that have occurred have generally not caused massive damage or affected many people adversely. The 1988 Internet Worm, the Citibank penetrations, and a few other similar cases are more like the tip of an iceberg. Fortunately, may serious security flaws have been detected by friendly people who have reported them before those flaws could be exploited.

People tend not to worry until they have been seriously affected (either individually or as part of a nationwide or worldwide effect), and by then it may be too late. It is generally unwise to wait until after the disaster to plan on what to do. The situation is perhaps akin to earthquake preparedness – you know it is going to happen eventually. In this case, the cost of preparedness should be chosen commensurate with the consequences of the risks that could be avoided.

3. A third factor has been a generally dampening effect on U.S. commercial development. This effect has resulted in part from the U.S. export control laws relating to cryptographic products. That is a very complex subject, and I refer you to the National Research Council report on U.S. crypto policy (Reference 6).

The situation is in some ways improving, and in some ways worsening. Infrastructural components that can improve security are emerging, such as firewalls and cryptographically based authentication. At the same time, the would-be attackers are getting smarter and more sophisticated, many fundamental flaws remain even with firewalls and better authentication, and the advent of new systems continually create new flaws that introduce new risks or new manifestations of old risks.

CONCLUSIONS

In these few pages, I have merely surveyed some of the important issues. Here is a brief summary.

Security is very difficult to attain with any certainty. Computer systems, networks, and human beings are all generally imperfect. As a consequence, today's infrastructure is seriously flawed and seriously at risk. The infrastructure may be good enough for low-risk applications, but it is not good enough for high-risk applications such as protection of sensitive corporate and national data, preservation of privacy, large-scale financial transactions over the Internet, and life-critical systems.

360

In the long run, better computer-communication security is absolutely fundamental to the preservation of a well-ordered society, and for national security and economic competitiveness reasons as well. Digital commerce could be very dangerous unless the infrastructure is greatly improved, with huge potential financial losses possible. Good cryptography that is properly embedded within the infrastructure is absolutely essential.

Privacy is also very difficult to attain. Undesired database access is often surprisingly easy to attain, in Government, corporate, commercial, and private databases. Detailed life profiles of arbitrary individuals can be obtained by aggregating information from different databases, with serious risks of impersonation, fraud, and harassment – which are becoming increasing prevalent. (See Reference 3 and 4 for examples, including misuses of Social Security Numbers.) Privacy is often considered to be a less important aspect of security, but it is something on which our lives all rest. It must be respected and cherished.

Research and prototype development are fundamental. The availability of adequately secure systems and networking cannot occur without appropriate high-quality research and prototype development, particularly that related to the configuration of trustworthy systems with both trustworthy and untrustworthy components. Above all, the necessary progress in computercommunication security requires that the U.S. Government must play a truly enlightened role in encouraging relevant research and prototype development in the public sector. Much greater effort must be devoted to having the system development community produce products that are so badly needed, such as better secure operating systems, secure networking, secure wireless communications, and well-constructed applications of cryptography. Beyond that, development of life-critical systems and Government systems with extreme requirements for dependable behavior demands extraordinary efforts.

Much greater awareness is essential – of security flaws and risks in the use of computercommunication systems, on the part of governments, businesses, and private citizens. (This seems to be a rather simple statement, but it is not easy to attain.) As systems become more complex, the more difficulties seem to arise, particularly relating to security.

Education is absolutely essential. Computer literacy is increasingly necessary, even to deal with daily life. Attempts to make computer systems "user-friendly" typically ignore the problems that arise when something goes wrong or assume that there are enough competent people around to keep the infrastructure sound.

The U.S. Government is vitally dependent on commercial technological developments for its computer-communication systems. Custom developments have often been counterproductive in the past. The Government must encourage developers to provide better security as a part of their normal product line. The Government must also encourage greater interconnectivity between government systems and the private sector – albeit with adequate protections for security and privacy.

We have been fortunate thus far, in that attacks on computer security have been relatively limited in their effects. However, the potential for enormous damage is present. We must not be complacent. Proactive prevention of serious consequences requires foresight and a commitment to the challenge ahead. The technology is ready for much better security than we have at present, although there will always be some risks. The Government has a strong role to play in ensuring that the information infrastructure is ready for prime time.

Perhaps the most fundamental question today is this: How much security is enough? The answer in any particular application must rely on a realistic consideration of all of the significant risks. For

simple home-grown computing that has only local sensitivity, some security is needed merely to prevent the system from being trashed by intruders. For situations with very high risks, significantly greater computer-communication security is prudent. There are many stages in between those two cases, and no easy answers. There is also a serious risk of ignoring risks that are difficult to deal with – unknown, unanticipated, or seemingly unlikely but with very serious consequences.

As noted in Reference 4, there are three fundamental gaps – all of which must be narrowed if we are trying to significantly improve the security of the infrastructure: (1) a technological gap between what computer systems and networks are actually *capable* of enforcing and what they are *expected* to enforce; (2) a sociotechnical gap between the expected computer system policies and the *social policies* such as laws and codes of ethical practice; and (3) a social gap between the social policies and actual human behavior. Closing all three of these gaps must be an ongoing challenge in our emerging infrastructure.

REFERENCES

 Susan Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P.G. Neumann and D. Sobel, Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy, ACM, June 1994.

2. Teresa Lunt, Securing the Information Infrastructure (Inside Risks, monthly column, edited by Peter Neumann), Communications of the ACM, vol 39, no 6, June 1996.

3. Peter G. Neumann, Illustrative Risks to the Public in the Use of Computer Systems and Related Technology. [Attached]

4. Peter G. Neumann, Computer-Related Risks, Addison-Wesley, 1995.

5. Computers at Risk: Safe Computing in the Information Age, National Academy Press, 5 December 1990. [Final report of the National Research Council System Security Study Committee.]

6. Cryptography's Role In Securing the Information Society, National Academy Press, prepublication copy, 30 May 1996; bound version in early August 1996. (The executive summary is on the world-wide web at http://www2.nas.edu/cstbweb) [Final report of the National Research Council System Cryptographic Policy Committee.]

7. The Unpredictable Uncertainty: Information Infrastructure Through 2000, National Academy Press, 1969. [Final report of the NII 2000 Steering Committee.]

8. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, U.S. General Accounting Office, May 1996, GAO/AIMD-96-84. [Briefed to this Subcommittee on 22 May 1996.]

9. "National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information," statement of Laurie E. Ekstrand, U.S. General Accounting Office, as testimony before the U.S. House of Representatives Subcommittee on Information, Justice, Agriculture, and Transportation, of the Committee on Government Operations, and the Subcommittee on Civil and Constitutional Rights, of the Committee on the Judiciary, 28 July 1993. The appendix to that testimony documents 62 cases of misuses of law-enforcement computer data.

10. For example, see the collection of IRS-related GAO reports, including Status of Tax Systems Modernization, ..., GAO/T-GGD/AIMD-96-88, 14 March 1996; Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome to Achieve Success, GAO/T-AIMD-96-75, 26 March 1996; Progress in Achieving IRS' Business Vision, GAO/T-GGD-96-123, 9 May 1996.

11. The New Encryption Universe, The New York Times, editorial, 10 June 1996.

Security Risks in the Infrastructure

Personal Background

By way of introduction, I note that I have been involved with the U.S. Government in different technological contexts for many years, including (for example) national security, law enforcement, air-traffic control, and NASA (for example, in the early stages of fly-by-wire research and space-station planning). My first computer-related job was for the Navy in the summer of 1953, 43 years ago.

I have long been concerned with security, reliability, human safety, system survivability, and privacy in computer-communication systems and networks, and with how to develop systems that can dependably do what is expected of them. For example, I have been involved in designing operating systems and networks, secure database-management systems, and monitoring systems that seek to identify abnormal patterns of behavior. I have also been seriously involved in identifying and preventing risks. Some of this experience is distilled into my recent book, *Computer-Related Risks* (Reference 4).

Last week I completed a 2.5-year term on the Internal Revenue Service Commissioner's Advisory Group, where I addressed privacy and security issues as well as the Tax Systems Modernization effort; I also appeared with Senators John Glenn and David Pryor on an IRS training video stressing the importance of taxpayer information privacy and data integrity throughout the IRS operations. From 1987 to 1989, I served on an expert panel for the House Judiciary Committee Subcommittee on Civil and Constitutional Rights, addressing law-enforcement database systems, at the request of Congressman Don Edwards.

In other activities, I was a member of the National Research Council committee (1994-96) study of U.S. cryptographic policy, which released the prepublication version of its final report on 30 May 1996 (Reference 6). I participated in an earlier study of the same subject sponsored by the ACM U.S. Policy Committee (USACM) (Reference 1). I was a coauthor of the 1988-90 National Research Council study report, *Computers at Risk* (Reference 5) that many of you saw when it came out in 1990. I am chairman of the Association for Computing (ACM) (committee on Computers and Public Policy, and Moderator of its widely read Internet Risks Forum (comp.risks).

I am a Fellow of the American Association for the Advancement of Science, the Institute for Electrical and Electronics Engineers, and the Association for Computing (ACM). My present title is Principal Scientist in the Computer Science Laboratory at SRI International (not-for-profit, formerly Stanford Research Institute), where I have been since 1971 – after ten years at Bell Telephone Laboratories in Murray Hill, New Jersey. I have doctorates from Harvard and the Technische Hochschule, Darmstadt, Germany (the latter obtained while I was on a Fulbright from 1958 to 1960).

VERBAL TESTIMONY

Risks to the U.S. Infrastructure from Cyberspace

Presented by ROBERT H. ANDERSON Head, Information Sciences Group RAND Corporation

June 25, 1996

before the Permanent Subcommittee on Investigations Senator Bill Roth, Chairman Government Affairs Committee, U.S. Senate

BACKGROUND AND QUALIFICATIONS¹

My name is Robert H. Anderson. I have been associated with The RAND Corporation in Santa Monica, California, for most of the past 28 years, serving as head of its Information Sciences Department, director of its Information Processing research program, and presently as a Senior Information Scientist and head of its Information Sciences Group.

My statement today is based primarily on work I have performed with my colleague, Richard O. Hundley, over the past five years, with support from the Defense Advanced Research Projects Agency, the Information Warfare office of the Assistant Secretary of Defense for C3I, the U.S. Air Force, and portions of the U.S. intelligence community. This statement is, however, my own and does not reflect the opinions or policies of The RAND Corporation or any of its research sponsors.

In our investigations, Dr. Hundley and/or I have talked with computer security researchers, computer emergency response teams, law enforcement professionals, legal professionals, the national security and intelligence communities, and providers and users of information systems. Our discussions have ranged across many countries in Europe, Australia and Asia.

I have provided to members of the subcommittee a recent article by Dr. Hundley and myself on cyberspace security and safety,² published in the Winter 1995/1996

¹ Headings are used as guides within this printed version of the testimony; neither they nor the footnotes are part of the verbal statement made to the subcommittee.

² Richard O. Hundley and Robert H. Anderson. "Emerging Challenge: Security and Safety in Cyberspace." IEEE Technology and Society Magazine, Winter 1995/1996, Vol. 14 No. 4.

issue of the *IEEE Technology and Society* magazine, containing a more thorough discussion of our perceptions and findings on this topic than can be presented in this forum.

- 2 -

TERMINOLOGY

The risks to the U.S. infrastructure from actions or events related to "cyberspace" is a confusing topic. By cyberspace, I refer to the global collection of internetted computers and communication systems. The term originated, I believe, in the novel *Neuromancer*, by William Gibson, in 1984. The public telephone network and the Internet provide the main backbone for cyberspace, but cyberspace also includes the computers that run many other control, communication, and information systems. The key word in the definition is "internetted," the characteristic that makes it possible to access some systems from others perhaps half a world away.

TWO MAIN POINTS REGARDING RISKS IN CYBERSPACE

I am familiar with the documents introduced in the first two of these hearings-particularly the recent GAO report on information security³ and the staff statement presented on June 5⁴. I concur with the findings and recommendations in these reports. Given this background, I believe two additional points need emphasis and attention regarding challenges in providing security in cyberspace:

1. The Information Revolution is Continuing, Bringing New Security Risks

The first point is that the U.S. cannot just solve today's cyberspace security problems. As the information revolution continues, we need structures and forums within which new problems can be addressed as they arrive. As the accompanying chart [Fig. 1] shows, during the last 15 years we have experienced at least three major information revolutions—each introducing unique security problems—with additional revolutions expected into the indefinite future.

The personal computer revolution begat viruses passed by floppy disk, or downloaded from bulletin boards. The widespread explosive growth of the Internet brought greatly increased hacking, and its related "packet sniffers" and "packet spoofers," that easily crossed international (and organizational) boundaries. The World Wide Web phenomenon with its browsers and the Java

³ Government Accounting Office (GAO), Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, GAO/AIMD-96-84, May 1996.

⁴ Ú.S. Senate Permanent Subcommittee on Investigations (Minority Staff), Staff Statement: Hearings on Security in Cyberspace, June 5, 1996.

language and "applets"⁵ is promoting the use of downloadable executable code from strangers, while bypassing normal firewall protections—a combination that is ripe for exploitation by malefactors.

A Continuing Series of Information Revolutions

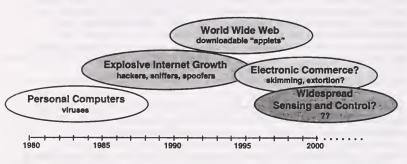


Figure 1

By their nature, the progress of future revolutions cannot be predicted. However, a good candidate for the next revolution--which builds on the previous ones--is widespread electronic commerce. It is quite possible that billions of dollars a year of commerce will be conducted by citizens and corporations on-line within the coming decade, including millions of "micro-payments" of pennies or hundredths of a cent for various forms of information access. The opportunities of abuse within such a system are manifold, and some are very likely unforeseen today.

A further, or co-incident, revolution might involve widespread dependence on electronic monitoring and control systems. U.S. residents' automobiles will soon be in automatic communication with toll booths, "smart roads," and even gas stations. Meters within their houses will increasingly be read remotely and automatically, and "smart houses" with many more control and feedback systems are in our future.

⁵ "Applets" are small application programs that can be downloaded to a personal computer, and executed in that user's own computing environment.

- 4 -

2. A Continuing Partnership Between Government and Industry is Needed

My second point is this: Since there will not be a "plateau" of information system developments during which existing security problems can be "solved," I believe the only viable solution is the development of a framework for a continuing partnership between government and industry within which new vulnerabilities and risks can be addressed as they are encountered. The government can't ignore market forces, and it can't ignore the private sector. There are, however, examples in which government and industry have worked--and are now working--together effectively, such as in improving the safety of automobiles and of the commercial airline industry. Such continuing cooperation, focused on safety and security, is needed today across all aspects of our national information infrastructure, including energy distribution, transportation control systems, financial networks, as well as the traditional telecommunications and internetworking sectors.

THREE ISSUES FOR CONSIDERATION

In RAND's studies on these topics to date, three issues are repeatedly raised, which should form a portion of a national dialog on cyberspace security. These issues are good candidates for the continuing structured dialog between government and industry that I recommended earlier.

First, there has been considerable discussion of the advisability and feasibility of creating a <u>Minimum Essential Information Infrastructure</u> (MEII). If all of our systems cannot be adequately protected to enable deployment of military forces, or to permit key transportation links to operate, or to allow other key societal activities to continue, is there some fallback level of system that will allow essential services? If there is, a number of questions, to which the United States does not yet have answers, must be addressed. These include:

• What are the essential services, and what are the minimum levels of these services, that our society requires?

• What types of communication and computation systems are required to support these essential services?

• How would an MEII be formed from the existing infrastructure? By "hardening" certain parts of it? By creating sufficient redundancy and resiliency that a minimum portion would always survive an attack?

• What would the costs of an MEII be, and how do these compare with the expected benefits?

Second, we should consider simple ways to increase the robustness of the U.S. infrastructure systems. For example, it may be possible, through incentives or regulations, to increase the "biodiversity" of the software and hardware of our systems, especially the public telephone system. Today, those systems are too dependent on a few suppliers; a flaw or bug, once uncovered, could be exploited within literally thousands of switches.

Third, I reiterate a point introduced in earlier hearings, because of its importance. <u>Roles and missions</u> among organizations having necessary roles to play <u>need</u> <u>clarification</u>. Although responsibility must be distributed, within the United States someone must coordinate the activities of:

- the national security and domestic agencies of government
- the U.S. public and private sectors and
- the national and international communities.

This would imply explicit coordination at the highest levels of the Executive branch, within the Executive Office of the President.

Let me close by saying that your hardest task will be putting the insecurity of our infrastructure into perspective. Is it more dangerous to our society than the threat of biological or chemical weapons, or nuclear proliferation? I don't believe anyone has clear answers to this question yet. At present, I don't believe that a standalone information warfare attack upon the U.S. civil sector would produce "significant and enduring consequences".⁶ However, in time of war or troop deployments, a coordinated cyberspace attack could have adverse military consequences, and it could be used by foreign elements to affect U.S. public opinion regarding an intervention or operation.

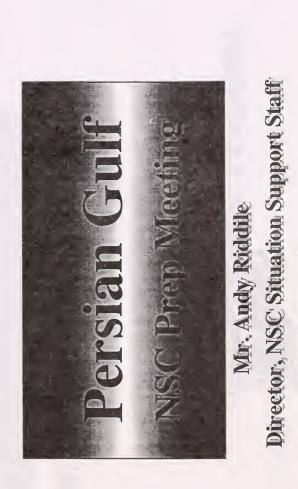
Of course, there are positive forces at work too. In particular, on-line commerce is creating a market for better on-line security, to everyone's benefit. In general, our country's infrastructure is very resilient, as various natural disasters and various incidents to date have shown.

There is much more to be said on all these topics, and I trust that further detail on many of these issues will be forthcoming in future hearings of this subcommittee. Thank you for your attention.

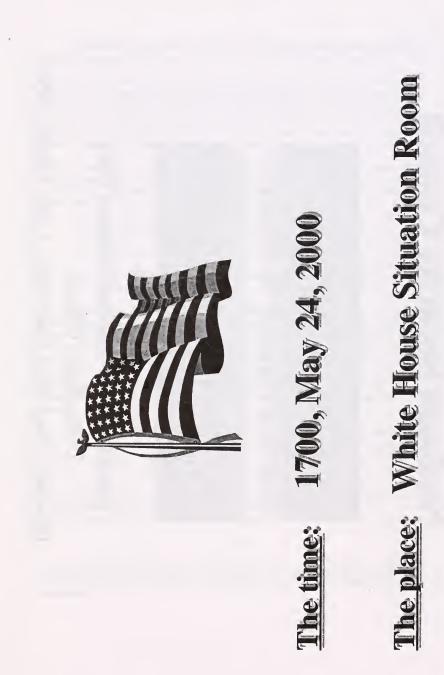
[end]

⁶ This phraseology is from Bell-Ringers or Duck-Bytes? A Workshop on Information Warfare Vulnerabilities in the Civil Sector, by Carl H. Builder, September 1995 (unpublished RAND project memorandum).





Director, Near East and South Asian Affairs, NSC Mr. Peter Wilson





National Sceneity Council -- May 24, 2000

Situation Update

- Meeting Objectives
- Memo to the President

O	
1	
evolu	
1	
e	
ion	
and the second s	
80	
00	
-	
2	
8	

National Security Council -- May 24, 20

- · Electronic commerce
- Cellular revolution
- National Info Infrastructure (NII)
- Global Info Infrastructure (GII)

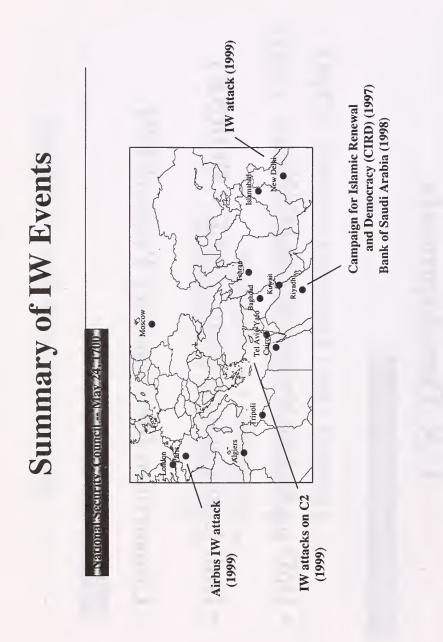
U.S. Developments

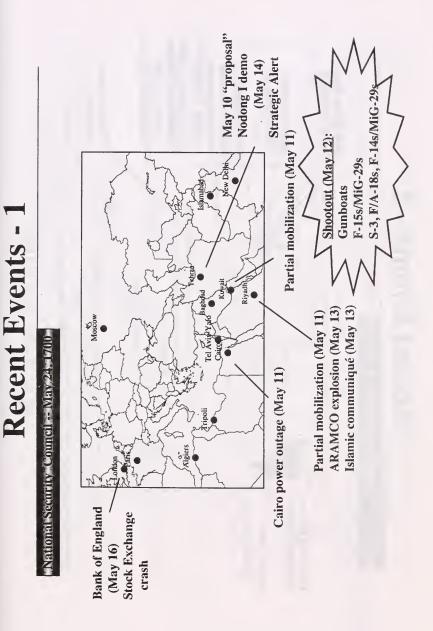
National Security Council -- May 24, 2000

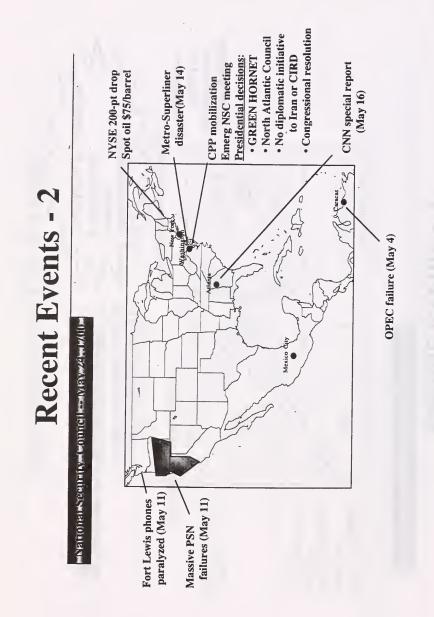
DoD on Public Switched Net (PSN)

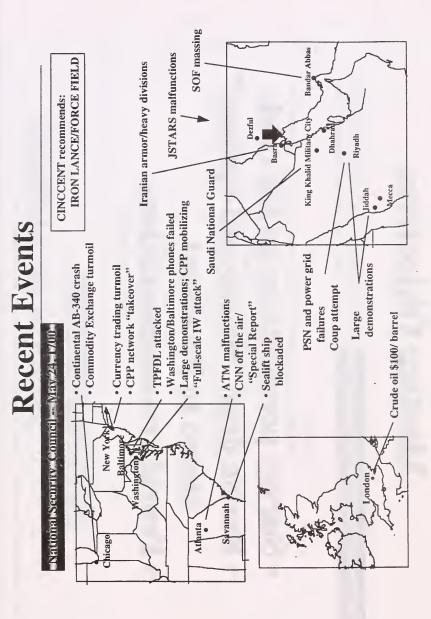
Gulf Contingency Plan: GREEN HORNET

• Consortium for Planetary Peace (CPP)

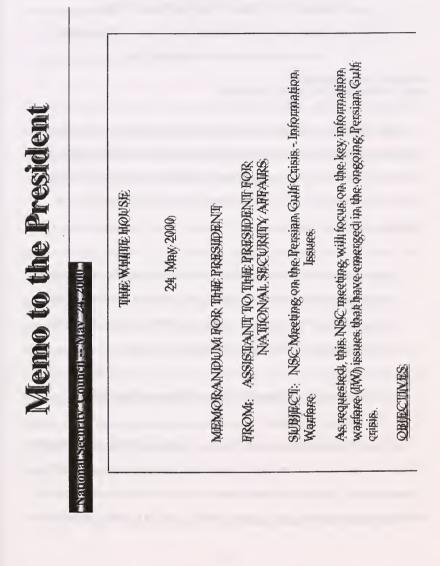








 Revise draft "issues-and-options" Survey perspectives on the crisis Meeting Objectives Provide recommendations memo to President itonal Security Council --- May 24, 2000



PREPARED STATEMENT OF SENATOR JON KYL

BEFORE THE SENATE GOVERNMENTAL AFFAIRS PERMANENT

SUBCOMMITTEE ON INVESTIGATIONS

TUESDAY, JULY 16, 9:30 A.M. SENATE DIRKSEN BUILDING -- ROOM 342

Mr. Chairman, I appreciate the opportunity to appear before the committee, and I thank you and Senator Nunn for your leadership in addressing this problem. Some time ago, Senators Bingaman, Robb, and I successfully offered an amendment to the Defense Authorization Act of 1996 (now public law) which required the President to give to Congress:

1) the outline of a plan to establish procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions regarding strategic attacks by foreign nations, groups, or individuals, or any other entity which invades the national information infrastructure; and

2) an assessment of the future of the National Communications System.

I offered this amendment because there is, at present, no defense against invasions of the nerve centers of our society (which include our defense, telephone, public utility, and banking systems). My fear is the military has little ability to protect our country from strategic assaults on the NII, and no legal or political authority to protect our information

systems against another country's offensive. Current CIA Director John Deutch said, at his Senate confirmation hearing, that "[t]his is a very important subject . . . which we really don't have a crisp answer to."

The threat is very real. According to the NSA, over 100 countries are working on information warfare techniques. The President must develop a comprehensive national policy that coordinates national security defense for both United States government and private sector users of our national information infrastructure.

Several things have changed in the last 10 years that demand the modernization of our current national security communications and emergency preparedness posture. The increased pace of technological innovation appears to have rendered previous legislation and administration action in this area inadequate. Moreover, standing programs for emergency preparedness have withered and the Cold War's end has encouraged a false perception that these things no longer matter. Today, we do not have answers to even the simplest of questions. How vulnerable to attack is the national information infrastructure? Who, what, and where are the threats? What is the specific technical nature of the threats? Could we, for example, detect an adversary's intelligence preparation of a simulated "information infrastructure battlefield"? How can government best engage various private sector elements on national security grounds?

Currently, no department, agency, or individual of the U.S. government has

responsibility for the mission ahead. During the Cold War, the intelligence community, with the help of the Department of Defense, had the indications, warning, and attack assessment responsibilities. The Cold War concept of indications and warning/ attack assessment focused exclusively on physical foreign attack, by aircraft or missiles. But a strategic attack on the NII is radically different from an ICBM attack, making the old practices virtually obsolete. It is one thing to have procedures in place to determine if an enemy is stockpiling Plutonium. It is very difficult to determine if someone is planning a strategic attack against the NII.

Interference with the U.S. information infrastructure increasingly means an attack on privately-owned, commercial networks, systems, and facilities (our banking, our utilities, and our transportation systems). It is important to note that such an attack might first be visible to the privately owned or controlled entities in the private sector -- not to the government.

Until now, concerns about the possibilities of a strategic assault on the NII have gone unaddressed. For example, the President's own National Security Telecommunications Advisory Council (NSTAC) recently wrote to the President with concerns on this subject. The President's response was lukewarm at best. My amendment, which required the President to report to Congress by June 10, has gone unanswered. On May 8, I wrote the President asking for a status of the report as well as offering assistance. His reply, which came from National Security Advisor Tony Lake, was,

frankly, inadequate.

I am aware that our report requirement is a tremendous task. Information assurance is too complicated, and in many ways, too revolutionary a concept to be addressed completely and with great precision right now. But there is no excuse for not starting. The amendment was not intended to be congressional harassment. Instead, I believe this report could help frame the country's public policy on dealing with strategic attacks against the NII. Once the report is finally delivered to Congress, I ask that the Senate Armed Services Committee and the Senate Intelligence Committee work diligently with the President to enact the appropriate changes in public policy.

The work performed by this committee and others has obviously sparked some action. I understand that the administration will respond to congressional inquiries like my amendment by establishing a commission that would investigate the threat of such attacks on the NII and formulate a policy that answers the questions in the amendment. I am aware that Attorney General Reno and Deputy Attorney General Jamie Gorelick have been active in trying to enhance the FBI's capability to handle a terrorist threat against the NII. Additionally, the intelligence community plans to create an information warfare technology center located at the NSA.

While the DOJ should be commended for its work, there must be leadership at the highest level -- the President. And the threat should be seen as a strategic one. The threat

4

is not just that of a domestic terrorist. Rogue countries might attack a system, either directly or by using terrorists. As I mentioned, there are reports that over 100 countries are working on developing weapons and techniques to conduct information attacks. DOJ, CIA, and DOD are important contributors to a national defense against attacks on our information systems, but the policy must come from the President.

My amendment was intended to spark planning led at the President's level. The President's lack of seriousness in responding to what is now law is terribly disappointing, and contributes to our lack of preparedness to deal with potentially serious disruptions in vital infrastructure systems. I believe that if a catastrophe of this kind were to occur, it is clear who is culpable – the President. Congress has done everything it can to spark leadership at the highest level. The President must comply with the law. It is not a suggestion; it is the law, it is important.

Now is the time for the President to be active. This is an important issue that must be addressed <u>before</u> our country's communications system is attacked. Congress has elevated its efforts to protect the national security interest of this country, now is the time for the President to reciprocate. I thank you again, Mr. Chairman, for the opportunity to address the committee.

U.S. SENATOR PATRICK LEAHY

VERMONT

STATEMENT OF SENATOR LEAHY AT HEARING ON SECURITY IN CYBERSPACE Permanent Subcommittee on Investigations Senate Committee on Governmental Affairs

July 16, 1996

I appreciate the opportunity to participate in this important series of hearings on how we can safeguard the security of our critical national computer networks and the information stored in, and carried on, those networks.

Our dependency on computers and the growth of the Internet are both integrally linked to people's confidence in the privacy, security and reliability of computer networks. That is why I have been working over the past decade to make sure the laws we have in place foster both privacy and security.

As this Subcommittee has heard over the course of these hearings, however, our computer networks remain vulnerable to the threat of attack by hackers, high-tech criminals, and spies. That is why, last summer, I introduced with Senators Kyl and Grassley, legislation to increase protection for computers, both government and private, and the information on those computers, from the growing threat of computer crime. I am pleased to report that this legislation, the "National Infrastructure Protection Act," was reported favorably by the Judiciary Committee last month, and we hope it will be considered by the Senate as early as this week.

We need to protect both government and private computers, and the information on those computers, from the very real and growing threat of computer crime. The facts speak for themselves -- computer crime is on the rise. You have already heard from the Computer Emergency and Response Team (CERT) at Carnegie-Mellon University. According to their most recent report, over 12,000 Internet computers were attacked in 2,412 incidents in 1995 alone.

You also heard the results of a survey conducted jointly by the Computer Security Institute and the FBI showing that 42 percent of the respondents have sustained an unauthorized use or intrusion into their computer systems in the past twelve months.

This is not just a law enforcement issue, but an economic one. Breaches of computer security are resulting in direct financial losses to American companies from the theft of trade secret and proprietary information. This hurts our economy. A December 1995 report by the Computer Systems Policy Project, which is comprised of the CEOs from thirteen major computer companies, estimates that financial losses in 1995 from breaches of computer security systems ranged from \$2 billion to \$4 billion. The report predicts that these numbers could rise in the year 2000 to \$40 to \$80 billion worldwide. The estimated amount of these losses is staggering.

This report quotes one unidentified U.S. based manufacturer, who said:

"We just lost a major...procurement in [a Middle-Eastern country] by a very small margin to [a state subsidized European competitor]. We were clearly breached; our unique approach and financial structure appeared verbatim in their competitor's proposal. This was a \$350 million contract worth over 3,000 jobs."

Yet another U.S. based manufacturer is quoted in the report, saying:

"We had a multi-year, multi-billion dollar contract stolen off our P.C. (while bidding in a foreign country). Had it been encrypted, [the foreign competitor] could not have used it in the bidding time frame."

Armed with a modem and a computer, a criminal can wreak havoc on computers located here in the United States from virtually anywhere in the world. This is a significant challenge in fighting cybercrime: there are no borders or passport checkpoints in cyberspace. Communications flow seamlessly through cyberspace across datelines and the reach of local law enforcement.

We have seen a number of examples of computer crimes directed from abroad. For example, the 1994 intrusion into the Rome Laboratory at Grifess Air Force Base in New York, was perpetrated by a 16-year old hacker in the United Kingdom. More recently, in March of this year, the Justice Department tracked down a young Argentinean man who had broken into Harvard University's computers from Buenos Aires and used those computers as a staging ground to hack into many other computer sites, including at the Defense Department and at NASA.

Every technological advance provides new opportunities for legitimate uses and the potential for criminal exploitation. Existing criminal statutes provide a good framework for prosecuting most types of computer-related criminal conduct. But as technology changes and high-tech criminals devise new ways to use technology to commit offenses we have yet to anticipate, we must be ready to readjust and update our criminal code.

Let me give you some examples of gaps in our current

computer crime laws that our legislation would address.

First, there is a new and emerging problem of computer-age blackmail. This is a high-tech variation on old-fashioned extortion. In a North Carolina case, a person threatened to crash a computer system unless he was given free access to the system and an account. One can imagine situations in which hackers could penetrate a system, encrypt a database and then demand money for the decoding key. The bill adds a new provision to the law that would ensure law enforcement's ability to prosecute modern day blackmailers, who threaten to harm or shut down computer networks unless their extortionate demands are met.

Second, current law gives special protection to information on the computer systems of financial institutions and consumer reporting agencies, because of their significance to the economy of our Nation and the privacy of our citizens. Yet, increasingly computer systems provide the vital backbone to many other industries, and carries private medical records and other private or proprietary information. This legislation would expand the protection of federal law to cover computers in interstate or foreign commerce or communications. Specifically, the legislation would penalize hackers who, without authorization, access those private computers to obtain information. In this way, we recognize the global nature of the problem of computer crime, and make clear that the United States has jurisdiction over international computer crime cases that effect U.S. computers.

Third, current law falls short of protecting our government and financial institution computer network infrastructure. Generally, hacker intrusions that inject "worms" or "viruses" into a government or financial institution computer system that is not used in interstate communications is not a Federal offense. The legislation would change that limitation and extend federal protection from intentionally damaging viruses to government and financial institution computers, even if they are not used in interstate communications.

Finally, the statutory scheme provided in this bill will provide a better understanding of the computer crime problem. By consolidating computer crimes in one section of Title 18, reliable crime statistics can be generated. This will make it easier to measure existing harms, anticipate trends, and determine the need for legislative reform. Additionally, as new computer technologies are introduced, and new computer crimes follow, reformers need only look to section 1030 to update our criminal laws, without parsing through the entire United States Code.

Addressing cybercrime with up-to-date criminal laws, and tough law enforcement, can only be part of the solution. While criminal penalties may deter some computer criminals, usually these laws come into play too late, after the crime has been committed and the injury inflicted. We should keep in mind the old adage that "The best defense is a good offense." We should encourage Americans and American firms to take preventive measures to protect their computer information and systems.

That is where encryption technology comes in. Encryption technology is one important tool in our arsenal to protect the security and confidentiality of our computer information. Encryption enables all computer users to scramble their electronic communications so that only the people they choose can read them.

Peter Neumann, who testified before you last month, commented in his written testimony that: "U.S. cryptographic policy has generally not been sufficiently oriented toward improving the infrastructure, in that it has been more concerned with limiting the use of good cryptography. U.S. crypto policy has instead acted as a deterrent to better security." Encryption cannot be the sole source of protection for our critical computer-based infrastructure, but we need to make sure the government is encouraging--and not standing in the way of--the use of strong encryption.

Our law enforcement and defense agencies cannot, and should not, carry the whole load for the security of our computer networks. Congress recognized this fact when it passed the Computer Security Act and put the responsibility for developing federal computer security standards for nonclassified information in the hands of a civilian government agency, rather than the NSA.

The federal government should play a critical role in gathering intelligence about threats to our vital computer networks, assessing vulnerabilities to these networks in light of threats, aggressively pursuing prosecutions of computer criminals, and working with industry on finding comprehensive solutions for protecting these networks.

But the government should not control or stand in the way of technical solutions. Its role should be to encourage the use of strong security.

Moreover, encryption technology is good for Americans and good business for American firms. Government export controls barring our high-tech industries from selling strong encryption overseas are hurting our economy. According to press reports, Netscape will start selling strong encryption software over the Internet today, but only to U.S. citizens and green-card holders. The company is not allowed to sell the strong encryption its foreign customers, and will have to take extra steps to verify the nationality of its customers. I am confident that Netscape's foreign customers want no less security than Americans are demanding here, but foreigners will have to look elsewhere. To maintain current controls on encryption technology is to lose control of the market.

Foreign competitors are only too willing to fill the void created by U.S. export restrictions. Foreign manufacturers are marketing hundreds of products using strong encryption that Americans can buy here, but American companies are restricted from selling overseas. Japan's Nippon Telegraph and Telephone Corporation (N.T.T.), one of the largest companies in the world, is selling "triple DES" encryption that was developed in this country but that American companies are barred from selling abroad.

Loosening export restrictions on encryption and encouraging the widespread availability of strong encryption is pro-business, pro-jobs and pro-privacy. This is an area where the government is standing in the way of better security. I look forward to working with other Members of Congress to craft a more constructive policy in this area.

STATEMENT BY

THE HONORABLE JAMIE S. GORELICK, DEPUTY ATTORNEY GENERAL OF THE UNITED STATES BEFORE THE SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

> JULY 16, 1996 9:30 A.M.

HEARINGS ON SECURITY IN CYBERSPACE

Thank you, Mr. Chairman, Senator Nunn, and other Members of the Subcommittee. I very much appreciate the opportunity to testify before you this morning on the issue of security in cyberspace. Both the Attorney General and I consider this issue to be one of the most important issues that our government, and our society as a whole, face today. I therefore welcome the chance to share my thoughts with you, and to begin what I think is a critical dialogue between the Executive and Legislative Branches on this topic. I also want to say that I believe this Subcommittee deserves to be commended for its foresight in recognizing the importance of this issue and for holding this very valuable set of hearings.

I would like to use my prepared remarks this morning to inform the Subcommittee of the important work we have been doing in the Administration to address some of the issues that this Subcommittee

has been examining over the last few months. Let me begin at the end, with the most recent action by the President, and then give you some background on what led up to that action. I would then be happy to answer any questions the Subcommittee may have.

The President yesterday signed Executive Order # 13010, on Critical Infrastructure Protection. That Order creates a Presidential Commission that will formulate policy recommendations to the President -- including any draft legislation -- on measures to protect the nation's critical infrastructures from terrorist and other forms of attack. The Order cites two sorts of potential threats to these infrastructures: bombings and other "physical" threats to tangible property; and computer-based, "cyber" attacks on the information or communications components that control the infrastructures. It is this latter set of "cyber" attacks that I will focus on today.

The infrastructures to be protected include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and continuity of government. As the Executive Order states, these infrastructures "are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."

2

Because most of the critical infrastructures are privately owned, the Executive Order emphasizes the need for close cooperation between the government and private sector. Thus, the Commission will be chaired by a presidential appointee chosen from the private sector, and will include representatives from both government agencies and the private sector infrastructures.

The Executive Order also creates an interim Infrastructure Protection Task Force at the Department of Justice to prevent, or respond to, attacks on the infrastructure that may occur while the Commission is performing its work and until the President acts on its recommendations. That Task Force will be headed by the FBI and will include representatives from other agencies, including the Department of Defense.

Now let me provide some background on the work that led to this Executive Order. Last year, in the aftermath of the Oklahoma City bombing, the President signed Presidential Decision Directive (PDD) 39, a classified document setting out the Administration's counterterrorism policy. In an unclassified portion of that PDD, the President directed the Attorney General to "chair a Cabinet Committee to review the vulnerability to terrorism of . . . critical national infrastructure[s] and make recommendations to [the President] and the appropriate Cabinet member or Agency head" on how to protect those infrastructures.

3

As a first step in carrying out this direction, the Attorney General convened a subgroup of relevant agency heads and deputies to consider the scope of the problem and determine how best to tackle it. That subgroup consisted of the Director of Central Intelligence, the Deputy Secretary of Defense, myself, the Deputy Assistant to the President for National Security Affairs, the Vice President's National Security Advisor, and the Director of the FBI.

393

The subgroup established a small interagency task force led by the Department of Justice, called the Critical Infrastructure Working Group ("CIWG"), to conduct a preliminary analysis of the problem. The CIWG set out to do the following:

 identify critical infrastructures and assess in broad terms the scope and nature of threats to those infrastructures;

ii. survey the existing mechanisms in the government for addressing those threats;

iii. propose options for a full-time group that will consider how the government should address threats to critical infrastructures over the long term; and

iv. propose options for how the government should address the threat in the interim.

Let me give you a summary of the our analysis of the problem, and then explain the proposed solutions. The first step was to identify the "critical infrastructures" that need protecting. First, the CIWG understood "infrastructures" as referring to interdependent networks and systems of industries and institutions that provide a continual flow of goods and services essential to the functioning of civil society, government, and the defense establishment. It deemed "critical" those infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on a regional or national level.

Using this definition, the CIWG settled on eight categories of critical infrastructures: Telecommunications; Electrical Power Systems; Gas and Oil; Banking and Finance; Transportation; Water Supply Systems; Emergency services (including medical, police, and fire and rescue services); and Continuity of Government and Government Operations.

The next step was to consider the nature of the threats to these infrastructures. Threats can be divided into two general categories: physical attacks and, for lack of a better term, "cyber" attacks. Physical threats consist of direct physical attacks on the "real property" component of the infrastructures. Such attacks can utilize not only conventional explosives, but also nuclear, biological, and chemical weapons. The World Trade Center bombing, conducted by international terrorists, and the bombing of

5

the Oklahoma City Federal Building last year are recent examples of physical security vulnerabilities inherent in our open society. This sort of physical attack could take on much more serious dimensions if a bomb were placed at a carefully selected critical infrastructure node, potentially debilitating a specific infrastructure on a regional or national scale, in addition to the death or destruction caused by the bomb directly.

The "cyber" threat consists of electronic, radio-frequency, or computer-based attacks on the information or communication components that control critical infrastructures. Logic bombs, viruses and other computer-based attacks may disrupt, manipulate, or destroy the information upon which our defense, security, economic, and societal fabric depends.

Such attacks can disable or disrupt the provision of services just as readily as -- if not more than -- a well-placed bomb. For example, a critical switching node in an AT&T telecommunications network could be destroyed by a truck bomb parked next to a building. Or it could be disabled by the introduction of a virus into the switch's computer operating system.

In other key infrastructures, the impact of a cyber attack is becoming increasingly apparent, as is the ripple effect disruptions in one area can have on other areas. Recent breakdowns of the air traffic control system -- although the result of aging systems

6

rather than electronic attacks -- illustrate the potential impact of a regional or system-wide collapse of such a key infrastructure.

Although we have not yet experienced a cyber attack by terrorists -- at least not that we know of -- we have seen attacks already that illustrate concretely the vulnerabilities in our information networks. The recent case involving Citibank is one example. Between June and October in 1994, approximately 40 wire transfers were attempted from Citibank's cash management system through the use of a computer and phone lines from St. Petersburg, Russia, by compromising the password and user identification code system. Citibank was successful in blocking most of the transfers or recovering the funds from recipient banks, limiting its losses. But the potential loss was enormous. Moreover, imagine what the impact might have been if the intruders' intent was not to steal funds from a few accounts, but to bring down the entire bank's accounting system; or to zero out the records of thousands of accounts; or to disrupt several major banks simultaneously.

Another example involves the telecommunications infrastructure. In 1989, a group of hackers called the "Legion of Doom" in Atlanta, Georgia, remotely accessed the administrative computers of Bell South and wiretapped calls and altered phone services. But, again, the potential harm was even greater; this group might have been able to shut down the phone network for the Southeastern United States.

Other examples involve the emergency services infrastructure. In 1992, a computer intruder was arrested for tampering with the emergency 911 systems in Virginia, Maryland, and New Jersey in order to introduce a virus and bring down the systems.

That same year, a fired employee of an emergency alert network sabotaged the firm's computer system by hacking into the company's computers, causing them to crash for about 10 hours. During that time, there was an emergency at an oil refinery. The disabled system was therefore unable to alert thousands of nearby residents to a noxious release from the refinery. Beyond that, the computer crash potentially jeopardized hundreds of thousands of people in 22 states and 6 areas of Canada where the alert network operated.

Still other examples involve an attack on critical law enforcement operations. From 1993 to 1995, a man in California gained control of the computers running local telephone switches, and discovered information concerning U.S. Government wiretaps conducted pursuant to the Foreign Intelligence Surveillance Act (FISA). He also uncovered a criminal wiretap and then disclosed the tap's existence. In another instance, this hacker's group notified a target of a Secret Service investigation that his telephone line had a dialed number recorder attached to it. Imagine the consequences for law enforcement and national security if a drug cartel or foreign intelligence service were able to use

8

such methods systematically to monitor or disrupt the most sensitive government investigations.

398

And in another case, a computer hacker penetrated the computers of, among others, the U.S. Marshals' Service, where he found the locations of individual federal prisoners, putting the security of our institutions at risk.

Finally, in 1992 a person hacked into Boeing's supercomputer center in Seattle. The hacker downloaded encrypted password files and used Boeing's computers to run hacker and cracker programs. То its credit, Boeing reported the intrusion to the FBI and partitioned its system to allow agents to trace the hackers to the source. In the course of its investigation, the FBI learned that the hacker had gained access to the computer system serving the Federal District Court in Seattle. In fact, he had obtained the passwords of both the system administrator and a Federal judge. The courthouse system was forced to close for a day to protect itself.

Having identified the types of threats to our critical infrastructures, the CIWG next considered the sources of those threats. It seems fair to say that physical threats mainly come from terrorists, both international and domestic, whose motivation is to coerce or intimidate a government or civilian population. State-sponsored acts tantamount to war and sabotage by disgruntled

insiders are also potential sources, but the main threat seems clearly to be from terrorists.

On the cyber side, however, the potential sources are more varied. An electronic intrusion could be a purely malicious hacking; the work of a negligent or disgruntled insider; part of an extortion or other criminal effort; a terrorist act; part of a clandestine espionage program; or, in a time of international crisis, part of an attack by a hostile foreign power. Any successful effort by an individual, group or country to destroy, disrupt. or deny access to the information systems of an infrastructure, or to introduce deceptive information into it or gain clandestine access to such systems for intelligence purposes, could have serious defense, national security, economic, or other societal consequences.

In light of the wide range of potential sources of attack on critical infrastructures, we reached two important conclusions. First, we determined that it did not make sense to focus only on potential terrorist attacks. Any comprehensive effort to protect our infrastructures must consider threats from all manner of individuals and groups.

Second, we concluded that the problem of cyber security could no longer be looked at solely as an issue for the defense establishment. People in the government sometimes refer to the

cyber security issue as "defensive information warfare." But this term can be misleading, because it suggests that it is purely a DoD problem, and should be addressed as part of our national defense strategy. Certainly, as Dr. White will tell you in his testimony, the military sits on a vulnerable platform consisting of different critical infrastructures. But civilian society sits on that same platform. This is therefore also an issue for the civilian world. Every person and institution that is connected to the "information superhighway" is vulnerable to attack, not just those people and institutions involved in our defense mission.

Having assessed the nature and source of threats, we turned to the difficult issue of how the government should address the problem of protecting our critical infrastructures against those threats. This is a difficult problem for several reasons. First, there are significant differences of perspective among the relevant government agencies. The Defense community naturally is focused on protecting and ensuring the viability of those elements of the infrastructures that are vital to the defense mission. Law enforcement is responsible for preventing, investigating, and prosecuting terrorist and other criminal acts against the infrastructures. The Intelligence Community also has a preventive mission, but is limited to looking at foreign-based threats. Other agencies, such as the Departments of Energy and Transportation, have concerns about the vulnerability of particular industries.

11

The problem is also difficult because ownership of critical infrastructures is largely in private hands. Absent statutory authority to regulate a particular industry, then, the government has limited ability to require private companies to take protective measures; it can merely advise industry and urge it to "do the right thing." And even if government succeeds in cajoling industry to take protective measures, much remains to be done with the private sector in the development of relevant technologies. There also is the knotty question of who will pay for such measures, or for restoration of service after an attack. Although private companies have an obvious financial incentive to take steps to reduce thefts, it is less clear that they would be willing to incur the costs necessary to protect their plants or information systems against a purely malicious or terrorist attack -- particularly in the absence of any clear indication that such an attack is likely in the near future.

Furthermore, there is less consensus in the private sector on the very need for a government role in protecting against cyber threats. While few people question government's responsibility, at some level, for protecting the physical plant of the nation's critical infrastructures against a bombing, the notion of government involvement in cyberspace typically engenders fears about infringements of privacy and free speech rights, about hampering economic competitiveness, and about stifling creativity. Yet, because the security and reliability of information and

12

communications systems are central to the continued operation of our critical infrastructures, and hence to our economic well-being and our national security, government clearly must take some responsibility for setting national policy.

To date, however, there has been no central mechanism in government responsible for protecting our critical infrastructures from attack, or for responding to an attack. Nor has there been any entity responsible for formulating policy in this area. To the contrary, there is a whole myriad of agencies, committees, commissions, task forces, working groups, and advisory councils with authority over various aspects of the issue -- but with no one to set direction or take responsibility.

This is particularly true on the cyber side of the issue. On the physical side, we have a bit more of a head start. For instance, several agencies, including the FBI and the Department of Defense, have "key asset protection programs," which consist of databases identifying key assets within each critical infrastructure and containing vulnerability information and emergency points of contact for each key asset. But even these programs are inadequate; many of the databases are out of date and insufficiently coordinated. We are currently working to rectify these problems.

13

But no such programs exist on the cyber side. We have several "centers of excellence" in the government that have expertise in dealing with cyber vulnerabilities and attacks. These include the National Security Agency (NSA), the Defense Information Systems Agency (DISA) and National Communications Systems (NCS), the FBI's Computer Analysis and Response Team and DoJ's Computer Crime Unit, and the Department of Commerce's National Institute of Standards and Technology (NIST). But none of these entities has been given responsibility, or adequate resources, to address problems encompassing the full breadth of critical infrastructures.

A similar lack of a coordination is evident in the private sector. While some individual companies have taken steps to secure their own information and communication systems from intrusion, few industries have taken an industry-wide approach to the problem. (A notable exception is the telecommunications industry, which has worked with the government through the National Security Telecommunications Advisory Committee to establish important policy guidelines for securing the telecommunications infrastructure.) And while entities such as the Computer Emergency Response Team at Carnegie-Mellon University (which receives funding from ARPA) have done an admirable job in responding to cyber attacks, too little thought has gone in to preventing attacks or restoring service on a large scale after an attack.

14

In light of the fragmentation of responsibility among government agencies, the Cabinet Committee agreed that it was vital that the government establish some mechanism to develop policy and to coordinate activities within the government and the private sector. Because there are so many agencies with equities in this issue, and because of the difficult legal questions raised, the Committee determined that further study was required of how the government should organize itself to address infrastructure assurance over the long term. This will require a combined effort by the Defense, Intelligence, and Law Enforcement Communities, combining their data and doing joint analyses. It will also require input from those agencies with jurisdiction over the critical infrastructures, such as the Departments of Energy and Transportation. And it will obviously require close consultation with Congress.

Most importantly, though, this effort will require an unprecedented amount of involvement by the private sector. There are several reasons for this. First, no analysis can be complete without information about what attacks industry has already experienced, and by whom. And only private industry knows the full story.

Second, much of the expertise on the technological aspects of the problem resides in the private sector. While the government has its own experts and resources, no one knows the ins and outs of

15

the infrastructures' computer and communications systems better than industry's own technical experts.

Finally, as I mentioned earlier, most components of the critical infrastructures are in private hands. This means that any solution will require participation by private industry. It is therefore important that industry have a say in devising that solution. And, hopefully, private sector involvement in crafting the solution will engender the trust and understanding between government and industry that will be necessary successfully to implement that solution.

What we need, then, is the equivalent of the "Manhattan Project" for infrastructure protection, a cooperative venture between the government and private sector to put our best minds together to come up with workable solutions to one of our most difficult challenges.

The Executive Order issued by the President yesterday does just that. The Commission it creates will be headed by a senior person from the private sector, who will be made a full-time government employee. Its members will include both representatives from the principal affected agencies as well as full-time representatives from the private sector (who will also become government employees for the duration of the Commission). It will also be aided by a private sector advisory committee, to allow for

even more input from segments of industry and the public at large that are not able to serve on the Commission full-time.

The assignment for the Commission is to assess more fully the scope and nature of the vulnerabilities of, and threats to, critical infrastructures; to determine what legal and policy issues are raised by efforts to protect critical infrastructures and assess how these issues should be addressed; to recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation; and to propose any statutory or regulatory changes necessary to effect its recommendations. The work of the Commission should be completed in one year.

At the same time, though, because our critical infrastructures are vulnerable to both physical and cyber attacks <u>right now</u>, some interim operational solution is necessary to help prevent, or respond to, attacks that might occur while the Commission is at work. Accordingly, on the advice of the Cabinet Committee, the Executive Order creates an interim Infrastructure Protection Task Force at the Department of Justice. This will be an interagency task force, chaired by the FBI, that will coordinate existing resources and expertise both within and outside the government, to help prevent, halt or confine an attack and to recover and restore service; to issue threat and warning notices in the event advance

406

information is obtained about a threat; to provide training and education on how to reduce vulnerabilities and respond to attacks on critical infrastructures; and to coordinate with the pertinent law enforcement authorities during or after an attack to facilitate any resulting criminal investigation. The idea is for the IPTF to operate for approximately the next 18 months, or until the Commission's work is completed and any final mechanism recommended by the Commission to deal with this problem is in place.

There are skeptics who have said that the nation will have to endure the cyber equivalent of Pearl Harbor or of the Oklahoma City bombing before the government and industry wake up to the problem of protecting our critical infrastructures from the new cyber threats. But I think the President's Executive Order, and these important hearings, disprove that pessimistic view. These events show that the President and Congress have taken important steps to prevent a problem before it occurs, and to do so in a way that ensures that all interested parties have a say in the ultimate solution.

But recognizing the problem, though important, is really the easy part. The difficult part of devising a solution remains. I look forward to working with Members of this Committee and with other Senators and Representatives in meeting that challenge.

With that I will conclude my prepared remarks and answer any questions you might have.

STATEMENT BY

THE HONORABLE JOHN P. WHITE

DEPUTY SECRETARY OF DEFENSE

BEFORE THE

SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

HEARINGS ON SECURITY IN CYBERSPACE

JULY 16, 1996

Mr. Chairman,

Thank you for the opportunity to share my views with the Subcommittee today and to represent the Department of Defense at these hearings dealing with the very timely and critical topic of security in cyberspace. Mr. Chairman, you and your colleagues on this subcommittee are to be commended for providing the increased focus and understanding of the national scope of these issues. These hearings have raised public awareness and highlighted both the current and potential threats emerging from the national and global information infrastructures on which we all are increasingly dependent.

The Department of Defense is dependent on a broad range of interconnected infrastructures, including telecommunications, electrical power

systems, gas and oil distribution, and transportation systems, among others. Reliance on this complex range of infrastructures is not unique to the DoD, but is common to all modern societies. Increasingly, these wide ranging infrastructure services are becoming interconnected and reliant on each other, driven in part by the rapid growth of telecommunications and computer technologies, but also by pressures to improve efficiency and to reduce costs. The connectivities and inter-dependencies are complex and difficult to assess and also raise a breadth of security challenges in assuring the availability of vital systems, services, and capabilities. Further, this complexity raises potential vulnerability and threat issues, where vital systems, capabilities, links and nodes could be threatened by a broad range of "cyber-intrusion" techniques as well as physical attacks on vital nodes.

409

These broad infrastructures grow increasingly more dependent on information technology, computer software and hardware systems, and networking. This introduces additional vulnerabilities. Your Subcommittee has focused on "cyber security," and I will address my remarks to DoD's concerns in this area.

I share your concerns that without adequate assurance of the security and proper operation of these infrastructures and the information systems and networks that support them, we incur significant risks. This is a topic to which I devote a significant amount of my time, for several reasons. It is an immensely important issue for the Department of Defense, and its importance will only increase due to the rapidly changing technological environment and the unprecedented pace of introduction of new information technology. Moreover, many aspects of this problem are not under our direct control. As with so much

of what the Department does, we are increasingly dependent on others, principally industry, to achieve our mission. For example, we are increasing the use of commercial services and commercial-off-the-shelf (COTS) systems within Defense to more rapidly avail ourselves of the important advancements in commercial information based technology. Finally, the Department of Defense has not yet institutionalized the culture and the basic approaches necessary to deal effectively with these challenges. These characteristics mean that this is an area that is still being shaped in the Department. Consequently, I view the issue of information security as one of my highest priorities as Deputy Secretary of Defense. Infrastructure and information systems vulnerabilities are not new problems but they will not get resolved without a long term and increased commitment by senior officials.

Before I begin to discuss the problems we face in more detail, I want to make two general observations. First, information security is not a problem we will ever "solve." We will never be able to declare victory and move on. We will make significant strides, but the penetrators will keep catching up. We have been working on this to some degree for years, and it will be a continuing process. Second, I think it is important to note that we are not alone in facing risks from information security vulnerabilities. We are certainly among the most technologically advanced societies in the world, but reliance on information technology is common throughout the world and others share our vulnerabilities.

The first and most obvious arena which we must deal with regarding the use of and vulnerabilities to information is on the military battlefield. In military operations today, battlespace and situational awareness are vital. Our

operational concepts include significant and increased information flows to and in the battlefield. Our ability to achieve this information superiority over any adversary is critical. Our quest for battlefield dominance makes us ever more dependent on highly networked information systems and communications. This is an issue that we are addressing constantly with substantial success.

The broader issue of interest to this Committee is how the Department of Defense protects its general information and information services.

Through the tremendous innovation of our microelectronics, computer, software, and communications industries, the technology and capability to access the global information infrastructure is affordable and readily available to anyone using a personal computer. On the plus side, the increased use of readily available commercial hardware and software for most organizations, including the Defense Department, has reduced system development time and costs, and operations costs, while increasing efficiency. Additionally, new "off-the-shelf" hardware and software applications permit the construction and integration of highly innovative multi-media information systems and databases. These innovations are limited only by the extent of our creativity and our ability to afford them.

This emphasis on innovation in these systems has not been matched by an equivalent emphasis on the information security aspects of this technology. The result has been some unintended consequences. Increased reliance on the information technology without a requisite amount of information assurance translates into a vulnerability, one we must systemically and systematically address. Dr. Peter G. Neumann, in his statement to this subcommittee, made a

411

very important observation concerning this reliance on commercial products when he said: "If we ignore security, it seems that the technology has advanced to the point where the required functionality can be configured out of off-theshelf products. However, when we insist on meaningfully secure systems that are resistant to all sorts of attacks and insider misuse, we discover that it is still very difficult to configure such systems from off-the shelf products."

Herein lies a dilemma for the Department, the Military Services and other organizations that require a sophisticated degree of protection for our information and information systems. This problem must be addressed. As a result, within the Department of Defense, we are employing approaches to our unclassified systems that capitalize on the security expertise and approaches we have developed and applied to our classified systems. We also need industry working in an active partnership with government to find better ways to mitigate these risks and to improve the security of commercial products. In working closely with industry, we need to agree on common concerns pertaining to infrastructure security and seek solutions that are common for government and the private sector, improving incentives where necessary to encourage industry cooperation and engagement.

As indicated by these Senate hearings, the challenge of assuring our Nation's Information Infrastructure is complex. As assessment of infrastructure vulnerabilities and threats to the infrastructure is a multi-faceted issue, so are the solutions, and we cannot fully consider the breadth and depth of those solutions until both the vulnerability and threat issues are better understood and evaluated. Awareness to both realistic vulnerabilities and the true degree of threat is an issue of primary importance throughout the department. The

412

Defense Department is pursuing a great many initiatives to improve the assurance of our information and other infrastructures. More effective use of existing security tools, such as passwords, is a necessity, especially for our networks which connect into the Public Switched Network and the Internet. Encryption of information, including unclassified and open systems, will aid in the availability, reliability, and security of that information. More effective firewalls to reduce intrusions are yet another element of the solution. The security architecture of our information networks and systems must include all of this and more. Monitoring and auditing systems are being put in place that will flag unauthorized intrusions such that security experts can respond as necessary. An improved threat assessment process with tools to provide better indications and warning for cyber threats is vital. In addition, there are legislative issues yet to be fully considered to advance aspects of our legal system into the information age, to protect the rights and privacy of our citizens while allowing rapid pursuit of cyber-terrorists and cyber-criminals.

413

We also need to recognize that the competitive market will improve security of commercial products to the extent the broader commercial market demands it. This level of security will suffice for many applications but will not be fully adequate against the most sophisticated threats. If the Nation and Defense are dependent on critical information infrastructures, but only protected by market accepted levels of security and practice -- likely inadequate -- what must government do?

We believe the recommendations contained in both your staff's and recent GAO reports appropriately emphasized the more comprehensive and integrated approach that must be employed within the Department of Defense and by others throughout the nation to achieve the levels of information

assurance required. Many of the recommendations will help address the nearterm operational issues we all face today.

414

"Hackers," and the Department's and Military Services' "Red Teams," for years have demonstrated the ease by which many of the security holes or flaws in commercial software or its implementation can be exploited. Previous hearings held by this Subcommittee have accurately characterized these problems. Our own data, developed through our assessments of the security of unclassified systems connected to the Internet, is similar to that noted in the Computer Security Institute survey data on the private sector presented at these hearings. GAO's recently completed report noted that implementation of computer security measures has not been uniform across the Department.

We agree with GAO that the implementation and practice of information system security is not uniformly and comprehensively addressed Departmentwide nor at the level adequate in all instances. We also agree that Departmentwide policies need to be strengthened as one element of a comprehensive program for improving information system security and accountability. As a long-term effort, consistent with these recommendations, DoD Directive 5200.28, "Security Requirements for Automated Information Systems" will be updated with increased attention placed on unclassified systems. In the interim, letter policies will be issued to address the near term operational improvements highlighted in the GAO report. When these information systems were not so highly networked in the Department, our policy construct provided significant latitude for the system owners to determine the level of security practice implemented. In our DoD policy and directive updates, we will assure more accountability by making specific security practices mandatory.

The Services over the past few years have focused organizational responsibility for strengthening and improving security through the establishment of the Army's Land Information Warfare Activity (LIWA), the Navy's Fleet Information Warfare Center (FIWC), and the Air Force Information Warfare Center (AFIWC). These efforts already underway will better prepare the Department to provide the assessments and capabilities also recommended by GAO.

Each of the Services has increased its training and awareness efforts. The increasing threat to our systems and the necessity that our personnel be more aware and trained to address potential threats, especially for the Internet environment, must be further strengthened. The Department will capitalize on the recently developed national level training standards produced by the National Security Telecommunications and Information Systems Security Committee (NSTISSC), chaired by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD) (C3I)). This will address the specific knowledge requirements for personnel having key responsibilities for system security.

We agree with the GAO that sufficiently trained and aware personnel are essential to a quality information systems security effort. I will direct a thorough Department-wide assessment of the adequacy of our efforts, especially in view of the increased threat and our increased dependency on automated information systems.

More broadly, these new technologies reflect major changes in the way the DoD functions. That is, we must adopt new ways of doing business. That, in turn, means changing our operating culture and "institutionalizing" these new realities. The Services are beginning to create these changes through training and reorganization. It will take time, but it is happening.

416

The Services have initiated programs to employ intrusion detection software into their systems, and the resulting data from these systems will be collected across the Department at Service and Agency levels and consolidated at DISA's Global Information Control Center. These efforts will provide an accurate assessment of the state of the Defense Information Infrastructure. This information will be fused with available intelligence information from the National Security Agency's (NSA's) National Security Operation Center to provide tactical warning and a current assessment of the state of the Defense Information Infrastructure.

Another initiative, discussed with your committee during the Director of Central Intelligence's (DCI's) testimony, is the Joint Defense and Intelligence Community Information Warfare Technical Center. This new Center which will reside at the National Security Agency, will bring together the expertise of the intelligence and military communities to define common problems and provide community specific technical solutions. This will contribute further to information and infrastructure assurance through employment of advance technology.

In addition, through the efforts of the NSA and the Defense Advanced Research and Planning Agency (DARPA), major initiatives are underway to strengthen the security of commercially available protection technology for

networks and applications to meet Department needs. A robust long-term investment effort in security technology and research is essential, if we are to achieve future security improvements beyond what the commercial marketplace can provide.

Information security policy responsibility for the OSD resides with the ASD(C3I). Under the Information Technology Reform Act of 1996, which requires departments to appoint a Corporate Information Office (CIO), the ASD(C3I) has been designated to exercise the CIO responsibilities for the Department. This will further provide clarity of responsibility and authority in assuring the security of all DOD information systems.

Many of the infrastructures Defense depends upon, such as the Public Switched Network, or the shipping and transportation systems, are owned and operated by the private sector. The vulnerability and preparedness to defend against "information warfare" attacks and disruptions are of concern, not only for private sector impact on DoD operations but for the potential for national infrastructure disruption that would affect the public's confidence in the Nation's institutions and economy. Our most recent Defense Planning Guidance (DPG), issued in April of this year, tasked Defense Department components to develop capabilities to assess and mitigate vulnerability of our information infrastructure and supporting infrastructures, such as power and transportation, to information warfare and traditional threats.

Defense has been proactive in reporting the results of its selfassessments and experiences with attempts at unauthorized intrusion. We do this to expand awareness of the problem. Most other organizations do not report or discuss the extent they experience these problems. I believe this under reporting further contributes to a continued general lack of awareness of the extent of the problems experienced, and this then translates into an insufficient effort towards addressing the issues. To implement the broader culture change required, we believe organizations that rely on information systems for the success of their mission must become more concerned with the entire spectrum of activities that provide the required level of "information assurance". This concept goes beyond what we traditionally think of as computer or information security. Information assurance is not the realm of just security specialists, it is the responsibility of all who plan operations, manage enterprises, and are responsible for the delivery of critical infrastructure services. This involves making informed risk management decisions, using the best expertise available.

418

Even if we adequately defend all of Defense's critical systems and infrastructures, the Department is still supported in its operations, whether during peacetime or conflict, by a complex, interrelated, and interdependent group of industries, institutions and organizations. This "system of systems" is composed of DoD systems, federal government systems, contractor systems and facilities, and private sector commercial entities, systems, and infrastructures. The tremendous explosion in use of communications and computer technologies has significantly increased DoD's dependence on a complex mix of sophisticated, interconnected telecommunications systems and networks, on which our "system of systems" is increasingly reliant. The assured availability of these supporting infrastructures, and of their underlying information systems, is critical to the successful accomplishment of DOD's mission. It is also clear that our national economic prosperity is similarly increasingly dependent on the same information infrastructures upon which our "system of systems" depends. One

can logically extend this understanding to the global community and our increasing dependence on a global information infrastructure.

Because of the dependence on infrastructures and technologies which are not under DoD control, we are working hard to build partnerships with stakeholders outside the national security community, both government and private. In the process, we are emphasizing incentives which might be used to encourage private sector solutions to reduce vulnerabilities. The encryption policy recently announced by the Vice President is a good example of our efforts to develop collaborative approaches among a wide range of interested parties to enhance security, and privacy, in the critical area of security in cyberspace.

The executive branch is focusing on these broader concerns through several key initiatives related to infrastructure and information assurance. An interagency Critical Infrastructure Working Group, consisting of representatives of the Departments of Defense and Justice, as well as the Intelligence Community and the White House, recently completed a preliminary assessment of infrastructure issues and their implications for national security. As a result of top level concurrence with this working group's report, an Executive Order has been signed by the President. It has two primary objectives, the first of which is the establishment of a President's Commission on Critical Infrastructure Protection. Through this full-time Commission, the federal government and the private sector will work together to develop a strategy for protecting and assuring the continued operation of critical national infrastructures. The Executive Order also establishes, as an interim measure while the President's Commission is doing its year-long work, that an Infrastructure Protection Task Force be established within the Department of Justice, to improve coordination among

government agencies in preventing and responding to infrastructure crises that would have a debilitating regional or national impact.

420

Defense will participate and share its expertise, concerns, and recommendations in these endeavors. The National Communication System (NCS) experience and model, especially the effective involvement of industry partners in the National Security Telecommunication Advisory Committee (NSTAC), provides excellent insights into how collaboration toward a common goal can be achieved through government and industry partnership. Their ongoing work in infrastructure and information assurance is directly applicable to the other infrastructure concerns we have discussed.

In addition, a current Defense Science Board (DSB) task force will provide the Department with a comprehensive assessment and recommendations for addressing information vulnerabilities.

In conclusion, although we are working hard on information assurance, cyberspace has no geographic boundaries and provides us all new problems and new challenges. It blurs the traditional concepts of sanctuary and jurisdiction. We need to assess what changes in policy, strategy, culture and incentives with industry will be necessary to deal with these new dimensions and concerns. Within the Department of Defense, there has been substantial progress in constructing the information infrastructure architecture and common operating environments for our critical command and control functions. We intend to expand these concepts and apply them to our combat support systems. We are actively working, along with many others, on the significant challenges this increased reliance on new information technology and the highly networked

information systems create. This is a long term effort-there is no going back. I am confident that with the collective collaboration and cooperation of government and industry, we will make significant progress in addressing these critical assurance issues.

Again, I compliment you and the committee for increasing the awareness and attention to this critical issue. I thank you for the opportunity to present the Department's views.

I would be pleased to take your questions.



United States General Accounting Office Report to Congressional Requesters



May 1996

INFORMATION SECURITY

Computer Attacks at Department of Defense Pose Increasing Risks





GAO/AIMD-96-84

United States General Accounting Office Washington, D.C. 20548

Accounting and Information Management Division

B-266140

÷Α(

May 22, 1996

The Honorable John Glenn Ranking Minority Member Committee on Governmental Affairs United States Senate

The Honorable Sam Nunn Ranking Minority Member Permanent Subcommittee on Investigations Committee on Governmental Affairs United States Senate

The Honorable William H. Zeliff, Jr. Chairman, Subcommittee on National Security, International Affairs and Criminal Justice Committee on Government Reform and Oversight House of Representatives

In view of the increasing threat of unauthorized intrusions into Department of Defense computer systems, you asked us to report on the extent to which Defense computer systems are being attacked, the actual and potential damage to its information and systems, and the challenges Defense is facing in securing sensitive information. This report identifies opportunities and makes recommendations to the Secretary of Defense to improve Defense's efforts to counter attacks on its computer systems.

We are sending copies of the report to the Senate Committee on Armed Services and the House Committee on National Security; the Senate Committee on Appropriations, Subcommittee on Defense, and the House Committee on Appropriations, Subcommittee on National Security; the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence; the Secretary of Defense; the secretaries of the military services; and the Director, Defense Information Systems Agency. Copies will also be made available to others upon request.

If you have any questions about this report, please call me at (202) 512-6240. Other major contributors to this report are listed in appendix I.

Jack L. Brock, Jr. Director, Defense Information and Financial Management Systems

Executive Summary

Purpose	Unknown and unauthorized individuals are increasingly attacking and gaining access to highly sensitive unclassified information on the Department of Defense's computer systems. Given the threats the attacks pose to military operations and national security, GAO was asked to report on the extent to which Defense systems are being attacked, the potential for further damage to information and systems, and the challenges Defense faces in securing sensitive information.
Results in Brief	Attacks on Defense computer systems are a serious and growing threat. The exact number of attacks cannot be readily determined because only a small portion are actually detected and reported. However, Defense Information Systems Agency (DISA) data implies that Defense may have experienced as many as 250,000 attacks last year. DISA information also shows that attacks are successful 65 percent of the time, and that the number of attacks is doubling each year, as Internet use increases along with the sophistication of "hackers" ¹ and their tools.
	At a minimum, these attacks are a multimillion dollar nuisance to Defense. At worst, they are a serious threat to national security. Attackers have seized control of entire Defense systems, many of which support critical functions, such as weapons systems research and development, logistics, and finance. Attackers have also stolen, modified, and destroyed data and software. In a well-publicized attack on Rome Laboratory, the Air Force's premier command and control research facility, two hackers took control of laboratory support systems, established links to foreign Internet sites, and stole tactical and artificial intelligence research data.
	The potential for catastrophic damage is great. Organized foreign nationals or terrorists could use "information warfare" techniques to disrupt military operations by harming command and control systems, the public switch network, and other systems or networks Defense relies on.
	Defense is taking action to address this growing problem, but faces significant challenges in controlling unauthorized access to its computer systems. Currently, Defense is attempting to react to successful attacks as it learns of them, but it has no uniform policy for assessing risks, protecting its systems, responding to incidents, or assessing damage.
	The term hackers has a relatively long history. Hackers were at one time persons who explored the inner workings of computer systems to expand their capabilities, as opposed to those who simply used computer systems. Today the term generally refers to unauthorized individuals who attempt to penetrate information systems; browse, steal, or modify data, deny access or service to others, or cause damage or harm in some other way.

GAO/AIMD-96-84 Defense Information Security

Executive Summary

	Training of users and system and network administrators is inconsistent and constrained by limited resources. Technical solutions being developed, including firewalls, ² smart cards, ³ and network monitoring systems, will improve protection of Defense information. However, the success of these measures depends on whether Defense implements them in tandem with better policy and personnel solutions.
Principal Findings	
Computer Attacks Are an Increasing Threat	In preventing computer attacks, Defense has to protect a vast and complex information infrastructure: currently, it has over 2.1 million computers, 10,000 local networks, and 100 long-distance networks. Defense also critically depends on information technology—it uses computers to help design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies. Indeed, its very warfighting capability is dependent on computer-based telecommunications networks and information systems.
	Defense's computer systems are particularly susceptible to attack through connections on the Internet, which Defense uses to enhance
	communication and information sharing. In turning to the Internet,
	Defense has increased its own exposure to attacks. More and more computer users—currently over 40 million worldwide—are connecting to the Internet. This increases the risks of unauthorized access to information and disruption of service by outsiders. Defense systems connected to outside networks contain information that, while unclassified, is nevertheless sensitive and warrants protection because of the role it plays in Defense missions.
Attacks Are Costly and Damaging	DISA estimates indicate that Defense may have been attacked as many as 250,000 times last year. However, the exact number is not known because, according to DISA, only about 1 in 150 attacks is actually detected and reported. In addition, in testing its systems, DISA attacks and successfully penetrates Defense systems 65 percent of the time. According to Defense
	² Firewalls are hardware and software components that protect one set of system resources (e.g., host systems, local area networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. See chapter 3 for a discussion of firewalls.
	³ Smart cards are access cards containing encoded information and sometimes a microprocessor and a user interface. The encoded information and/or the information generated by the processor are used to gain access to a computer system or facility.

.

Executive Summary

	officials, attackers have obtained and corrupted sensitive information—they have stolen, modified, and destroyed both data and software. They have installed unwanted files and "back doors" which circumvent normal system protection and allow attackers unauthorized access in the future. They have shut down and crashed entire systems and networks, denying service to users who depend on automated systems to help meet critical missions. Numerous Defense functions have been adversely affected, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll.
	In addition to the security breaches and service disruptions they cause, these attacks are expensive. The 1994 Rome Laboratory incident alone cost Defense over \$500,000 to assess the damage to its systems, ensure the reliability of the information in the systems, patch the vulnerabilities in its networks and systems, and attempt to identify the attackers and their locations. Although Defense has not estimated the total cost of repairing damage caused by the thousands of attacks experienced each year, it believes they are costing tens or possibly even hundreds of millions of dollars.
Potential Threat to National Security	There is mounting evidence that attacks on Defense computer systems pose a serious threat to national security. Internet connections make it possible for enemies armed with less equipment and weapons to gain a competitive edge at a small price. As a result, this will become an increasingly attractive way for terrorist or adversaries to wage attacks against Defense. For example, major disruptions to military operations and readiness could threaten national security if attackers successfully corrupted sensitive information and systems or denied service from vital communications backbones or power systems.
	The National Security Agency has acknowledged that potential adversaries are developing a body of knowledge about Defense's and other U.S. systems and about methods to attack these systems. According to Defense officials, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. In some extreme scenarios, studies show that terrorists or other adversaries could seize control of Defense information systems and seriously degrade the nation's ability to deploy

	Executive Summary
	countries already have or are developing such computer attack capabilities.
Challenges in Countering Attacks	In guarding its information, Defense faces the same risks and challenges as other government and private sector organizations that rely heavily on information technology. The task of preventing unauthorized users from compromising the confidentiality, integrity, or availability ⁴ of sensitive information, is increasingly difficult in the face of the growth in Internet use, the increasing skill levels of attackers themselves, and technological advances in their tools and methods of attack.
	Defense is taking actions to strengthen information systems security and counter computer attacks, but increased resources, and management commitment are needed. Currently, many of Defense's policies relating to computer attacks are outdated and inconsistent. They do not set standards or mandate specific actions for important security activities such as vulnerability assessments, internal reporting of attacks, correction of vulnerabilities, and damage assessments. Many of Defense's policies were developed when computers were physically and electronically isolated and do not reflect today's "networked" environment. Computer users are often unaware of system vulnerabilities and weak security practices. The majority of system and network administrators are not adequately trained in security and do not have sufficient time to perform their duties. Technical solutions to security show promise, but these alone do not ensure security. While Defense is attempting to react to attacks as it becomes aware of them, it will not be in a strong position to deter them until it develops and implements more aggressive, proactive detection and reaction programs.
Recommendations	Chapter 4 of this report contains recommendations to the Secretary of Defense for ensuring that sufficient priority, resources, and top-management attention are committed to establishing a more effective information systems security program—one that includes (1) improving security policies and procedures, (2) increasing user awareness and accountability, (3) setting minimum standards for ensuring that system and network security personnel have sufficient time and training to properly do their jobs, (4) implementing more proactive technical
	*Confidentiality refers to keeping information from being disclosed to unauthorized parties, i.e., protecting its secrecy. Integrity refers to keeping information accurate, i.e., keeping it from being modified or corrupted. Availability refers to ensuring the ability of a system to keep working efficiently and keep information accessible.

428	
	Executive Summary
	protection and monitoring systems, and (5) evaluating Defense's incident response capability. It also includes a recommendation to the Secretary for assigning clear responsibility and accountability throughout the Department for the successful implementation of the security program.
Agency Comments	GAO provided Department of Defense officials a draft of this report and discussed it with them on May 15, 1996. These officials generally agreed with the findings, conclusions, and recommendations in this report. The Department's comments and our evaluation are discussed in chapter 4 and have been incorporated where appropriate.

Contents

Executive Summary		2
Chapter 1 Introduction	Defense's Computer Environment The Internet How Computer Systems Are Attacked Objectives, Scope, and Methodology	10 10 11 12 15
Chapter 2 Computer Attacks Pose Critical Risks to Defense	Number of Attacks Is Increasing Attacks Have Caused Considerable Damage Future Attacks Could Threaten National Security	18 18 22 26
Chapter 3 Defense Faces Significant Challenges in Countering Attacks	Elements of a Good Information Systems Security Program Defense's Policies on Information Security Are Outdated and Incomplete Defense Personnel Lack Sufficient Awareness and Technical Training Technical Solutions Show Promise, but Cannot Alone Provide Adequate Protection Defense's Incident Response Capability Is Limited	29 29 32 34 36 38
Chapter 4 Conclusions, Recommendations, and Agency Comments and Our Evaluation	Conclusions Recommendations Agency Comments and Our Evaluation	40 40 40 41
Appendix	Appendix I: Major Contributors to This Report	44
Figures	Figure 1.1: The Defense Information Infrastructure Figure 1.2: Attackers Require Less Knowledge as Tool Sophistication Increases Figure 2.1: Results of DISA Vulnerability Assessments	11 15 20

Page 8

Contents

430

Figure 2.2: Number of Reported Attacks Figure 2.3: Computer Sites Attacked During Rome Laboratory Incident

Abbreviations

Page 9

GAO/AIMD-96-84 Defense Information Security

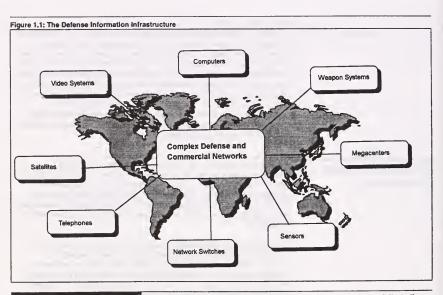
21 23

Introduction

	As a result of the rapid growth in computer technology, the Department of Defense, like the rest of government and the private sector, has become extremely dependent on automated information systems. These systems have also become increasingly interconnected worldwide to form virtual communities in cyberspace. The Department calls its portion of this global community the Defense information infrastructure. ¹ To communicate and exchange unclassified information, Defense relies extensively on a host of commercial carriers and common user networks. This network environment offers Defense tremendous opportunities for streamlining operations and improving efficiency, but also greatly increases the risks of unauthorized access to information.
Defense's Computer Environment	As depicted in figure 1.1, the Department of Defense has a vast information infrastructure of computers and networks to protect including over 2.1 million computers, 10,000 local networks, 100 long-distance networks, 200 command centers, and 16 central computer processing facilities or MegaCenters. There are over 2 million Defense computer user and an additional two million non-Defense users that do business with the Department.
	As discussed in chapter 2, Defense systems contain very valuable and sensitive information including commercial transactions, payrolls, sensitive research data, intelligence, operational plans, procurement sensitive source selection data, health records, personnel records, and weapons systems maintenance records. This unclassified but sensitive information constitutes a majority of the information on Defense computers. The systems are attractive targets for individuals and organizations seeking monetary gain, or dedicated to damaging Defense and its operations. Generally, classified information such as war planning data or top secret research is safer from attack since it is (1) protected on computers isolated from outside networks, (2) encrypted, or (3) only transmitted on dedicated, secure circuits.

The Defense information infrastructure consists of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing, storage, and communications needs of Defense users in prace and wartime.

Page 10



The Internet

The Internet is a global network interconnecting thousands of dissimilar computer networks and millions of computers worldwide. Over the past 20 years, it has evolved from its relatively obscure use by scientists and researchers to its significant role today as a popular, user-friendly, and cost-effective means of communication and information exchange. Millions of people conduct business over the Internet, and millions more use it for entertainment.

Internet use has been more than doubling annually for the last several years to an estimated 40 million users in nearly every country today. Connections are growing at an ever increasing rate; the Internet is adding a new network about every 30 minutes. Because the Internet strives to be a seamless web of networks, it is virtually impossible today to distinguish where one network ends and another begins. Local, state, and federal government networks, for example, are interconnected with commercial

Page 11

	networks, which in turn are interconnected with military networks, financial networks, networks controlling the distribution of electrical power, and so on.
	Defense itself uses the Internet to exchange electronic-mail, log on to remote computer sites worldwide, and to download and upload files from remote locations. During the conflict in the Persian Gulf, Defense used the Internet to communicate with U.S. allies and gather and disseminate intelligence and counter-intelligence information. Many Defense and information technology experts predict that Defense will increase its reliance on Internet in the future. They believe that public messages originating within regions of conflict will provide early warnings of significant developments earlier than the more traditional indications and warnings obtained through normal intelligence gathering. They also envision the Internet as a back-up communications medium if other conventional channels are disrupted during conflicts.
	Though clearly beneficial, the Internet also poses serious computer security concerns for Defense and other government and commercial organizations. Increasingly, attempted break-ins and intrusions into their systems are being detected. Federal law enforcement agencies are likewise initiating more investigations of computer systems intrusions, based on the rising level of Internet-related security breaches and crimes. Similarly, security technologies and products are being developed and used to enhance Internet security. However, as new security tools are developed, hackers quickly learn how to defeat them or exploit other vulnerabilities.
How Computer Systems Are Attacked	A variety of weaknesses can leave computer systems vulnerable to attack. For example, they are vulnerable when (1) inexperienced or untrained users accidentally violate good security practices by inadvertently publicizing their passwords, (2) weak passwords are chosen which can be easily guessed, or (3) identified security weaknesses go uncorrected. Malicious threats can be intentionally designed to unleash computer viruses ² trigger future attacks, or install software programs that compromise or damage information and systems.

 $^4\!A$ virus is a code fragment that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users.

Page 12

Attackers use a variety of methods to exploit numerous computer system vulnerabilities. According to Defense, the three primary methods described below account for most of the successful attacks.

Sendmail is a common type of electronic mail used over the Internet. An attacker can install malicious code in an electronic mail message and mail it to a networked machine. Sendmail will scan the message and look for its address, but also execute the attacker's code. Since sendmail is executing at the system's root level, it has all systems privileges and can, for example, enter a new password into the system's password file which gives the attacker total system privileges.

Password cracking and theft is a technique in which attackers try to guess or steal passwords to obtain access to computer systems. This technique has been automated by attackers; rather than attackers trying to guess legitimate users' passwords, computers can very efficiently and systematically do the guessing. For example, if the password is a dictionary word, a computer can quickly look up all possibilities to find a match. Complex passwords comprised of alphanumeric characters are more difficult to crack. However, even with complex passwords, powerful computers can use brute force to compare all possible combinations of characters until a match is found. Of course, if attackers can create their own passwords in a system, as in the sendmail example above, they do not need to guess a legitimate one.

Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use to break into systems.

Once they have gained access, attackers use the computer systems as though they were legitimate users. They steal information, both from the systems compromised as well as systems connected to them. Attackers also deny service to authorized users, often by flooding the computer system with messages or processes generated to absorb system resources, leaving little available for authorized use.

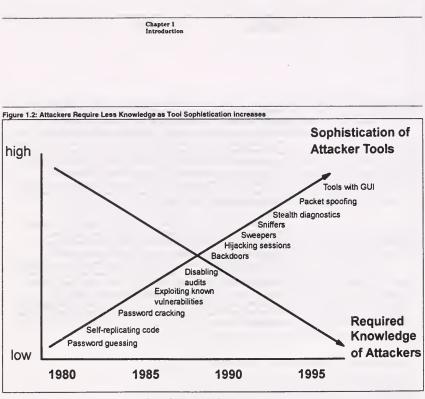
Attackers have varied motives in penetrating systems. Some are merely looking for amusement; they break in to obtain interesting data, for the challenge of using someone else's computers, or to compete with other

Page 13

attackers. They are curious, but not actively malicious, though at times they inadvertently cause damage. Others—known as computer vandals—are out to cause harm to particular organizations, and in doing so, attempt to ensure that their adversary knows about the attack. Finally, some attackers are professional thieves and spies who aim to break in, copy data, and leave without damage. Often, their attacks, because of the sophistication of the tools they use, go undetected. Defense is an especially attractive target to this type of attacker, because, for example, it develops and works with advanced research data and other information interesting to foreign adversaries or commercial competitors.

Attackers use a variety of tools and techniques to identify and exploit system vulnerabilities and to collect information passing through networks, including valid passwords and user names for both local systems as well as remote systems that local users can access. As technology has advanced over the past two decades, so have the tools and techniques of those who attempt to break into systems. Figure 1.2 shows how the technical knowledge required by an attacker decreases as the sophistication of the tools and techniques increases. Some of the computer attack tools, such as SATAN,³ are now so user-friendly that very little computer experience or knowledge is required to launch automated attacks on systems.

¹SATAN is an acronym that stands for Security Administrator Tool for Analyzing Networks. It was designed to help network administrators scan their computers for security weaknesses, but has been used effectively by hackers to break into systems.



436

Source: Department of Defense.

Also, informal hacker groups, such as the 2600 club, the Legions of Doom, and Phrackers Inc., openly share information on the Internet about how to break into computer systems. This open sharing of information combined with the availability of user-friendly and powerful attack tools makes it relatively easy for anyone to learn how to attack systems or to refine their attack techniques.

Objectives, Scope, and Methodology The Ranking Minority Member, Senate Committee on Governmental Affairs; the Ranking Minority Member, Permanent Subcommittee on

Page 15

Investigations, Senate Committee on Governmental Affairs; and the Chairman, Subcommittee on National Security, International Affairs and Criminal Justice, House Committee on Government Reform and Oversight requested information on the extent to which Defense computer systems are being attacked, the damage attackers have caused, and the potential for more damage. We were also asked to assess Defense efforts to minimize intrusions into its computer systems.

To achieve these objectives, we obtained documentation showing the number of recent attacks and results of tests conducted by Defense personnel to penetrate its own computer systems. We obtained data on actual attacks to show which systems were attacked, and how and when the attack occurred. We also obtained information available on the extent of damage caused by the attack and determined if Defense performed damage assessments. We obtained documentation that discusses the harm that outsiders have caused and can potentially cause to computer systems.

We also assessed initiatives at Defense designed to defend against computer systems attacks. We reviewed the Department's information systems security policies to evaluate their effectiveness in helping to prevent and respond to attacks. We discussed with Defense officials their efforts to provide information security awareness and training programs to Defense personnel. We obtained information on technical products and services currently available and planned to protect workstations, systems, and networks. We also obtained and evaluated information on obstacles Defense and others face in attempting to identify, apprehend, and prosecute those who attack computer systems.

We interviewed officials and obtained documentation from the

- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Washington, D.C.;
- Defense Information Systems Agency, Center for Information Systems Security, Washington, D.C.;
- Army, Navy, and Air Force Headquarters Offices, Washington, D.C.;
- National Security Agency, Ft. Meade, Maryland;
- Air Force Information Warfare Center, Kelly Air Force Base, San Antonio, Texas;
- Navy Fleet Information Warfare Center, Norfolk, Virginia;
- Air Force Office of Special Investigations, Bolling Air Force Base, Washington, D.C.;
- Naval Criminal Investigative Service, Navy Yard, Washington, D.C.;

Page 16

- · Army Criminal Investigation Command, Ft. Belvoir, Virginia;
- · Rome Laboratory, Rome, New York;
- · Naval Research Laboratory, Washington, D.C.;
- · Army Military Traffic Management Command, Falls Church, Virginia;
- · Pentagon Single Agency Manager, Washington, D.C.;
- · Wright-Patterson Air Force Base, Dayton, Ohio;
- · Army Intelligence and Security Command, Ft. Belvoir, Virginia;
- · Army 902d Military Intelligence Group, Ft. Meade, Maryland;
- · Science Applications International Corporation, McLean, Virginia; and
- Department of Justice, Washington, D.C.

We also interviewed officials and obtained data from the Computer Emergency Response Team Coordination Center, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, Pennsylvania. In response to computer security threats, Defense established the Coordination Center in 1988, to support users of the Internet. The Center works with the Internet community to detect and resolve computer security incidents and to prevent future incidents.

Our review was conducted from September 1995 to April 1996 in accordance with generally accepted government auditing standards. We provided a draft of this report to the Department of Defense for comment. On May 15, 1996, we discussed the facts, conclusions, and recommendations with cognizant Defense officials. Their comments are presented and evaluated in chapter 4 and have been incorporated where appropriate.

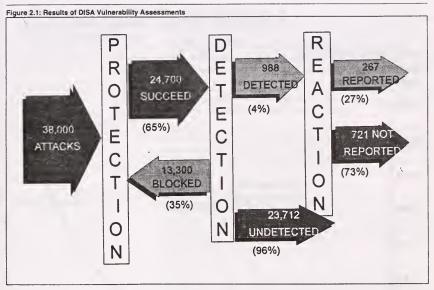
Page 17

	Defense is moving from a co information systems that per integrated information struc computers to the Internet as dependence on computer an military functions worldwide	in a technologically sophisticated world, imputing environment of stand-alone rform specific functions to a globally ture. In doing so, it has linked thousands of well as other networks and increased its id network technology to carry out important e. As a result, some operations would now be g technology failed or (2) information was imple:
	 functioning inventory and lo Defense relies heavily on co simulators that emulate corr it is impossible to pay, assig networked information syst Defense cannot control cost or release funds, or report o 	mputer technology—especially a network of uplex battle situations—to train staff; n, move, or track people without globally ems; s, pay vendors, let or track contracts, allocate n activities without automation; and ions of dollars in financial transactions for pay,
	Attackers seeking financial direct fraudulent payments, fictitious claims, direct orde entire organization's budget want to strengthen their cor contain valuable information sophisticated research and contracts and evaluation cri themselves against our milit	g targets for attackers for several reasons. gain may want to access financial systems to transfer money between accounts, submit rs for unneeded products, or wipe out an . Companies doing business with Defense may npetitive position by accessing systems that n about billions of dollars worth of development data and information on teria. Enemies may want to better position ary by stealing information on force locations aigns and use this data to locate, target, or
Number of Attacks Is Increasing	Defense may have experien- the number of attacks is inc is difficult since some attack addition, the Department do	exact number, DISA estimates show that ceed about 250,000 attacks last year, and that reasing. Establishing an exact count of attacks kers take measures to avoid detection. In bes not detect or react to most attacks, not report the majority of attacks it does
	Page 18	GAO/AIMD-96-84 Defense information Security

Estimates of the number of computer attacks are based on DISA's Vulnerability Analysis and Assessment Program. Under this program, DISA personnel attempt to penetrate computer systems at various military service and Defense agency sites via the Internet. Since the program's inception in 1992, DISA has conducted 38,000 attacks on Defense computer systems to test how well they were protected. DISA successfully gained access 65 percent of the time (see figure 2.1). Of these successful attacks, only 988 or about 4 percent were detected by the target organizations. Of those detected, only 267 attacks or roughly 27 percent were reported to DISA. Therefore, only about 1 in 150 successful attacks drew an active defensive response from the organizations being tested. Reasons for Defense's poor detection rates are discussed in chapter 3.

Page 19

Chapter 2 Computer Attacks Pose Critical Risks to Defense



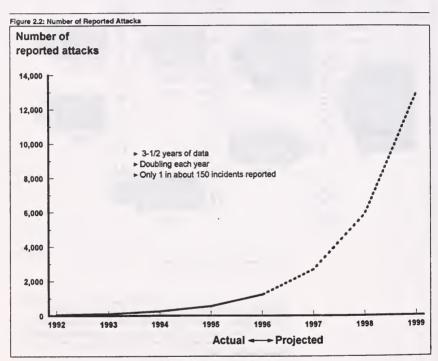
Source: Defense Information Systems Agency.

The Air Force conducts similar vulnerability assessments. Its data shows better success in detecting and reacting to attacks than DISA's data. However, Defense officials generally acknowledge that, because the Air Force's computer emergency response team resources are larger and more experienced, they have had better success in detecting and reacting to attacks than either the Navy or Army.

DISA also maintains data on officially reported attacks. Defense installations reported 53 attacks in 1992, 115 in 1993, 255 in 1994, and 559

Page 20

in 1995. Figure 2.2 shows this historical data on the number of officially reported attacks and projections for future attack activity.



Source: Defense Information Systems Agency.

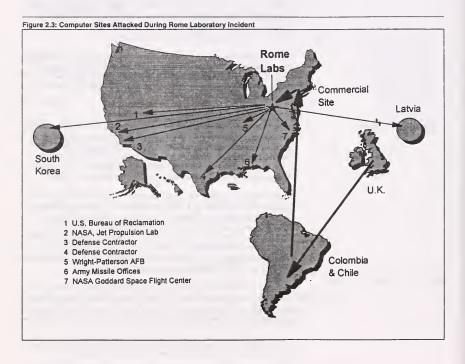
GAO/AIMD-96-84 Defense Information Security

442

Page 21

	Chapter 2 Computer Attacks Pose Critics Defense	d Risks to
Attacks Have Caused Considerable Damage	have been costly and cor modified, and destroyed unwanted files and "back protection and allow att have shut down entire sy users who depend on au Numerous Defense funct weapons and supercomp	Trials, attacks on Department computer systems usiderably damaging. Attackers have stolen, both data and software. They have installed c doors" which circumvent normal system uckers unauthorized access in the future. They restems and networks, thereby denying service to tomated systems to help meet critical missions. tions have been adversely affected, including outer research, logistics, finance, procurement, military health, and payroll.
	Following are examples Rome Laboratory, New Y particular concern to con	of attacks to date. The first attack we highlight, or /ork, was well-documented by Defense and of mmittees requesting this report because the attack o of hackers can easily and quickly take control of
Rome Laboratory	research facility. The fac intelligence systems, rad tracking systems. The la institutions, commercial	York, is Air Force's premier command and control ility's research projects include artificial ar guidance systems, and target detection and boratory works cooperatively with academic research facilities, and Defense contractors in and relies heavily on the Internet in doing so.
	made on the Laboratory The attackers used troja Rome's operational netw measures to prevent a co Rome Laboratory comp various phone switches	1994, more than 150 Internet intrusions were by a British hacker and an unidentified hacker. n horses ¹ and sniffers to access and control york. As depicted in figure 2.3, they also took omplete trace of their attack. Instead of accessing iters directly, they weaved their way through in South America, through commercial sites on the then to the Rome Laboratory.
	several days and establis they copied and downlo	to seize control of Rome's support systems for sh links to foreign Internet sites. During this time, aded critical information such as air tasking order erading as a trusted user at Rome Laboratory, they
	function, but also performs unaut ² Air tasking orders are the messa	program that when called by an authorized user performs a useful horized functions, often usurping the privileges of the user. ges commanders use during wartime to communicate air battle information to pilots and other weapons systems operators.
	Page 22	GAO/AIMD-96-84 Defense Information Securit

were also able to successfully attack systems at other government facilities, including the National Aeronautics and Space Administration's (NASA) Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations. Figure 2.3 illustrates the route the hackers took to get to the Rome Laboratory computers and the computer sites they successfully attacked from Rome.



Page 23

Because the Air Force did not know it was attacked for at least 3 days, vast damage to Rome Laboratory systems and the information in those systems could potentially have occurred. As stated in the Air Force report on the incident,³ "We have only the intruders to thank for the fact that no lasting damage occurred. Had they decided, as a skilled attacker most certainly will, to bring down the network immediately after the initial intrusion, we would have been powerless to stop them." However, the Air Force really does not know whether or not any lasting damage occurred. Furthermore, because one of the attackers was never caught, investigators do not know what was done with the copied data.

The Air Force Information Warfare Center (AFWC) estimated that the attacks cost the government over \$500,000 at the Rome Laboratory alone. Their estimate included the time spent taking systems off the networks, verifying systems integrity, installing security patches, and restoring service, and costs incurred by the Air Force's Office of Special Investigations and Information Warfare Center. It also included estimates for time and money lost due to the Laboratory's research staff not being able to use their computer systems.

However, the Air Force did not include the cost of the damage at other facilities attacked from the Rome Laboratory or the value of the research data that was compromised, copied, and downloaded by the attacker. For example, Rome Laboratory officials said that over 3 years of research and \$4 million were invested in the air tasking order research project compromised by the attackers, and that it would have cost that much to replace it if they had been unable to recover from damage caused by the attackers. Similarly, Rome laboratory officials told us that all of their research data is valueble but that they do not know how to estimate this value.

There also may have been some national security risks associated with the Rome incident. Air Force officials told us that at least one of the hackers may have been working for a foreign country interested in obtaining military research data or information on areas in which the Air Force was conducting advanced research. In addition, Air Force Information Warfare Center officials told us that the hackers may have intended to install malicious code in software which could be activated years later, possibly jeopardizing a weapons system's ability to perform safely and as intended,

*Final Report, A Technical Analysis of the Rome Laboratory Attacks, Air Force Information Warfare Center, January 20, 1996

Page 24

	and even threatening the lives of the soldiers or pilots operating the system.
Other Attacks	 The U.S. Naval Academy's computer systems were penetrated by unknown attackers in December 1994. The intrusions originated from Great Britain, Finland, Canada, the University of Kansas, and the University of Alabama. During the attack, 24 servers⁴ were accessed and sniffer programs were installed on 8 of these. A main router⁵ was compromised, and a system's name and address were changed, making the system inaccessible to authorized users. In addition, one system back-up file and files from four other systems were deleted. Six other systems were corrupted, two encrypted password files were compromised, and over 12,000 passwords were changed. The Navy did not determine how much the attack cost and Navy investigators were unable to identify the attacker(s). At a minimum, however, the attack caused considerable disruptions to the Academy's ability to process and store sensitive information. Between April 1990 and May 1991, hackers from the Netherlands penetrated computer systems to obtain full privileges allowing them future access. They read e-mail, in some cases searching the messages for key words such as nuclear, weapons, missile, Desert Shield, and Desert Storm. In several instances, the hackers copied and stored military data on systems at major U.S. universities. After the attacks, the hackers modified
	systems logs to avoid detection and to remove traces of their activities. We testified on these attacks before the Subcommittee on Government Information and Regulation, Senate Committee on Governmental Affairs, on November 20. 1991. ⁶
	 In 1995 and 1996, an attacker from Argentina used the Internet to access a U.S. university system, and from there broke into computer networks at the Naval Research Laboratory, other Defense installations, NASA, and Los Alamos National Laboratory. The systems at these sites contained
	sensitive research information, such as aircraft design, radar technology, and satellite engineering, that is ultimately used in weapons and command and control systems. The Navy could not determine what information was compromised and did not attempt to determine the cost of the incident.
	⁴ A server is a network computer that performs selected processing operations for computer users on the network.
	⁶ A router is a component that interconnects networks. Packets of information traversing the Internet travel from router to router until they reach their destination.
	*Computer Security: Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5, November 20, 1991).

Page 25

	 Unknown person(s) accessed two unclassified computer systems at the Army Missile Research Laboratory, White Sands Missile Range and installed a sniffer program. The intruder was detected entering the systems a second and third time, but the sniffer program was removed before the intruder could be identified. The missile range's computer systems contain sensitive data, including test results on the accuracy and reliability of sophisticated weaponry. As with the case above, the Army could not determine what data was compromised. However, such data could prove very valuable to foreign adversaries.
	While these are specific examples, Defense officials say they reflect the thousands of attacks experienced every year. Although no one has attempted to determine the total cost of responding to these attacks, Defense officials agreed the cost of these incidents is significant and probably totals tens or even hundreds of millions of dollars per year. Such costs should include (1) detecting and reacting to attacks, repairing systems, and checking to ensure the integrity of information, (2) lost productivity due to computer shutdowns, (3) tracking, catching, and prosecuting attackers, and (4) the cost and value of information compromised.
Future Attacks Could Threaten National Security	Because so few incidents are actually detected and reported, no one knows the full extent of damage caused by computer attacks. However, according to many Defense and private sector experts, the potential for catastrophic damage is great given (1) the known vulnerabilities of the Department's command and control, military research, logistics, and other systems, (2) weaknesses in national information infrastructure systems, such as public networks which Defense depends upon, and (3) the threat of terrorists or foreign nationals using sophisticated offensive information warfare techniques. They believe that attackers could disrupt military operations and threaten national security by successfully compromising Defense information and systems or denying service from vital commercial communications backbones or power systems.
	The National Security Agency (NSA) has acknowledged that potential adversaries are developing a body of knowledge about the Defense's and other U.S. systems, and about methods to attack these systems. According to NSA, these methods, which include sophisticated computer viruses and automated attack routines, allow adversaries to launch untraceable attacks from anywhere in the world. In some extreme scenarios, experts state that terrorists or other adversaries could seize control of Defense

Page 26

information systems and seriously degrade the nation's ability to deploy and sustain military forces. The Department of Energy and NSA estimate that more than 120 countries have established computer attack capabilities. In addition, most countries are believed to be planning some degree of information warfare as part of their overall security strategy.

At the request of the Office of the Secretary of Defense for Command, Control, Communications and Intelligence, the Rand Corporation⁷ conducted exercises known as "The Day After . . . " between January and June 1995 to simulate an information warfare attack. Senior members of the national security community and representatives from national security-related telecommunications and information systems industries participated in evaluating and responding to a hypothetical conflict between an adversary and the United States and its allies in the year 2000.

In the scenario, an adversary attacks computer systems throughout the United States and allied countries, causing accidents, crashing systems, blocking communications, and inciting panic. For example, in the scenario, automatic tellers at two of Georgia's largest banks are attacked. The attacks create confusion and panic when the automatic tellers wrongfully add and debit thousands of dollars from customers' accounts. A freight train is misrouted when a logic bomb⁸ is inserted into a railroad computer system, causing a major accident involving a high speed passenger train in Maryland. Meanwhile, telephone service is sabotaged in Washington, a major airplane crash is caused in Great Britain; and Cairo, Egypt loses all power service. An all-out attack is launched on computers at most military installations, slowing down, disconnecting, or crashing the systems. Weapons systems designed to pinpoint enemy tanks and troop formations begin to malfunction due to electronic infections.

The exercises were designed to assess the plausibility of information warfare scenarios and help define key issues to be addressed in this area. The exercises highlighted some defining features of information warfare, including the fact that attack mechanisms and techniques can be acquired with relatively modest investment. The exercises also revealed that no adequate tactical warning system exists for distinguishing between information warfare attacks and accidents. Perhaps most importantly, the

⁷Rand is a nonprofit institution whose charter is to improve public policy through research and analysis. This information warfare research was performed by Rand's National Defense Research institute, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, and the defense agencies.

⁸A logic bomb is unauthorized code that creates havoc when a particular event occurs, e.g. the perpetrator's name is deleted from the payroll or a certain date occurs.

Page 27

study demonstrated that because the U.S. economy, society, and military rely increasingly on a high performance networked information infrastructure, this infrastructure presents a set of attractive strategic targets for opponents who possess information warfare capabilities.

The Defense Science Board, a Federal Advisory Committee established to provide independent advice to the Secretary of Defense, acknowledged the threat of an information warfare attack and the damage that could be done in its October 1994 report, "Information Architecture for the Battlefield",⁹ The report states

"there is mounting evidence that there is a threat that goes beyond hackers and criminal elements. This threat arises from terrorist groups or nation states, and is far more subtle and difficult to counter than the more unstructured but growing problem caused by hackers. The threat causes concern over the specter of military readiness problems caused by attacks on Defense computer systems, but it goes well beyond the Department. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected. This is especially so for those tied to the NII (National Information Infrastructure)."

The report added that a large structured attack with strategic intent against the United States could be prepared and exercised under the guise of unstructured activities and that such an attack could "cripple U.S. operational readiness and military effectiveness."

These studies demonstrate the growing potential threat to national security posed by computer attacks. Information warfare will increasingly become an inexpensive but highly effective tactic for disrupting military operations. As discussed in chapter 3, successfully protecting information and detecting and reacting to computer attacks presents Defense and our nation with significant challenges.

*The report was prepared by a Defense Science Board task force chartered to develop recommendations on implementing an information architecture to enhance the combat effectiveness of theater and joint task force commanders.

Chapter 3

Defense Faces Significant Challenges in Countering Attacks

	The task of precluding unauthorized users from compromising the confidentiality, integrity, or availability of information is increasingly difficult given the complexity of Defense's information infrastructure, growth of and reliance on outside networks including the Internet, and the increasing sophistication of the attackers and their tools. Absolute protection of Defense information is neither practical nor affordable. Instead, Defense must turn to risk management to ensure computer security. In doing so, however, it must make tradeoffs that consider the magnitude of the threat, the value and sensitivity of the information to be protected, and the cost of protecting it.
Elements of a Good Information Systems Security Program	In our review of key studies and security documents and discussions with Defense security experts, certain core elements emerged as critical to effective information system security. A good computer security program begins with top management's understanding of the risks associated with networked computers, and a commitment that computer security will be given a high priority. At Defense, management attention to computer security has been uneven. The Defense information infrastructure has evolved into a set of individual computer systems and interconnected networks, many of which were developed without sufficient attention to the entire infrastructure. While some local area networks and Defense installations have excellent security programs, others do not. However, the overall infrastructure is only as secure as the weakest link. Therefore, all components of the Defense infrastructure must be considered when making investment decisions.
	In addition, policies and procedures must also reflect this philosophy and guide implementation of the Department's overall security program as well as the security plans for individual Defense installations. The policies should set minimum standards and requirements for key security activities and clearly assign responsibility and accountability for ensuring that they are carried out. Further, sufficient personnel, training, and resources must be provided to implement these policies.
	While not intended to be a comprehensive list, following are security activities that all of the security studies and experts agreed were important:
	(1) clear and consistent information security policies and procedures,

Page 29

(2) vulnerability assessments to identify security weaknesses at individual Defense installations,

(3) mandatory correction of identified network/system security weaknesses,

(4) mandatory reporting of attacks to help better identify and communicate vulnerabilities and needed corrective actions,

(5) damage assessments to reestablish the integrity of the information compromised by an attacker,

(6) awareness training to ensure that computer users understand the security risks associated with networked computers and practice good security,

(7) assurance that network managers and system administrators have sufficient time and training to do their jobs,

(8) prudent use of firewalls, smart cards, and other technical solutions, and

(9) an incident response capability to aggressively detect and react to attacks and track and prosecute attackers.

Defense has recognized the importance of good computer security. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence has stated,

"The vulnerability to . . . systems and networks is increasing . . . The ability of individuals to penetrate computer networks and deny, damage, or destroy data has been demonstrated on many occasions. . . As our warfighters become more and more dependent on our information systems, the potential for disaster is obvious."

In addition, as part of its Federal Managers' Financial Integrity Act¹ requirements, the Department identified information systems security as a system weakness in its <u>Fiscal Year 1995 Annual Statement of Assurance</u>, a report documenting high-risk areas requiring management attention. In its statement, Defense acknowledged a significant increase in attacks on its information systems and its dependence on these systems.

¹Public Law 97-255, September 8, 1982.

Page 30

Also, Defense has implemented a formal defensive information warfare program. This program was started in December 1992 through Defense Directive 3600.1. The directive broadly states that measures will be taken as part of this program to "protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within those systems." DISA, in cooperation with the military services and defense agencies, is responsible for implementing the program. The Department's December 1995 Defensive Information Warfare Management Plan defines a three-pronged approach to protect against, detect, and react to threats to the Defense information infrastructure. The plan states that Defense must monitor and detect intrusions or hostile actions as they occur, react quickly to isolate the systems under attack, correct the security breaches, restore service to authorized users, and improve security.

DISA has also taken a number of actions to implement its plan, the most significant being the establishment of its Global Control Center at DISA headquarters. The center provides the facilities, equipment, and personnel for directing the defensive information warfare program, including detecting and responding to computer attacks. DISA has also established its Automated Systems Security Incident Support Team (ASSIST) to provide a centrally coordinated around-the-clock Defense response to attacks. DISA also performs other services to help secure Defense's information infrastructure, including conducting assessments of Defense organizations' vulnerability to computer attacks. AFWC has developed a computer emergency response capability and performs functions similar to DISA. The Navy and Army have just established similar capabilities through the Fleet Information Warfare Center (FWC) and Land Information Warfare Activity (LWA), respectively.

Defense is incorporating some of the elements we describe above as necessary for strengthening information systems security and countering computer attacks, but there are still areas where improvement is needed. Even though the technology environment has changed dramatically in recent years, and the risk of attacks has increased, top management at many organizations do not consider computer security to be a priority. As a result, when resources are allocated, funding for important protective measures, such as training or the purchase of protection technology, take a back seat.

As discussed in the remainder of this chapter, Defense needs to establish a more comprehensive information systems security program. A program

Page 31

•
which ensures that sufficient resources are directed at protecting information systems. Specifically, (1) Defense's policies for protecting, detecting, and reacting to computer attacks are outdated and incomplete, (2) computer users are often unaware of system vulnerabilities and weak security practices, (3) system and network administrators are not adequately trained and do not have sufficient time to perform their duties, (4) technical solutions to security problems show promise, but these alone cannot guarantee protection, and (5) while Defense's incident response capability is improving, it is not sufficient to handle the increasing threat.
The military services and Defense agencies have issued a number of information security policies, but they are dated, inconsistent, and incomplete. At least 45 separate Defense policy documents address various computer and information security issues. The most significant Defense policy documents include Defense Directive 3600.1, discussed above, and Defense Directive 5200.28, entitled Security Requirements for Automated Information Systems, dated March 21, 1988, which provides mandatory minimum information systems security requirements. In addition, Defense Directive 8000.1, entitled Defense Information Management Program, dated October 27, 1992, requires DISA and the military services to provide technology and services to ensure the availability, reliability, maintainability, integrity, and security of Defense information. However, these and other policies relating to computer attacks are outdated and inconsistent. They do not set standards, mandate specific actions, or clearly assign accountability for important security activities such as vulnerability assessments, internal reporting of attacks, correction of vulnerabilities, or damage assessments.
Shortcomings in Defense's computer security policy have been reported previously. The Joint Security Commission found similar problems in 1994, and noted that Defense's policies in this area were developed when computers were physically and electronically isolated. Consequently, the Commission reported that Defense information security policies were not suitable for today's highly networked environment. The Commission also found that Defense policy was based on a philosophy of complete risk avoidance, rather than a more realistic and balanced approach of risk reduction. In addition, the Commission found a profusion of policy formulation authorities within Defense. This has led to policies being developed which create inefficiencies and implementation problems when organizations attempt to coordinate and interconnect their computer systems.

Page 32

GAO/AIMD-96-84 Defense Information Security

ł

Defense policies do not specifically require the following important security activities.

Vulnerability Assessments: DISA established a Vulnerability Analysis and Assessment Program in 1992 to identify vulnerabilities in Defense information systems. The Air Force and Navy have similar programs, and the Army plans to begin assessing its systems next year. Under its program, DISA attempts to penetrate selected Defense information systems using various techniques, all of which are widely available on the Internet. DISA personnel attack vulnerabilities which have been widely publicized in their alerts to the military services and defense agencies. Assessment is performed at the request of the targeted Defense installation, and, upon completion, systems and security personnel are given a detailed briefing. Typically, DISA and the installation develop a plan to strengthen the site's defenses, more effectively detect intrusions, and determine whether systems administrators and security personnel are adequately experienced and trained. Air Force and Navy on-line assessments are similar to DISA vulnerability assessments.

However, there is no specific Defensewide policy requiring vulnerability assessments or criteria for prioritizing who should be targeted first. This has led to uneven application of this valuable risk assessment mechanism. Some installations have been tested multiple times while others have never been tested. As of March 1996, vulnerability assessments had been performed on less than 1 percent of the thousands of defense systems around the world. Disk and the military services recognize this shortcoming, but state that they do not have sufficient resources to do more. This is a concern because vulnerabilities in one part of Defense's information infrastructure make the entire infrastructure vulnerable.

Correction of Vulnerabilities: Defense does not have any policy requirement for correcting identified deficiencies and vulnerabilities. Defense's computer emergency response teams—ASSIST, AFIWC, FIWC, and LIWA—as well as the national computer emergency response team at the Software Engineering Institute routinely identify and broadcast to Defense network administrators system vulnerabilities and suggested fixes. However, the lack of specific requirements for correcting known vulnerabilities has led to no action or inconsistent action on the part of some Defense organizations and installations.

Reporting Attacks: The Department also has no policy requiring internal reporting of attacks or guidance on how to respond to attacks. System and

Page 33

network administrators need to know when and to whom attacks should be reported and what response is appropriate for reacting to attacks and ensuring systems availability, confidentiality, and integrity. Reporting attacks is important for Defense to identify and understand the threat, i.e., size, scale, and type of attack, as well as to measure the magnitude of the problem for appropriate corrective action and resource allocation. Further, since a computer attack on federal facility is a crime, it should be reported.

Damage Assessments: There is no policy for Defense organizations to assess damage to their systems once an attack has been detected. As a result, these assessments are not usually done. For example, Air Force officials told us that the Rome Laboratory incident was the exception rather than the rule. They said that system and network administrators, due to lack of time and money, often simply "patch" their systems, restore service, and hope for the best. However, these assessments are essential to ensure the integrity of the data in those systems and to make sure that no malicious code was inserted that could cause severe problems later.

Defense Personnel Lack Sufficient Awareness and Technical Training The Software Engineering Institute's Computer Emergency Response Team estimates that at least 80 percent of the security problems it addresses involve poorly chosen or poorly protected passwords by computer users. According to the Institute, many computer users do not understand the technology they are using, the vulnerabilities in the network environment they are working in, and the responsibilities they have for protecting critical information. They also often do not understand the importance of knowing and implementing good security policies, procedures, and techniques. Defense officials generally agreed that user awareness training was needed, but stated that installation commanders do not always understand computer security risk and, thus, do not always devote sufficient resources to the problem. The officials told us they are trying to overcome the lack of resources by low cost alternatives such as banners that warn individuals of their security responsibilities when they turn on their computers.

In addition, network and system administrators often do not know what their responsibilities are for protecting their systems, and for detecting and reacting to intrusions. Critical computer security responsibilities are often assigned to personnel as additional or ancillary duties. We interviewed 24 individuals responsible for managing and securing systems at four military installations. Sixteen stated that they did not have enough

Page 34

time, experience, or training to do their jobs properly. In addition, eight stated that system administration was not their full-time job, but rather an ancillary duty. Our findings were confirmed by an Air Force survey of system administrators. It found that 325 of 709 respondents were unaware of procedures for reporting vulnerabilities and incidents, 249 of 515 respondents had not received any network security training, and 377 of 706 respondents reported that their security responsibilities were ancillary duties.

In addition, Defense officials stated that it is not uncommon for installations to lack a full-time, trained, experienced information systems security officer. Security officers generally develop and update the site's security plan, enforce security statutes and policy, aggregate and report all security incidents and changes in the site's security status, and evaluate security incidents and changes in the site's security status, and evaluate security with physical and personnel security, develop back-up and contingency plans, manage access to all information systems with sound password and user identification procedures, ensure that audit trails of log-ins to systems are maintained and analyzed, and perform a host of other duties necessary to secure the location's computer systems. Without a full-time security official, these important security activities are usually done in an ad hoc manner or not done at all. Defense officials again cited the low priority installation commanders give security difficers.

Defense has developed training courses and curricula which focus on the secure operation of computer systems and the need to protect information. For example, DISA's Center for Information Systems Security offers courses on the vulnerability of networks and computer systems security. Each of the military services also provides training in this area. While we did not assess the quality of the training, it is clear that not enough training is done. Defense officials cite resource constraints as the reason for this limitation. To illustrate, in its August 1995 Command and Control Protect Program Management Plan, the Army noted that it had approximately 4000 systems administrators, but few of these had received formal security training. The plan stated that the systems administrators have not been taught security basics such as how to detect and monitor an active intrusion, establish countermeasures, or respond to an intrusion. The plan added that a single course is being developed to train systems administrators, but that no funds are available to conduct the training. This again demonstrates the low priority top Defense management officials often give security.

Page 35

In its February 1994 report, Redefining Security, the Joint Security Commission had similar concerns, stating:

"Because of a lack of qualified personnel and a failure to provide adequate resources, many information systems security tasks are not performed adequately. Too often critical security responsibilities are assigned as additional or ancillary dutes."

The report added that the Department lacks comprehensive, consistent training for information systems security officers, and that Defense's current information systems security training efforts produce inconsistent training quality and, in some cases, a duplication of effort. The report concluded that, despite the importance of security awareness, training, and education programs, these programs tend to be frequent and ready targets for budget cuts.

According to Defense officials, installation commanders may not understand the risks associated with networked computers, and thus may not have devoted sufficient priority or resources to address these problems. These officials also cite the lack of a professional job series for information security officials as a contributing factor to poor security practices at Defense installations. Until systems security is supported by the personnel system—including potential for advancement, financial reward, and professional training—it will not be a full-time duty. As a result, security will continue to be the purview of part-time, inadequately trained personnel.

Technical Solutions Show Promise, but Cannot Alone Provide Adequate Protection As described below, Defense and the private sector are developing a variety of technical solutions which should assist the Department in preventing, detecting, and reacting to attacks on its computer systems. However, knowledgeable attackers with the right tools can defeat these technologies. Therefore, these should not be an entity's sole means of defense. Rather, they should be prudently used in conjunction with other security measures discussed in this chapter. Investment in these technologies should also be based on a comprehensive assessment of the value and sensitivity of the information to be protected.

One important technology is a smart card called Fortezza. The card and its supporting equipment, including card readers and software, were

developed by the NSA. The card is based on the Personal Computer Memory Card International Association industry standard and is a credit card size electronic module which stores digital information that can be

Page 36

recognized by a network or system. The card will be used by Defense and other government agencies to provide data encryption² and authentication³ services. Defense plans to use the card in its Defense Message System⁴ and other systems around the world.

Another technology that Defense is implementing is firewalls. Firewalls are hardware and software components that protect one set of system resources from attack by outside network users by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users. Several large commercial vendors have developed firewall applications which Defense is using and tailoring for specific organizations' computing and communications needs and environments. Like any technology, firewalls are not perfect; hackers have successfully circumvented them in the past. They should not be an installation's sole means of defense, but should be used in conjunction with the other technical, physical, and administrative solutions discussed in this chapter.

Many other technologies exist and are being developed today which DISA, NSA, and the military services are using and considering for future use. These include automated biometrics systems which examine an individual's physiological or behavioral traits and use that information to identify an individual. Biometrics systems are available today, and are being refined for future applications, that examine fingerprints, retina patterns, voice patterns, signatures, and keystroke patterns. In addition, a technology in development called location-based authentication may help thwart attackers by pinpointing their location. This technology determines the actual geographic location of a user attempting to access a system. For example, if developed and implemented as planned, it could prevent a hacker in a foreign country, pretending to come from a military installation in the United States, from logging into a Defense system.

These technical products show promise in protecting Defense systems and information from unauthorized users. However, they are expensive—firewalls can cost from \$5,000 to \$40,000 for each Internet

²Data encryption is the transformation of original text (also known as plaintext or cleartext) into unintelligible text (also called ciphertext) to help maintain the secrecy and integrity of the data.

³Authentication is the process of proving that a user or system is really who or what it claims to be. It protects against the fraudulent use of a system or the fraudulent transmission of information.

"The Defense Message System will replace Defense's current e-mail and record message systems with a single, common electronic messaging system. It will add important features to Defense's current system such as multiple levels of security, message traceability, electronic signatures, and firewalls.

Page 37

	access point, ⁵ and Fortezza cards and related support could cost about \$300 for each computer. ⁶ They also require consistent and departmentwide implementation to be successful; continued development to enhance their utility; and usage by personnel who have the requisite skills and training to appropriately use them. Once again, no single technical solution is foolproof and, thus, combinations of protective mechanisms should be used. Decisions on which mechanisms to use should be based on an
	assessment of threat, the sensitivity of the information to be protected, and the cost of protection.
Defense's Incident Response Capability Is Limited	Because absolute security is not possible and some attacks will succeed, an aggressive incident response capability is a key element of a good security program. Defense has several organizations whose primary mission is incident response, i.e. the ability to quickly detecting and reacting to computer attacks. These organizations—DISA's Center for Information Systems Security, ASSIST, and the military service teams—as discussed previously in this chapter provide network monitoring and incident response services to military installations. The AFIWC, with its Computer Emergency Response Team and Countermeasures Engineering Team, was established in 1993 and has considerably greater experience and capability than the other military services. Recognizing the need for more incident response capability, the Navy established the FIWC in 1995, and the Army established its LIWA this year. However, these organizations are not all fully staffed and do not have the capability to respond to all reported incidents, much less the incidents not reported. For example, when the FIWC was established last year, 30 personnel slots were requested, but only 3 were granted. Similarly, the LIWA is just beginning to build its capability.
	Rapid detection and reaction capabilities are essential to effective incident response. Defense is installing devices at numerous military sites to automatically monitor attacks on its computer systems. For example, the Air Force has a project underway called Automated Security Incident Measurement (ASIM) which is designed to measure the level of unauthorized activity against its systems. Under this project, several automated tools are used to examine network activity and detect and identify unusual network events, for example, Internet addresses not
	normally expected to access Defense computers. These tools have been installed at only 36 of the 108 Air Force installations around the world.
	⁸ Although there are no comprehensive estimates of the number of Internet access points, it is probably in the thousands.

⁶Defense has more than two million personal computers and workstations.

Page 38

Selection of these installations was based on the sensitivity of the information, known system vulnerabilities, and past hacker activity. Data from the ASIM is analyzed by personnel responsible for securing the installation's network. Data is also centrally analyzed at the AFIWC in San Antonio, Texas.

Air Force officials at AFWC and at Rome Laboratory told us that ASIM has been extremely useful in detecting attacks on Air Force systems. They added, however, that as currently configured, ASIM information is only accumulated and automatically analyzed nightly. As a result, a delay occurs between the time an incident occurs and the time when ASIM provides information on the incident. They also stated that ASIM is currently configured for selected operating systems and, therefore, cannot detect activity on all Air Force computer systems. They added that they plan to continue refining the ASIM to broaden its use for other Air Force operating systems and enhance its ability to provide data on unauthorized activity more quickly. AFWC officials believe that a well-publicized detection and reaction capability can be a successful deterrent to would-be attackers.

The Army and Navy are also developing similar devices, but they have been implemented in only a few locations. The Army's system, known as Automated Intrusion Monitoring System (Ants), has been in development since June 1995, and is intended to provide both a local and theater-level monitoring of computer attacks. Currently, AIMS is installed at the Army's 5th Signal Command in Worms, Germany and will be used to monitor Army computers scattered throughout Europe.

DISA officials told us that although the services' automated detection devices are good tools, they need to be refined to allow Defense to detect unauthorized activity as it is occurring. DISA's Defensive Information Warfare Management Plan provides information on new or improved technology and programs planned for the next 1 to 5 years. These efforts included a more powerful intrusion detection and monitoring program, a malicious code detection and eradication program, and a program for protecting Defense's vast information infrastructure. These programs, if developed and implemented as planned, should enhance Defense's ability to protect and react to attacks on its computer systems.

GAO/AIMD-96-84 Defense Information Security

Page 39

Chapter 4

Conclusions, Recommendations, and Agency Comments and Our Evaluation

Conclusions	Networked computer systems offer tremendous potential for streamlining and improving the efficiency of Defense operations. However, they also greatly increase the risks that information systems supporting critical Defense functions will be attacked. The hundreds of thousands of attacks that Defense has already experienced demonstrate that (1) significant damage can be incurred by attackers and (2) attacks pose serious risks to national security. They also show that top management attention at all levels and clearly assigned accountability are needed to ensure that computer systems are better protected. The need for such attention and accountability is supported by the Joint Security Commission which considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century. The Commission itself believes there is insufficient awareness of the grave risks Defense faces in this arena.
	We recognize that no organization can anticipate all potential vulnerabilities, and even if one could, it may not be cost-effective to implement every measure available to ensure protection. However, Defense can take some basic steps to vastly improve its position against attackers. These steps include strengthening (1) computer security policies and procedures, (2) security training and staffing, and (3) detection and reaction programs. Since the level of protection varies from installation-to-installation, the need for corrective measures should be assessed on a case-by-case basis by comparing the value and sensitivity of information with the cost of protecting it and by considering the entire infrastructure.
Recommendations	To better focus management attention on the Department's increasing computer security threat and to ensure that a higher priority and sufficient resources are devoted to addressing this problem, we recommend that at a minimum the Secretary of Defense strengthen the Department's information systems security program by
	developing departmentwide policies for preventing, detecting, and responding to attacks on Defense information systems, including mandating that (1) all security incidents be reported within the Department, (2) risk assessments be performed routinely to determine vulnerability to attacks and intrusions, (3) vulnerabilities and deficiencies be expeditiously corrected as they are identified, and (4) damage from intrusions be expeditiously assessed to ensure the integrity of data and systems compromised;

Page 40

	Chapter 4 Conclusions, Recommendations, and Agency Comments and Our Evaluation
	 requiring the military services and Defense agencies to use training and other mechanisms to increase awareness and accountability among installation commanders and all personnel as to the security risks of computer systems connected to the Internet and their responsibility for securing their systems; requiring information system security officers at all installations and setting specific standards for ensuring that these as well as system and network managers are given sufficient time and training to perform their duties appropriately; continually developing and cost-effectively using departmentwide network monitoring and protection technologies; and evaluating the incident response capabilities within DISA, the military services, and the Defense agencies to ensure that they are sufficient to handle the projected threat.
	Defense agencies for ensuring the successful implementation of this computer security program.
Agency Comments and Our Evaluation	On May 15, 1996, we discussed a draft of this report with officials from the Office of the Secretary of Defense, DISA, Army, Navy, and Air Force who are responsible for information systems security. In general, these officials agreed with the report's findings, conclusions, and recommendations. They stated that the report fairly represents the increasing threat of Internet attacks on the Department's computers and networks and acknowledges the actions Defense is taking to address that threat. In concurring with our conclusions and recommendations, Defense officials acknowledged that with increased emphasis and additional resources, more could be done to better protect their systems from attack and to effectively detect and aggressively respond to attacks. They stressed that accountability throughout the Department for implementing policy was as important as the policy itself and that cost-effective technology solutions should be encouraged, particularly in light of the increasing sophistication of the future threat.
	Defense officials believe that a large part of the Department's security problems result from poorly designed systems or the use of commercial off-the-shelf computer hardware and software products that have little or no inherent security. We agree that this is a serious problem. They also cited some of the more recent actions being taken to improve security,

462

Page 41

Chapter 4 Conclusions, Recommendations, and Agency Comments and Our Evaluation

such as DISA's information systems security implementation plan and the Joint Chiefs of Staff instruction on defensive information warfare. These are positive steps that will help focus attention on the importance of information security. In this context, it is important that our recommendations be effectively implemented to ensure that sufficient management commitment, accountability, priority, and resources are devoted to addressing Defense's serious information security problems.

We have incorporated the Department's comments and other points of clarification throughout the report where appropriate.

Page 42

Appendix I Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Rona B. Stillman, Chief Scientist for Computers and Telecommunications John B. Stephenson, Assistant Director Keith A. Rhodes, Technical Assistant Director Kirk J. Daubenspeck, Evaluator-in-Charge Patrick R. Dugan, Auditor Cristina T. Chaplain, Communications Analyst
Chicago/Dayton Field Office	Robert P. Kissel, Jr., Senior Evaluator
Office of the General Counsel	Frank Maguire, Senior Attorney



465

Senate Permanent Subcommittee on Investigations

2c. EXHIBIT #

COMPUTER SECURITY ISSUES & TRENDS VOL.11, NO.2

1996 CSI/FBI Computer Crime and Security Survey

By Richard Power, Editor Computer Security Institute

Recendy, the Computer Security Institute (CSI) released the results of its 1996 CSI/FBI Computer Crime and Security Survey. The news spread throughout the world via Reuters, Knight-Ridder and other wire services. Within a few hours, we went live with CNN. CBS, NBC and National Public Radio broadcast it over the air waves. Major newspapers all the country gave the story front page coverage in their business sections.

The bright media spodight culminated an effort that began at a meeting with the Federal Bureau of Investigation's San Francisco branch of its International Computer Crime Squad. They had some scrious questions they wanted answered (for example, "How bad is the threat to our country's public, semi-public and private information systems?") and some serious problems they wanted to tackle (for example, "How to encourage greater cooperation between the private sector and law enforcement in order to lessen the threat?"). We agreed to collaborate on a survey of information systems security professionals in corporations, government agencies, financial and medical institutions and universities. It was strictly an outreach effort on behalf of both CSI and the FBI. The FBI supplied the questions and CSI took full responsibility for conducting the survey and publishing the results. The results serve as a warning and a wake-up call.

For example, 42% of respondents acknowledged that they had experienced unauthorized use of computer systems within the last 12 months. And we're not talking about users playing solitaire on company time—respondents reported a diverse array of attacks from brute force password guessing (13.9% of attacks) and scanning (15% of attacks) to denial of service (16.2% of attacks) and data diddling (15.5% attacks). The figures concerning data didding in financial institutions (21% of attacks) and medical instirutions (36.8% of attacks) were higher than both the averages for other specific industry segments and the overall average. This data is chilling. It shows that private medical records, financial transactions and credit histories are at risk.

Some of the results challenge some of the "conventional wisdom" that is bandied about.

Respondents reported that their networks were being probed with frequency from several access points. Over 50% reported incidents on their internal networks and almost 40% reported frequent incidents through both remote dial-in and Internet on nections. These results tear at the "conventional wisdom" that 80% of the information security problem is due to insiders (i.e. disgruntled or dishonest employees, contractors, etc.).

Over 50% of respondents said that the information sought in probes would be of use to U.S.-owned corporate competitors. Over 50% also said that they considered U.S.-owned corporate

Computer Security Institute is the oldest international membership organization specifically serving the information security professional. Established in 1974, CSI has thousands of members worldwide and provides a wide variety of information and education programs to assist practitioners in protecting the information assets of corporations and governmental organizations.

© 1996 by Computer Security Institute all rights reserved.

competitors likely sources for eavesdropping, system penetration and other forms of attack. Foreign competitors and foreign government intelligence services also drew double-digit numbers as likely sources of attack. These results indicate that another bit of "conventional wisdom"—the pre-occupation with "hackers" from the electronic underground and disgrundled ot dishonest employees—may be ill-founded.

Perhaps the most disturbing data relates to the level of preparedness within organizations.

Over 50% of respondents don't have a written policy on how to deal with network intrusions.

■ Over 60% of respondents don't have a policy fot preserving evidence fot criminal or civil proceedings. Over 70% of respondents don't have a "Warning" banner stating that computing activities may be monitored. (Absence of "Warning" banners hampers investigations and expose an organization to liability.)

Over 20% of respondents don't even know if they've been atracked. Less than 17% of respondents who experienced intrusion(s) indicated that they reported it to law enforcement. Over 70% cited fear of negative publicity as the primary reason for not reporting.

The questionnaires were sent in February 1996. By the March 30th deadline, we had received 428 responses (8.6% of the 4, 971 questionnaires mailed). This level of response is toward the high end for such surveys dealing with the sensitive subject of information security in the past; for example, CSI's own 1995 surveys on Internet Security and Crypto, *Information Weelt* Ernst & Young's 3rd Annual "Information Security Survey" and the American Society for Industrial Security's "Trends in Intellectual Property Theft" survey.

Does the CSI/FBI survey answer every question? No. Is it the final word? There will never be a final word. Is it "scientific"? No. But it is an extensive, fascinating snapshot of the "facts on the ground" for the 428 U.S. organizations whose information security professionals took the time to answer 39 touchy questions—and as such, it is an important indicator of the overall range of threats and level of preparedness in cyberspace. Hopefully, it will lead you to ask the same questions for the sake of your own organization and measure your situation against that of our respondents.

Jim R.Freeman, Special Agent in Charge of the FBI's San Francisco office underscored the importance of this survey, stating that it reinforces the need for mutual cooperation. "I can understand," he said, "the initial reluctance of many within the private sector to report allegations of computer crime for investgation and prosecution, but as our society becomes increasingly dependent upon computer enhanced technology, with its potential abuse, it will be crucial that a more effective partnership be developed. The FBI, through its establishment of these International Computer Crime Squads stands ready to play a significant role in this partnership."

Patrice Rapalus, the Director of CSI, concurs.

"The survey results serve as a warning. There has to be a

2 🔳 1996 CSI/FBI Survey

greater commitment of resources to information systems security and increased cooperation between the private sector and law enforcement. The information age has already arrived, but most organizations are woefully unprepared," says CSI Director Patrice Rapalus. "The lack of preparedness in most organizations makes it easier for perpertators to steal, spy or sabotage without being noticed and with little culpability if they are."

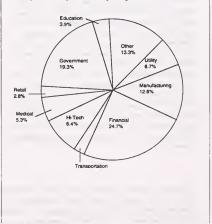
What is CSI?

CSI, established in 1974, is a San Francisco-based association of information security professionals. It has thousands of members worldwide and provides a wide variety of information and education programs to assist practitioners in protecting the information assets of corporations and governmental organizations.

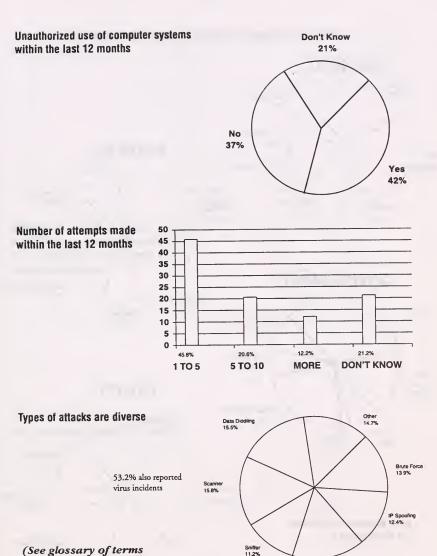
What is the FBI International Computer Crime Squad? The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, has established International Computer Crime Squads in selected offices throughout the United States. The mission of these squads is to investigate violations of Computer Fraud and Abuse Act of 1986, including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial group onage, pirated computer software and other crimes where the computer is a major factor in committing the criminal offense.

(con't. on back page)

Response by industry segment



© 1996 by Computer Security Institute all rights reserved.

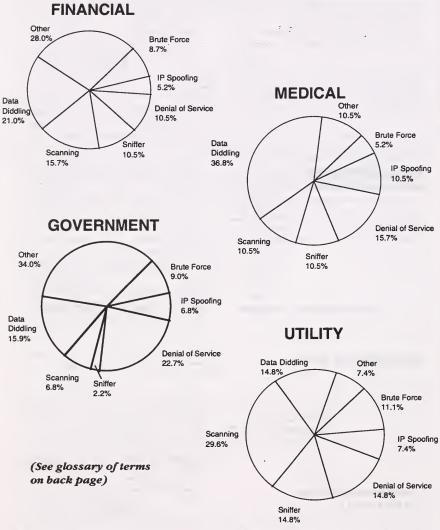


(See glossary of terms on back page)

© 1996 by Computer Security Institute all rights reserved.

1996 CSI/FBI Survey 🔳 3

Denial of Services 16.2%

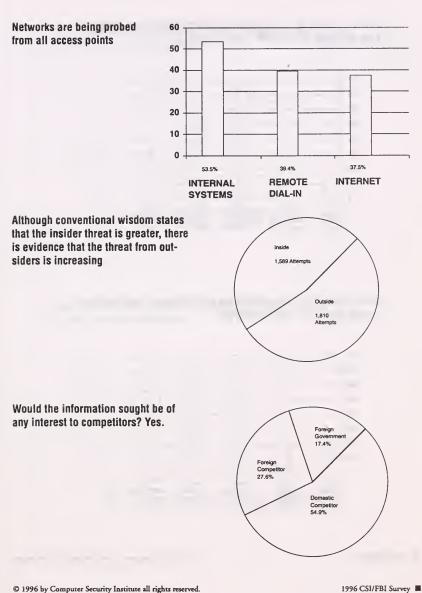


CHARACTERIZATION OF ATTACKS BY INDUSTRY SEGMENT

4 🔳 1996 CSI/FBI Survey

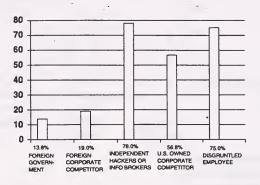
© 1996 by Computer Security Institute all rights reserved.

468

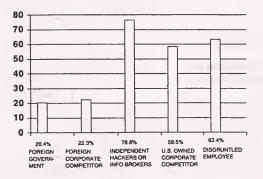


1996 CSI/FBI Survey 🔳 5

Most consider U.S. competitors (as well as hackers and insiders) a likely source for SYSTEM PENETRATION



Most consider U.S. competitors (as well as hackers and insiders) a likely source for EAVESDROPPING

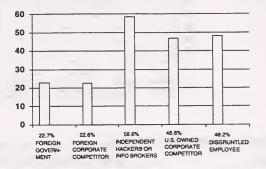


6 🔳 1996 CSI/FBI Survey

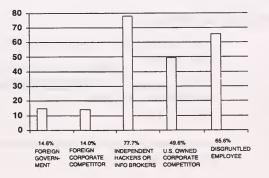
© 1996 by Computer Security Institute all rights reserved.

1.2

Most consider U.S. competitors (as well as hackers and insiders) a likely source for WIRETAPPING



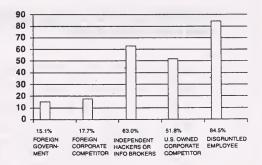
Most consider U.S. competitors (as well as hackers and insiders) a likely source for SPOOFING



© 1996 by Computer Security Institute all rights reserved.

1996 CSI/FBI Survey 🔳 7

Over 50% consider U.S. competitors a likely source for unauthorized ACCESS BY INSIDERS



Most organizations have performed some risk analysis

Has your organization performed a qualitative and/or quantitative risk assessment to determine the specific areas of potential risk that could impact your ability to perform day-today business functions?

If so, have risk assessment results been prioritized to facilitate budget allocation?

YES - 42.5%

YES - 57.5%

Most organizations have taken the next step...

Does your organization have a security awareness program?

YES - 66.0%

Does your organization have an ethics program dealing with information access and expectations of privacy?

YES - 63.1%

Does your organization have a written policy on e-mail usage?

YES - 63.5%

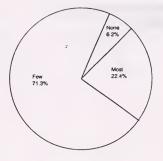
If so, does it state that management reserves the right to examine employees' e-mail?

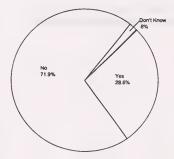
YES - 68.2%

8 🔳 1996 CSI/FBI Survey

© 1996 by Computer Security Institute all rights reserved.

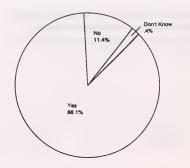
BUT...Over 70% said that few employees have a working knowledge of the current laws on misuse of computer systems





And over 70% don't have a "Warning" banner stating that computing activities may be monitored

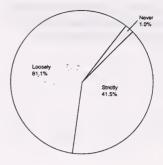
And although over 80% have a written policy on the misuse of computing facilities...

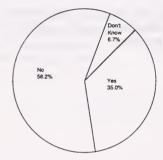


© 1996 by Computer Security Institute all rights reserved.

1996 CSI/FBI Survey 🔳 9

Over 60% state that the policy is loosely enforced





58.2% don't have a written policy on how to deal with network intrusions

And 49.8% of those that do have a policy, don't include a provision for notifying appropriate law enforcement authorities



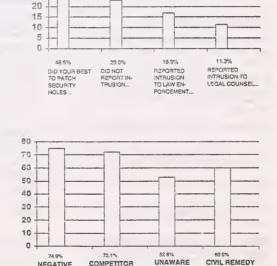
10 🔳 1996 CSI/FBI Survey © 1996 by Computer Security Institute all rights reserved.

Over 60% don't have a policy for preserving evidence for civil or criminal proceedings after a successful intrusion in which valuable information has been contoromised

Only 16.5% who experienced computer intrusions in 1995 reported them to law enforcement

Over 70% cited negative publicity and fear of competitors as likely reasons for not reporting, but over 50% also cited lack of awareness as a likely reason

© 1996 by Computer Security Institute all rights reserved.







SEEMED BEST

50 45

40

35

30 25

NEGATIVE

PUBLICITY

USE TO



Over 80% would find it useful to receive a general presentation on computer crime from the FBI



Definitions of Types of Attack

Brute force - In a brute force password guessing attack, every possibility is attempted until a match is found.

IP spoofing- A method of disguise in which an attacker forges the address on data packers sent over the Internet so that they appear to come from inside a network in which systems rust each other.

Data diddling - Altering of data in an unauthorized manner.

Denial of service - An action or actions that prevent a network or any of its parts from functioning normally.

Sniffer - A password sniffer monitors all traffic on a network to collect passwords.

VITUS - A self-propagating program that may cause damage in some way, for example, by corrupting or erasing files.

Scanner - For example, an automated program such as SATAN that probes for network vulnerabilities or a war dialer that dials relephone numbers to identify those connected to moderns.

Acknowledgements

CSI would like to thank FBI Supervisory Special Agent George V. Vinson, FBI Special Agent Patrick K. Murphy, FBI Special Agent Willard L. Hatcher and FBI Media Coordinator George E. Grotz for their tireless efforts to make this outreach a success.

Inquiries

For further information on survey results, contact: Richard Power, Editor, Computer Security Institute 600 Harrison SL, San Francisco, CA. 94107 tel #: 415-905-2218 or email: power@mfi.com

For specific computer crime referrals, contact: Patrick Murphy, Special Agent, FBI International Computer Crime Squad 450 Golden Gate Ave, San Francisco, CA 94102 et#: 415-553-2049, fax #: 415-553-7674

FREE one month introductory membership offer!

Computer Security Institute (CSI) is the industry's leading membership organization whose goal is to assist members, provide practical and cost-effective solutions to information security protection. As a CSI



member, you have the most up-to-date information on computer security at your fingertips. CSI is a solid support resource you can count on—giving you expert, practical advice and information. Since 1974 CSI has been serving and training thousands of members worldwide.

YES! SIGN ME UP FOR FREE ONE MONTH INTRODUCTORY OFFER.

Stote	Zip
Fex	

FAX OR MAIL THIS COUPON TO:

Computer Security Institute 600 Harrison Street San Francisco, CA 94107 Phone: 415-905-2626 Fax 415-905-2218 Email: alupear@mfi.com

		CERT (s	m) Coordination C	enter Statistics	EXHIBIT #	3a.
Year	Number of	: Incidents Reported(1)		Information Requests Received(2)		-
1988		6	539			-
1989		132	2867			
1990		252	4448			
1991		406	9629			
1992		773	14463	275	1995	
1993		1334	21267	1270	2282	
1994		2341	29580	1527	3664	
1995		2412	32084	1683	3428	

Footnotes

- (1) Please note that an incident may involve one site, or hundreds or thousands of sites. Also, some incidents consist of ongoing activity for long periods of time (more than a year).
- (2) Information requests have been tabulated beginning July 1992. This number does not include requests to be added to mailing lists.
- (3) Incoming hotline calls have been tabulated since January 1992. This number does not reflect total telephone activity related to incidents because outgoing calls made by CERT staff are not included.

Comments on Trends in CERT Statistics

Each year since The CERT Coordination Center was established in November 1988, we have seen dramatic increases in activity. The primary causes are

- * Increases in the number of Internet hosts * Corresponding increases in intruder activity
- * Increases in the Internet community's awareness of security issues and of the existence of the CERT/CC

The 1995 statistics show a shift from previous trends.

Incidents:

The number of incidents reported to the CERT/CC continued to increase, but the growth rate has decreased for the first time. We believe the factors include

- * Existence of incident response teams that serve a specific constituency of the Internet community. Many incidents are now reported to these teams rather than to the CERT/CC.
- * Improved ability of site personnel to handle incidents directly. Sites with whom we have worked now handle some repeat incidents without reporting them to the CERT/CC.

- Note: The CERT/CC would still like to receive information about all incidents, even the ones sites handle themselves. This information enables the staff to build a "big picture" of intruder activity; we can then provide that broad view to the Internet community, increasing their ability to assess risk.
- Increased facility for the CERT staff to identify related intruder activities from diverse incident reports. As a result, there are fewer separate incidents but more large, complex ones.

What the statistics in this file do not show are the increased sophistication of the toolkits used by intruders and the way knowledgeable intruders share their expertise with novices.

Hotline calls:

In 1995, the CERT/CC has seen a decrease in the number of hotline calls received. We have encouraged sites to report incidents by encrypted email or FAX because written details enable us to provide better assistance. Because we support both DES and PGP, sites can report incident information by email without concern about the information being intercepted.

Interestingly, in 1995 we saw an increase in the number of hotline calls from sites requesting information on how to connect to the Internet securely "before" the site actually connected. We hope to see this trend continue.

Copyright 1996 Carnegie Mellon University.

This material may be reproduced and distributed without permission provided it is used for noncommercial purposes and the CERT Coordination Center is acknowledged.

CERT is a service mark of Carnegie Mellon University.

Senate Permanent Subcommittee on Investigations

EXHIBIT # 5c.



479

Emerging Challenge

IEEE Technology and Society Magazine

Reprinted from

Security and Safety in Cyberspace

Richard O. Hundley and Robert H. Anderson

Emerging Challenge: Security and Safety in Cyberspace

the more and more of the activities of individuals, organizations, and nations county of those activities is an emerging challenge for society. The medium has thus created new potentials for criminal or hostile actions, "bad actors" in cyberspace carrying out these hostile actions, and threats to societal interests as a result of these hostile actions.

IF CARLEN AL

Potential Hostile Actions

Security holes in current computer and telecommunications systems allow these systems to be subject to a broad spectrum of adverse or hostile actions. The spectrum includes: inserting false data or harmful programs into information systems; stealing valuable data or programs from a system, or even taking over control of its operation; maaipulating the performance of a system, by changing data or programs, introducing communications delays, etc.; and disrupting the performance of a system, by causing erratic behavior or destroying data or programs, or by denying access to the system. Taken together, the surreptitious and remote nature of these actions can make their detection difficult and the identification of the perpetrator even more difficult. Furthermore, new possibilities for hostile actions arise every day as a

The authors are with the Rand Corporation, Santa Monica, CA. Email:Richard_Hundley@rand.org and Robert_Anderson@rand.org. This work was partly supported by the Office of the Secretary of Defense, and the Advanced Research Projects Agency. result of new developments and applications of information technology.

The bad actors who might perpetrate these actions include: hackers, zealots or disgruntled insiders, to satisfy personal agendas; criminals, for personal financial gain, etc.; terrorists or other malevolent groups, to advance their cause; commercial organizations, for industrial espionage or to disrupt competitors; nations, for espionage or economic advantage or as a tool of warfare. Cyberspace attacks mounted by these different types of actors are indistinguishable from each other, insofar as the perceptions of the target personnel are concerned. In this cyberspace world, the distinction between "crime" and "warfare" in cyberspace also blurs the distinction between police responsibilities, to protect societal interests from criminal acts in cyberspace, and military responsibilities, to protect societal interests from acts of war in cyberspace

We call protecting targets in cyberspace, such as government, business, individuals, and society as a whole, against these actions by bad actors in cyberspace, "cyberspace security." In addition to deliberate threats, information systems operating in cyberspace can also cause unforeseen actions or events — without the intervention of any bad actors — that create unintended (potentially or actually) dangerous

¹As one consequence of the electronic digitization of information and the worldwide intermetting of computer systems, more and more activities throughout the world are mediated and controlled by information systems. The global world of intermeted computers and communications systems in which these activities are being carried out has come to be called "cyberspace," a term originated by William Gibson in his novel "Neuromancer."

19

Reprinted by permission from *IEEE Technology and Society Magazine*, Vol. 14, No. 4, Winter 1995–1996, pp. 19–28. Copyright © 1995 the Institute of Electrical and Electronics Engineers, Inc.

_

SECURINITY AND SAFETY

situations for themselves or for the physical and human environments in which they are embedded. Such safety hazards can result from both software errors and hardware failures. We call protection against this additional set of cyberspace hazards "cyberspace safety." In the new cyberspace world, government, business, individuals, and society as a whole require a comprehensive program of cyberspace security and safety (CSS) [1]-[5]."

> Cyberspace information systems are subject to a broad spectrum of adverse or hostile actions.

Consequence Categories

We have used four categories to define the consequences of cyberspace attacks, categories based on the degree of economic, human, or societal damage caused. From the least to the most consequential, they are:

 minor annoyonce or inconvenience, which causes no important damage or loss, and is generally self-healing, with no significant recovery efforts being required;

2) limited misforune, which causes limited economic or human or societal damage, relative to the resources of the individuals, organizations, or societal elements involved, and for which the recovery is straightforward, with the recovery efforts being well within the recuperative resources of those affected, organizations, or societal elements;

3) major or widespread loss, which causes significant economic or human or societal dam-

⁻²In addressing questions of cyberspace security and safety, we have relied on a variety of anecdotal information obtained from a number of sources. The anecdotal data by no means constitute a comprehensive, statistically valid sample, In principle, one could develop auch a sample from databases from the various computer emergency response teams (CERTs), law enforcement databases, and private sector incident data. However, we have yet to find anyone who has done so.

There are a number of reasons for this. One is that many if not most cyberspace security incidents apparently go unreported to authorities, particularly in the financial community. It is therefore unclear if the incidents that are reported are "the tip of the iceberg," or all there is to the problem. Lacking a comprehensive sample, the total quantitative

Lacking a comprehensive sample, the total quantitative dimensions of the cyberspace security problem are unclear. Therefore, we present here our qualitative impressions of the problem. age, relative to the resources of those involved, and/or which may affect, or threaten to affect, a major portion of society, and for which recovery is possible but difficult, and strains the recuperative resources of the affected individuals, organizations, or societal elements; and

4) major disaster, which causes great damage or loss to affected individuals or organizations, and for which recovery is extremely difficult, if not impossible, and puts an enormous, if not overwhelming, load on the recuperative resources of those affected.

We assert that it is not always possible to measure human or societal damage in purely economic terms.

Past Incidents

CSS incidents constituting a minor annoyance or inconvenience have been a frequent occurrence across the entire spectrum of target categories. For some targets (e.g., the AT&T Bell Labs computer network or the unclassified Pentagon network) such minor annoyances can occur one or more times every day. For many computer installations, such incidents have becomes to commonplace that they are no longer reported.

CSS incidents constituting a limited misfortune — e.g., computer installations disrupted for limited periods of time, or limited financial losses (relative to the resources of the target) — have occurred less frequently, but nevertheless numerous examples exist across the entire spectrum of targets. A number of these are reported in [1] and [4].

There have even been a few cases of incidents which many observers would class as major or widespread loss to the target(s) involved. Exam-ples include the "AIDS Trojan" attack in December 1989, which caused (among many other things) an AIDS research center at the University of Bologna in Italy to lose 10 years of irreplaceable data [4]; the AT&T network failure on January 15, 1990, due to a software error. which disrupted and virtually shut down a major portion of the U.S. nationwide long-distance network for a period of about nine hours [1], [4]: the almost total disruption of the computers and computer networks at the Rome (NY) Air Force Base for a period of 18 days in early 1994, during which time most (if not all) of the information systems at Rome were "disconnected from the Net" [6]; and the MCI calling-card scam during 1992-1994, in which malicious software was installed on MCI switching equipment to record and steal about 100 000 calling card numbers and personal identification codes that were then sold to hackers throughout the U.S. and Europe and posted on bulletin boards, resulting in an estimated \$50 million in unauthorized long-distance calls [7].

IEEE Technology and Society Magazine, Winter 1995/1996

482

	Table I enetration Incidents Carnegle-Mellon CER
Year	Incidents Reported
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2241

We know of no clear examples to date of a CSS incident constituting a major disaster.

Potential Future Incidents

Whatever may have happened in the past, we expect cyberspace security and safety incidents to become much more prevalent in the future, due to the facts that more and more people are becoming "computer smart" all over the world; bad actors of many different types are becoming more and more aware of opportunities in cyberspace; connectivity is becoming more widespread and universal; more and more systems and infrastructures are shifting from mechanical/electrical control to electronic/software control; and human activities in cyberspace are expanding much faster than security efforts.

Recent data support this expectation. For example, the number of Internet penetration incidents reported to the computer emergency response team (CERT) at Carnegie-Mellon University each year since 1982 are shown in Table I [8].

Accordingly, we expect that, in the future, CSS incidents constituting a minor annoyance or inconvenience will become commonplace across the entire spectrum of targets; incidents constituting a limited misfortune could also become a common occurrence; CSS incidents constituting a major or widespread loss are quite possible for all targets in cyberspace; and CSS incidents constituting a major disaster are definitely possible for some targets in special cases. Some examples of special cases in which major

disasters may be possible include the following:

- Physical and functional infrastructures, such as the air traffic control system, possibly leading to the crashes of one or more aircraft.
- Milliary and national security. For example, if a cyberspace-based attack were to bring down an essential military command and control system at a critical moment in a battle, it might lead to the loss of the

IEEE Technology and Society Magazine, Winter 1995/1996

battle. If the battle were pivotal, or the stakes otherwise high enough, this could ultimately lead to military disaster.

 Other societal organizations and activities.
 With medical care becoming increasingly dependent on information systems, many of them intermetted, a perpetrator could make changes to data or software, possibly resulting in the loss of life.

Other examples of possible cases leading to major disasters may occur to the reader. Today these examples are all hypothetical. Tomorrow one or more of them could well be real. Our impression is that CSS incidents will become much more prevalent; they will impact almost every corner of society in the developed nations of the world; and the consequences could become much preater.

Infrastructure Fragility

There are many uncertainties associated with this projection of future cyberspace security and safety incidents. Attacks on vital infrastructures are one of the things most likely to cause widespread repercussions for society. Accordingly, one of the most important uncertainties has to do with the degree of robustness of current and future infrastructures. Are the key physical and future infrastructures. Are the key physical and future inflastructures in various nations highly robust, due to built-in redundancies and self-healing capabilities? Or do some infrastructures have hidden fragilities that could lead to failures having important consequences?

Conventional wisdom regarding these questions is not always correct. For example, prior to 1990, the AT&T long distance network in the U.S. was usually thought to be very robust, with many alternative paths for long distance calls to take, going through different switching centers. But all of these switching centers use the same software, and when new software was introduced in 1990, every long-distance switch had the same bad line of code. So at the software level, here was no redundancy at all, but rather a fragility that brought a large part of the AT&T long-distance network down [1], [4].

The message is clear: many infrastructures may not be as robust as they seem; a detailed look at vulnerabilities of specific infrastructures is needed.

Actors Responsible for Incidents

By far the greatest portion of past cyberspace security incidents have been perpetrated by "hackers": individuals satisfying a variety of personal agendas, which in their view do not include criminal motives [9], [10]. This continues to be the case regarding current incidents.

In recent years, the role of criminals in cyberspace incidents has increased. According to law enforcement professionals consulted by the authors, this has come about not as a result of the criminal element becoming more aware of opportunities in cyberspace, but rather primarily as a result of computer hackers "growing up" and some (small) fraction of them realizing and exploiting the financial opportunities open to them via criminal acts.

There are no known cases in the open literature of cyberspace security incidents perpetrated by terrorists or other malevolent groups, commercial organizations, or nations. However, there are plenty of rumors of business organizations and intelligence agencies outside the U.S. that have mounted cyberspace-based attacks against companies in other nations as a means of industrial or economic expionage.

New possibilities for hostile actions arise every day.

In addition, police authorities in Europe have recently begun to discern a number of potentially more dangerous actors manipulating and guiding some malicious hacker activity. This appears to include professional hackers, who are often the source of the penetration tools used by the "ordinary" hackers; information brokers, who frequently post notices on European hacker bulletin boards offering various forms of "payment" for specific information; private detectives, who also often use the European hacker bulletin boards as a means of obtaining information regarding targeted individuals or organizations; foreign embassies, who appear to have been behind the bulletin board activities of least some European private detectives and information brokers; and organized crime

Whatever may have happened in the past, in the future we expect all five of our classes of bad actors to continue participating in cyberspace security incidents.

Mechanisms: Past and Future

A number of mechanisms have been prevalent in past cyberspace security and safety incidents and are likely to be prevalent in future incidents as well. Many incidents involve more than one of these mechanisms, which include:

- ▼Operations-based attacks, taking advantage of inadequate or lax recently environments. Exploitation of deficient security environments has been a feature of many/most past successful cyberspace penetrations and is likely to continue to be prevalent in the future — as long as tax security continues to be commonplace.
- Vser authentication-based attacks, which bypass or penetrate login and password protections. Such attacks are a common feature of many/most past cyberspace security incidents and are also likely to be prevalent in the future.
- Software-based attacks, exploiting software features (e.g., maintenance backdoors), programmatic flaws, and logical errors or misjudgments in software implementation, as well as the insertion of maincous software.
- ▼ Network-based attacks. which take advantage of network design, protocol, or topology in order to gather data, gain unauthorized system access, or disrupt network connectivity. This can include alterations of routing tables, password sniffing, and the spoofing of TCP/IP packet addresses. Attacks of this type have not been common in the past. However, beginning in 1994 hackers have been detreted pentrating Internet routers to instal't password sniffers, etc.; TCP/IP packet address poofing was first detected in early 1905. Such attacks — including attempts to disrupt Internet connectivity. — could become much more commen in the future, unless Internet security is marketife improved.
- ▼ Hardware-based attacks or funares, exploiting programmatic or legical flaws in hardware design and implementation, or component failures. These have not been a feature of past cyberspace security incidents (i.e., diliberately prepertical incidents), but have playeo a role in occasional safety hazards (i.e., accidental incidents). This is likely to commune when where where

Additional Key Factors

There are a number of additional factors impacting on the cyberspace security problem and of necessity shaping any effective protective strategies.

Increasing Transnationalism

As is well known, cyberspace does not respect national boundaries. In recent years more and more nations throughout the world have become "connected" to the world network, and within those nations connectivity has become more and more universal.

IEEE Technology and Society Magazine, Winter 1995/1996

Every year greater numbers of individuals and organizations in the U.S. are taking advantage of this increasing worldwide connectivity to become involved, via cyberspace, in economic or social activities with individuals and organizations in other nations. These transnational activities are becoming increasingly important to the U.S. individuals and organizations involved; they will not willingly give them up.

Since threats in cyberspace pay no regard to regional or national boundaries, knowledge of computer hacking techniques has spread around the globe, and the perpetrator of a security incident can just as well be on the other side of the world as across the street.

For both of these reasons—the nature of activities in cyberspace and the nature of threats cyberspace has become effectively transnational. No nation has effective sovereignty over cyberspace. Any effective cyberspace protective strategy must take this into account.

Current Security inadequate

The information processing systems and telecommunications systems currently in use throughout the world are full of security flaws, and new security flaws are being uncovered almost every day, usually as a result of hacker activity. As new developments and applications of information technology become available and as human activities in cyberspace continually expand, security efforts appear to be lagging behind. There is currently no effective way to police cyberspace. Considering the rapid increase in the number of reported security incidents in recent years, along with the apparent increase in the severity of these incidents, it does not appear that the "good guys" are winning; they may not even be holding their own.

Current security operations in cyberspace are inadequate. This is not the result of a lack of security technology. Rather, it reflects a very limited application of available technology; most of the available computer security technology is not used in most of the computers in the world.

Acceptance Lacking

The U.S. has had a computer security program since the 1960s. In spite of these efforts, the U.S. is full of insecure computers today. There are several reasons for this. A primary reason is that user acceptance and utilization of available computer security safeguards has been reluctant and limited. There are several causes of this lack of user acceptance.

 Typically, user interfaces accompanying security features are awkward. As a result, the secure systems are more difficult to use than the nonsecure systems. Many users are not motivated to take the extra effort.

IEEE Technology and Society Magazine, Wester 1995/1996

- Users have not considered security features as adding value, and therefore are reluctant to pay extra for such features.
- Computer hardware and software manufactures have not perceived the security market as being attractive. Rather, it has usually been considered a limited, niche market. Therefore the largest commercial manufacturers (hicrosoft, Apple, etc.) have not included many security features in their primary product lines.
- Many individual users do not understand the need for a communal role in cyberspace security and do not accept responsibility for such a role.
- Most users don't take computer security seriously until something bad has happened to them or to their immediate organization.

For reasons such as these, most of the computer security technology currently available is not used on most of the computers in the world. A typical computer on the Internet uses a garden variety Unix operating system with few additional security safeguards. Similarly, a typical desktop computer uses the MS-DOS, MS-DOS plus Windows, or Macintosh operating systems, once again with few additional security safeguards. The various secure operating systems, multilevel security systems, and Orange Book² compliant software systems that have been developed are primarily used in restricted, niche applications.

Isolation Disappearing as Option

Twenty or thirty years ago there was a simple solution to this problem: the physical isolation of computer systems, what is now called an "air gap." This is no longer a viable option. As more and more human activities move into cyberspace to take advantage of the efficiencies provided by interconnection. organizations and individuals who fail or refuse to connect will increasingly fall behind the pace of economic and social activity, will become increasingly noncompetitive in their area of activity, and will have difficulty accomplishing their missions. This idea is stated succinctly in a report of the Joint Security Commission appointed by the U.S. Secretary of Defense and the Director of Central Intelligence to develop a new approach to security to meet the challenges facing the Department of Defense and the Intelligence Community in the post-Cold War era [13]:

"Those who steadfastly resist connectivity will be perceived as unresponsive and will ultimately be considered as offering little value to

³The "Orange Book" is a common term for the DOD Trusted Computer System Evaluation Criteria (TCSEC) [12].



STATISTIC AND SAFETY

their customers. ... The defense and intelligence communities share this imperative to connect."

▼ Roles and Missions Blurred

By their nature, developments in cyberspace blur the distinction between crime and warfare, hereby also blurring the distinction between police responsibilities to protect U.S. interests from criminal acts in cyberspace, and military responsibilities to protect U.S. interests from acts of war in cyberspace.

In addition, providing protection against transnational threats in cyberspace, and apprehending their perpetrators, frequently goes well beyond the reach and resources of local and regional authorities.

These two characteristics of security in cyberspace — the blurring of the distinction between crime and warfare, and the transational nature of many security incidents — raise new questions regarding the proper roles and missions in cyberspace security and safety. Some of the agencies, organizations, and institutions that have essential roles to play, from the viewpoint of one living in the U.S. include:

- U.S. federal government, including intelligence agencies, the Department of Defense, federal law enforcement agencies; civilian regulatory agencies; and other civilian agencies;
- U.S. State and local governments, including law enforcement agencies and regulatory agencies;
- Nongovernmental organizations such as CERTs, business and professional associations, vendors, industry standard-setting bodies, and private businesses;
- Governments of other nations, including intelligence agencies, ministries of defense, and law enforcement agencies;
- International organizations such as the United Nations, supranational governing bodies, Interpol, and international standards bodies.

Today this is "everybody's" problem, and therefore "nobody's" problem. It falls into all of the cracks.

Useful Metaphors

These various characteristics of the current security situation in cyberspace suggest three metaphors which may stimulate thinking about protective strategies.

▼ "Wild West" World

Cyberspace has many similarities to a Wild West world.

In the Wild West almost anything could occur. There was no one to enforce overall law and order, only isolated packets of local law. The same is true in cyberspace.

- There were both "good guys" and "outlaws" in the Wild West, often very difficult to tell apart. "Friends" were the only ones a person could trust, even though he or she would frequently have to deal with "strangers." This is also true in cyberspace.
- Outside of the occasional local enclaves of law and order, everyone in the Wild West was primarily dependent for security on their own resources and those of their trusted friends. This is also true in cyberspace.

The message of this metaphor for cyberspace security is clear. If there is no way to enforce law and order throughout all of cyberspace, which appears to be the case, one must rely on local enclaves of law and order, and trusted friends.

Medieval World

The medieval world depended on local enclaves for security: castles and fortified cities, protected by a variety of fortifications – moats, walls, and drawbridges. Communication and commerce between these fortified enclaves was carried out and/or protected by groups of armored individuals.

This metaphor also suggests a message for cyberspace security: cyberspace fortifications (i.e., firewalls) can protect the local enclaves in cyberspace, just as moats and walls protected the castles in the medieval world.

We have found the security concepts suggested by these two metaphors — local enclaves and firewalls — to be very compelling, and usable as part of a basic paradigm for cyberspace security.

Biological Immune System

The problems faced by biological immune systems have a number of similarities to the challenges confronting cyberspace security. This suggests that the "security" solutions employed by immune systems could serve as another useful model for cyberspace security. For example:

- Higher-level biological organisms are comprised of a large number of diverse, complex, highly interdependent components. So is cyberspace.
- Biological organisms face diverse dangers (from microbes) that cannot always be described in detail before an individual attack occurs, and which evolve over time. Organisms cannot defend against these dangers by "disconnecting" from their environment. The same is true of information systems exposed to threats in cyberspace.

LEEE Technology and Society Magazine, Winter 1995/1996



▼ Biological organisms employ a variety of complementary defense mechanisms, including both barrier defense strategies involving the skin and cell membranes, and active defense strategies that 9 nse the presence of outsiders (i.e., antigens) and respond with circulating killers (i.e., antibodies). The cyberspace firevalls are an obvious analogue to the biological barrier defenses. But what about the active

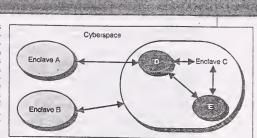


Fig. 1. An orchitectural concept and basic paradigm for cyberspace security: local enclaves, of various sizes, some of them nested, protected by firewalls.

defenses? Perhaps software agents could be created providing a cyberspace active defense analogue to biological antibodies.

The biological agents providing the active defense portion of the immune system employ certain critical capabilities: the ability to distinguish "self" from "nonself"; the ability to create and transmit recognition templates and killer mechanisms throughout the organism; and the ability to evolve defenses as the "threat" changes.

Software agents providing a cyberspace active defense analogue to these biological antibodies would need the same capabilities.⁴

The message of this metaphor is clear: Cyberspace security would be enhanced by active defenses capable of evolving over time.

We find this third metaphor as compelling as the first two; however, we are not as far along in exploiting it in our analysis.

Security Strategy

Using the concepts suggested by the Wild West and Medieval metaphors, Fig. 1 depicts the basic paradigm and overarching architectural concept we suggest for cyberspace security: local enclaves protected by firewalls. These enclaves can be of various sizes, some of them can be nested, and the firewalls can be of various permeabilities. The enclaves have protected connections to other trusted enclaves, and timited connections to the rest of cyberspace.

In this architectural concept, no attempt is made to maintain centralized law and order throughout all of cyberspace. Each authority maintains local law and order in its own enclave. Everything outside of the enclaves is left to the "wild west."

These enclaves can come in a variety of sizes, ranging from an individual computer to a com-

⁴We are not the first to be intrigued by this metaphor. Forrest *et al.* [14] and Kephart [15] discuss software implementations of certain aspects of the biological immune system metaphor.

IEEE Technology and Society Mayzzine, Winter 1995/1996

plete network. The firewalls protecting these various size enclaves come in several different types, with different degrees of permeability.⁵

In the most extreme case, one can have an air gap, i.e., the absence of any electronic connection between the interior of the enclave and the outside world. Within this overall category, there can be various degrees of permeability, depending upon what software and/or data are allowed in and out, on diskettes, tapes, etc., and how rigorously this software and data are checked.

When electronic connections are allowed, a firewall computer stands between the world outside the enclave and the internal machines. Two main categories of variations are possible:

1) Different services can be allowed to come in or to go out, depending on the permeability desired of the firewall. Typical service categories include electronic mail, file transfer (e.g., FTP), information servers (e.g., World Wide Web browsers), and remote execution (e.g., Telnet). Of these four categories, electronic mail is the safest to interchange with the outside world and remote execution is the most dangerous in the sense of providing opportunities that hackers can exploit to penetrate the firewall barrier and gain control of internal machines. Accordingly, even the tightest firewalls usually allow the passage of electronic mail in both directions, whereas only the loosest firewalls allow the passage of remote execution services, particularly in the inward direction.

2) Some allowed services can terminate (or originate) at the firewall machine, while oblers can go right through the firewall to the internal machines (incoming services) or to the outside world (outgoing services). The fewer services that pass through the firewall, the tighter it is.

These variations in the permeability of electronic firewalls can be tuned to the circumstances of the particular enclave.

³We are certainly not the first to suggest firewalls as a protective technique or as a central element of a protective strategy. See [16]-[18].



1.1.4. A. (1)。4.答:"是不

Protective Techniques and Procedures

In addition to firewalls, there are a number of other protective techniques and procedures which have important roles to play in our strawman protective strategy. These include:

- Improved access controls, including onetime passwords, smart cards, and shadow passwords.
- More secure of ware. This could include expanded use of software independent verification and validation (IV&V) techniques, to find and eliminate software bugs and security holes in widely used software, as well as more secure operating systems.
- Encrypted communications, both between and within protected enclaves.
- Encrypted files, for data that is particularly sensitive.
- Improved capabilities to detect penetrations, including user and file-access profiling.
- Active counteractions, to harass and suppress bad actors. This is something that is woefully lacking today; almost all current computer security measures are either passive or counteractive, leaving the initiative to the perpertator.
- Software agents, perhaps acting in a manner similar to a biological immune system.

Motivating Users

The best protective strategy in the world and the best set of protective techniques and procedures will be ineffective if users do not employ them. Necessary (and hopefully sufficient) ways to motivate users include:

 A vigorous program of education and training, of both users and managers concerned with information systems in potential target organizations — education, so that people will understand the magnitude of the risk to their interests and the importance of cyberspace security, and training, so that people will know how to protect themselves.

2) Proactive programs to demonstrate vulnerabilities — sometimes called "red teams" — and thereby to increase organizational and individual awareness of cyberspace vulnerabilities. The Vulnerability Analysis and Assistance Program (VAAP) of the U.S. Center for Information Systems Security (CISS) is a good example of such a proactive program [20].

3) Mandates, tailored to different societal elements. These can include mandatory security procedures established by an organization for all of its employees or members to follow, mandatory security standards that a computer host must meet in order to be permitted to connect to a network, security standards and procedures that organizations and individuals must adhere to in order not to incur legal liability, and even possibly laws mandating certain minimum levels of security standards for information systems engaged in certain types of public activity.

4) Sanctions, to enforce the mandates.

Complete Protective Strategy

In addition to the elements we have discussed thus far, a complete cyberspace protective strategy needs at least two additional elements.

1) A set of prescriptions governing the application of the basic security paradigm and the set of protective techniques and procedures to different security situations: for protecting different elements of society; for countering different actors; and for determining what role various agencies and organizations should play in cyberspace security, in which situations. These prescriptions — in particular those associated with the assignment of roles and missions in cyberspace security — may well differ from nation to nation.

2) A built-in mechanism or mechanisms to continually update the protective techniques and procedures, and the overall strategy, as information technology continues to evolve and its applications to expand, and as new threats emerge.

These elements remain to be developed.

Open Questions, Key Issues

A number of open questions and key issues should be resolved in the process of proceeding further. These include:

- What specific organizations and activities comprise what we will call the "National Interest Element" in the U.S. or any other nation? That is, what organizations, information systems, and activities play such vital roles in society that their disruption due to cyberspace attacks would have national consequences, and their protection should therefore be of national concern?
- Which organizations (in each nation) should play what roles in the protection of the National Interest Element?
- How robust or fragile are essential infrastructures contained in the National Interest Element of each nation? This is one of the key uncertainties in our current understanding of the cyberspace security situation. A detailed look at the vulnerabilities of specific infrastructures in various nations is needed to resolve this issue.
- How does one protect against the trusted insider? Our basic security paradigm of local enclaves protected by firewalls protects against malicious outsiders, but not necessarily against malicious insiders, individuals inside the firewall with all of the

IEEE Technology and Society Magazine, Winter 1995/1996



access privileges of a trusted member of the enclave. As knowledge of hacker techniques spreads throughout the population. adverse actions by malicious insiders is becoming more and more of a problem. We have not discussed this here, but it is an important threat with which any complete cyberspace security strategy should deal. It becomes particularly important for very large protected enclaves, encompassing large numbers of individuals; the more people within an enclave, the greater the probability that at least one of them might be a had actor.

Increasingly Complex World, **Expanding Security Concerns**

A number of points are worth emphasizing: Fifty years after ENIAC, the network has become the computer (paraphrasing the Sun Microsystems slogan "The Network Is the Computer").

In the future, cyberspace security and safety incidents in this networked environment will become much more prevalent; cyberspace security and safety incidents will impact almost every corner of society; and the consequences of cyberspace security and safety incidents could become much greater.

Local enclaves protected by firewalls appear promising as a basic cyberspace security paradigm, applicable to a wide range of security situations

We're all in this together; weak links in the net created by any of us (software developers, end users, network providers, etc.) increase the problem for all of us.

Much more attention must be paid to user motivation, for all classes of users, with different approaches required for each class. Inadequate user acceptance and utilization of security techniques and procedures has been the bane of most previous attempts at cyberspace security.

No one's in charge; the problem transcends all usual categories. The question of "roles and missions" is an important one, both philosophically (e.g., do we need more centralized control, or are there decentralized effective solutions) and pragmatically (what roles do we give DoD versus FBI versus CIA; UN versus U.S.; Interpol versus whom?).

The world has become much more complex. It is a useful complexity, but with this complexity has come security and safety problems that we are only beginning to understand and appreciate.

Acknowledgment

The authors thank their RAND colleagues Steven C. Bankes, Mark Gabriele, James J. Gil-

IEEE Technology and Society Magazine, Winter 1995/1996

logly, Anthony C. Hearn, and Willis H. Ware for numerous suggestions and insights that have contributed very significantly to the course of this research and to the results presented here.

The authors are indebted to Special Agent Jim Christy and his team at the Computer Crime Unit, Air Force Office of Special Investigations, Bolling Air Force Base; Supervisory Special Agent Harold Hendershot, Economic Crimes Unit, Federal Bureau of Investigation; Jack Lewis, Electronic Crimes Branch, Financial Crimes Division, U.S. Secret Service; Detective Inspector John Austen, Computer Crime Unit, Metropolitan Police, New Scotland Yard, London; and Harry Onderwater, Computer Crime Unit, National Criminal Intelligence Division, National Police Agency, The Netherlands, for sharing their perceptions of computer crime, its current perpetrators, and likely future trends.

The authors are also indebted for stimulating discussions to Michael Higgins, Defense Information Systems Agency; Professor Roger Needham and Ross Anderson, University of Cambridge Computer Laboratory, Cambridge, England; Dennis Jackson, JANET-CERT Coordinator, UKERNA, Chilton, England; Christoph Fischer, Director, Micro-BIT Virus Center/CERT, University of Karlsruhe, Germany; Professor Dr. Ulrich Sieber, Chair for Criminal Law, Criminal Procedural Law & Legal Philosophy, University of Würzburg, Germany; Klaus-Peter Kossakowski. Deutsches Forschungnetz Computer Emergency Response Team (DFN-CERT), University of Hamburg, Germany; Dr. Wietse Venema, Department of Mathematics and Computing Science, Eindhoven University of Technology, The Netherlands; and Dr. Giam piero E.G. Beroggi, Delft University of Technology, The Netherlands.

References

[1] P. Neumann, Computer Related Risks. Reading, MA: Addisonley. 1994.

[2] P.J. Denning, Computers Under Attack: Instuders, Worms, and K. Hafner and J. Markoff, Cyberpunk: Outlows and Hackers on

[5] I. C. Hande, and J. Askini, L. Corptani, C. Unitaris and Hackers on the Computer Frontier. New York, NY: Simon & Schuster, 1991. [4] P. Mungo and B. Clough, Approaching Zero: The Extraordinary Underworld of Hackers, Phrealers, Virus Writers, and Keyboard Criminalis. New York, NY: Random House, 1992. [5] P. Wallach, "Wire pirates," Sci. Amer., vol. 270, pp. 90-101, Mar. 104.

1994

1934. (6) Presentation by Air Force Computer Emergency Response Team (APCEPT). Kelly AFB, at Sixth Aan. Computer Security Ineident Handing Wickip, hosted by the Forum of Incident Response and Sourity Team (FRST). Boston, ML July 2529, 1934 and 11) R.E. Yates, "Hackers solid phone card numbers in \$30 million scam. Churger Jraho, pp. 1, 0, Nov. 2, 1934, (B)Data presented by Computer Emergency Response Team (CERT), Cameger Mellion University, at Stuth Ann. Computer Security Inci-dent Handling Wiship, hooted by the Forum of Incident Response dent Handling Wiship, hosted by the Forum of Incident Response.

can be dring Wishp, hosed by the Forum of Incident Response and Security Teams (FIRST), Boston, MA, July 25-29, 1994 – supplemented by CERT 1994 Aoa, Rep. web homepage (http://www.set.emu.edu/SEI/ programs/cert/1994_CERT_Summary html)



[9] S. Levy, Hackers, Heroes of the Computer Revolution. Anchor,

(1) S. Lety, neuror, arrest q in computer Arronnian, ARGO, 1984, 1097, Garana, Campure Ehicz, 2nd Ed. Englewood Cliffs, NJ. Prenice Hall, 1994, 1110 B. Hofman, "Responding to enrowing across the technological spectrum, TAANO Computer System: Evolution Content (TCSEC), 1010 (2000), 2000), 2000 (2000), 2000 (2000), 2000), 20000, 2000 (2000), 20000, 2000), 20000, 2000, 2000, 2000, 2000), 20000, 20000, 200

28

Simulation of Living Systems, R.A. Brooks and P. Maes, Eds. Cam-bridge, MA: M.I.T. Press, 1994, pp. 130-139 [16] W.R. Chewick and S.M. Bellovin, *Firewalls and Internet* Security: Repelling the Wily Hacker, Reading, MA: Addison-Wesley, 100.

1994

1994. 1713. Gurinket and G. Spatford. Proceed UNYX Security. Seba-topol. CA: O'Reilly & Associates. 1991. 1818 Proc. 17th Aux Comparet Security Conf., vols. 1 and 2, Nanonal Inst. of Standards and Technology/National Comparet Security Ce-re, Cet. 11-14. 1994. 119) M.R. Higgins. "Threas to DoD unclassified systems." DoD 1991, Nat. Higgins. Status and Security. Automated Systems Incr-ment Security Center for Information Systems Security, Functions and Services." Center for Information Systems Security, Editors Information Systems Agency, 1994

IEEE Technology and Society Magazine, Winter 1995/1996

Senate Permanent Subcommittee

EXHEBIT #_

7b

OFFICE OF INSPECTOR GENERAL OFFICE OF SECURITY OVERSIGHT

AUDIT OF UNCLASSIFIED MAINFRAME SYSTEMS SECURITY (U)

EXECUTIVE SUMMARY (U) 1

(U) Introduction. The Department's large "sensitive but unclassified" information processing network consists of nine administrative and consular systems running on five IBM mainframe processors at five locations. Those systems are under the authority of the Under Secretary for Management (M). Domestically, the Assistant Secretary for Administration's Deputy for Information Management (A/IM) manages the Foreign Affairs Data Processing Center (FADPC) operating dual information processing centers; one in the Main State Department building in Washington, D.C., and a second facility in Beltsville, Maryland. The Chief Financial Officer's Bureau of Finance and Management Policy (FMP) maintains single systems running on individual IBM mainframes at the Financial Service Centers (FSCs)² in Paris, Bangkok, and Mexico City. (The Mexico City FSC is in the process of relocating to Charleston, S.C.) These systems, which are networked worldwide, process various financial transactions worth approximately \$7.9 billion annually and support visa and passport operations which make an average of 25,000 name checks daily.

(U) Material internal control weaknesses have existed in the Department's mainframe computer operations for several years. The Department has reported these material weaknesses to the Office of Management and Budget (OMB) and the Congress in its annual Federal Mangers' Financial Integrity Act report. For example, Mainframe Security has been reported as a material internal control weakness since 1987. In addition, the Department of State's reports to the President and the Congress on its 1993 and 1994 reviews of management controls and financial management systems has designated four material internal control weaknesses to focus on as high risk areas. Each of these areas of high risk control weakness either support or are dependent on mainframe system processing:

- Information Management: Modernization, contingency planning, and mainframe security;
- The Department's financial and accounting systems;
- Worldwide disbursing and cashiering; and

¹ CLASSIFICATION: This four page Executive Summary is unclassified when removed from the report. (U)

² During the audit, the Chief Financial Officer (CFO) changed the designation of the three overseas mainframe data processing centers from Regional Administrative Management Center (RAMC) to Financial Service Center (FSC). (U)

Immigrant and non-immigrant visa fraud.

(U) Objectives. The purpose of this audit was to determine the status of security controls protecting the confidentiality, integrity and availability of unclassified information assets at the State Department's five mainframe data processing centers and to assess the adequacy of those controls. Therefore, we included an assessment of the status and adequacy of security management, risk assessment, systems integrity, access control software implementation, counterbalancing controls, physical and procedural controls, and contingency planning.

(U) Audit Results. The audit confirmed previous reporting by the Bureau of Diplomatic Security (DS), A/IM, other Office of Inspector General (OIG) entities, and various contractors. The Department cannot assure that its unclassified but sensitive information is protected from unauthorized and undetected access and manipulation of data. However, the audit went further by evaluating all of the Department's mainframe data processing centers in a consistent approach and assessing the systemic management problems. While some security efforts and features are actively protecting mainframe system assets, that security is not complete and there is no security plan. As a result, the Department is not in a position to reliably know if information has been compromised. The lack of senior Department management's involvement in addressing authority, responsibility, accountability and policy is the critical issue perpetuating the Department's lax approach to mainframe security reflected in this report's overall findings. More profoundly, the lack of clear management responsibility has resulted in incomplete and unreliable security administration lacking essentials such as clear authority to act on audit trail discrepancies, trained Information Systems Security Officers (ISSOs) and authoritative policy. Specifically:

- Responsibility and accountability for mainframe systems security is fragmented and vague. No one activity or official has been assigned or accepted responsibility for the security of mainframe system operations. (See page 9.)
- The Department does not have a security program to identify and reduce risks to its unclassified but sensitive mainframe computer network. Assessments have not been completed of the threats and risks to either the specific mainframe data processing centers or to the overall mainframe data network. (See page 19.)
- The Department cannot rely on its configuration management process to assure the integrity of its nine networked mainframe computer systems. The Department has not established the necessary change control processes to protect the mainframe operating and access systems from unauthorized access or alterations. (See page 27.)
- Implementation of Access Control Facility 2 (ACF2), the IBM security software selected by the Department to protect its mainframe systems, has not been completed and was not supported by approved procedures. (See page 34.)

-ii-SBU/NOFORN

- The Department cannot rely on the controls associated with the individual software applications to counterbalance weaknesses in system integrity and the operating system's access controls and to detect or prevent unauthorized use of information assets supported by the Department's mainframe systems. This is caused by a lack of nonsystem procedural controls, such as a lack of separation of duty and reliance on key personnel, and inadequate guidance, standards, and policies. In addition, no mainframe application has been certified as being fully secure, and only 1 of 77 application programs has received provisional security certification. (See page 45.)
- FSC Bangkok did not have adequate controls over physical access and protection of its mainframe data processing center. (See page 57.)
- An estimated 26,000 unclassified but sensitive tapes at the Department's domestic mainframe data processing centers are not adequately protected and controlled. (See page 62.)
- The Department's continuity of operations planning and disaster recovery plans are incomplete. Plans to reestablish any of the Department's mainframe data processing operations following a catastrophic system loss have not been fully developed or tested. (See page 64.)

POSITIVE INITIATIVES (U)

(U) Over the past year, the Under Secretary for Management and his staff have taken an interest in addressing and correcting deficiencies vetted by this audit. Management has initiated inter-bureau efforts to address some of the more significant problems. Work groups from the financial and information management bureaus have gone to FSCs Bangkok (June 1994) and Paris (March/April 1995) to establish control over the software security systems. In addition, the Under Secretary sponsored a November 1994 off-site which coordinated a series of decision meetings for his principal managers and their staff (Report Exhibit A). That effort had three significant results:

- The January 25, 1995, decision by the Under Secretary for Management's principal managers on who would assume responsibility for drafting a mainframe security policy and for addressing systems security vulnerabilities (Report Exhibit B).
- Development of and consensus on a policy directive, signed by the Under Secretary on February 1, 1995, which lends management support and assigns general responsibilities for the "Security of Automated Information Systems" (Report Exhibit C).
- Formation of an inter-bureau Automated Information Systems (AIS) Work Group to propose solutions to outstanding mainframe security issues.

(U) Benefits of the Audit. This report summarizes the major vulnerabilities which place the information assets supported by the Department's unclassified mainframe facilities at risk and impact executive management's reliance on information security. It identifies the executive level actions taken and those needed to be taken to address those vulnerabilities and to improve management reliance on protection for the confidentiality, reliability and availability of mainframe information assets.

(U) Summary of Recommendations. This report and its classified addendum make 21 unclassified recommendations and two classified recommendations. Those recommendations are to the Under Secretary for Management, the Designated Senior Official for Information Resources Management, the Assistant Secretary for Diplomatic Security, the Chief Financial Officer and the Deputy Assistant Secretary for Information Management. The recommendations address the need to establish authoritative policy:

- Identifying responsibilities and authorities for establishing a security program,
- Assessing the threats and risks to mainframe data processing centers,
- Establishing configuration management,
- Formalizing access controls,
- Certifying the security of applications,
- Reporting on the reliability of the systems of management controls,
- Physically protecting facilities and staff,
- Controlling data tapes, and
- Reporting on the reliability of contingency planning.

(U) Management Comments. The draft report was reviewed with management officials at an exit conference held with officials from M, DS, FMP, A and the Chief Information Officer (CIO) on July 25, 1995. Separate conferences were held with Bureau of Consular Affairs (CA) and Bureau of Personnel (M/DGP) officials on August 4 and August 8 respectively. Appropriate clarifications requested during that review were incorporated, and on August 25, 1995 the draft report was sent for their formal comments. Written comments were provided by M, A, DS, and FMP and are incorporated in this report as appendices. The Assistant Secretary for Administration found "the report accurate" and expressed the intention to take the recommended actions. Comments from M, DS, and FMP on specific recommendations are addressed following those recommendations and at the end of the Classified Addendum's findings.

> -iv-SBU/NOFORN

Senate Permanent Subcommittee

FIGHERT # 11

NASA 1995 INCIDENT SUMMARY REPORTS

Summary of Incidents 1995

Total = approximately \$280,000 - with some items still open and charging.

Incident # : 950001 Date Opened: 1/10/95 Status: closed 1/10/95 Impact: low - \$50

NASIRC received a report that an NEU.edu system had been compromised, and that NSIOPS was trying to determine if any NASA sites were involved. Upon further investigation, it was determined that NASA was merely the domain name server for the site, and was not compromised. Case closed.

Incident # : 950002 Date Opened: 1/11/95 Status: closed 1/25/95 Impact: low - \$5,100

The Dark 1801 virus was found at a NASA center. NASIRC researched it and found it to actually be the Dark Avenger virus, which is deadly to the data residing on the infected PC. The only fix is to run the McAfee scanner on that system, which will eradicate the virus, but the extended damage is that all data files will be lost. There were two PC's involved, and both had to be completely reformatted.

Incident # : 950003 Date Opened: 1/13/95 Status: closed 1/25/95 Impact: low - \$17,850

A NASA computer system located at a university site was found to have a sniffer running on it. The NASA system's root password was apparently grabbed by a sniffer running on a system at the University of Massachusetts. No files on the NASA system were damaged, and the system administrators at sites whose passwords may have been compromised were notified.

Incident # : 950004 Date Opened: 01/13/95 Status: Open Impact: high - \$61,500 at \$50/hour to restore and check systems. Plus additional NASIRC and OIG time.

NSIOPS reported that a NASA system may have been compromised. The system administrator was notified immediately. He backed up the entire system and then took it down. NASIRC staff went to the center the following Tuesday and confirmed that the hacker had fully penetrated the system and installed a trojaned telnet sniffer to gather user passwords. A number of hacker logs were captured, as were some hacker executables and source files in the directory path /usr/ucb/.cr. Further investigation of the hacker logs indicated the break-in originated from Harvard University. Contact with the Harvard system administrator resulted in Harvard identifying the , hacker. Harvard officials disabled his account but refused to provide any further information. The center security personnel have chosen to try to pursue prosecution. The center IG and Security Manager have asked that the IMPACT be adjusted to reflect an hourly rate of \$50 to restore and check all affected systems. The case is currently still open pending final word from the NASA IG regarding prosecution. This case is currently being reviewed by the NASA IG and the FBI for prosecution.

Incident # : 950005 linked to 950003 Date Opened: 1/23/95 Status: closed 2/6/95 Impact: low - \$250

A NASA center asked for NASIRC's help in investigating the sniffer reported in incident 960003. This incident was opened up before it was discovered to be related to 960003. NASIRC offered assistance to the system administrator at the university site that was not cooperating with the investigation, and was able to get a little more information from him. The center agreed to close the case.

Incident # : 950006 Date Opened: 1/24/95 Status: Open/Ctr E investigating- will be closed-not prosecuting Impact: High (don't have \$\$ yet- 15,000 phone calls made)

A NASA center PBX switch was hacked after there were some vender adjustments made to it. The security that had been installed, was never reinstalled after the vendor worked on it. Within a couple of days, the number had apparently been published on the Internet, and about 15,000 unauthorized long distance and international long distance calls had been recorded. NASIRC recently found out that the NASA IG is not going to prosecute this, and we will be closing this incident.

Incident # : 950007 Date Opened: 1/26/95 Status: closed 2/13/95 Impact: low - \$1,500

A NASA center was scanned by the University of Minnesota. When the university was contacted, they said that the system doing the attacking had just been hacked, and they were trying to clean it up. Although the university said that they had disabled an account for a user that had some hacker tools, the scan continued at the NASA site, forcing that site to block the university at the router level.

Incident # : 950008 Date Opened: 1/30/95 Status: closed 1/31/95 Impact: Iow - \$1,350

A system administrator at a NASA center called to report a possible IP spoofing attack. NASIRC visited the site, and found no evidence of an IP spoofing attack. NASIRC supplied the system administrator with some security tools to use on his system.

Incident # : 950009 Date Opened: 2/1/95 Status: Closed 3/8/95 Impact: Iow - \$4,150

A system at a NASA center (Sensitivity Level 2) which is the security firewall for the Ground Data System Uplink systems (also level 2) was found to have what appeared to be an electronic bulletin board system containing pirated software. The files were uploaded into the anonymous FTP area. From the name of the files and directories found, it appeared that the system contained pirated, copyrighted software belonging to Microsoft, Corp.

After discussions with the NASA IG. and Microsoft, the center concluded that no actual Microsoft software resided on the machine, only bootlegged game files. The center cleaned up the computer system affected and closed the incident.

Incident # : 950010 Date Opened: 2/13/95 Status: closed 2/13/95 Impact: low - \$100

A center reported the anti-EXE virus on one system. It was found and eradicated with Norton Antivirus.

Incident # : 950011 Date Opened: 2/16/95 Status: to be closed Impact: low - \$1,250

Information from a NASA center was sent to Austria, and was thought to be an illegal export of information. The IG has informed NASIRC that this case is not going to prosecution, and it will therefore be closed.

Incident # : 950012 Date Opened: 2/17/95 Status: closed 1/29/96 Impact: Low - \$1,840

A center system was penetrated from Stanford.edu. The hacker set up two accounts on the NASA system, one corresponding to his first name and one corresponding to his surname. The NASA system was taken off-line for clean-up. NASIRC received word from Stanford University that they were seeking FBI involvement in this incident. The system administrator for the compromised system discovered the identity of the hacker by looking at some old email files left on the system by the hacker. The hacker did not do any actual damage, he only installed PINE to beta test it.

Incident # : 950013

Date Opened: 2/22/95 Status: closed - 1/29/96 Impact: low - \$1960

A hacker bulletin board was installed on a NASA computer. NASIRC received and reviewed the system logs, discovering the possible presence of copyrighted software and pornographic images. NASIRC coordinated response actions with the C-ITSM and the Center IG to support possible prosecution. The bulletin board activity was shut down due to the high usage by unauthorized users, preventing legitimate users from accessing the ftp archives. It was determined that there was questionable pornography on the system by way of reviewing the .gif files, and the Center IG elected to present that information to the FBI. Since the identity of the "owner" could not be confirmed, the IG elected not to prosecute this case.

Incident # : 950014 Date Opened: 3/13/95 Status: closed 3/27/95 Impact: Low - \$2,100

Two NASA center machines were found on a sniffer log at vexcel.com. The two machines checked out okay, but it was discovered that nine others may have been sniffed. All of those systems subsequently checked out clean.

Incident # : 950015 Date Opened: 3/15/95 Status: closed 4/20/95 Impact: Low - \$550

A large number of login failures to a Cisco router at a center was reported. The center system administrator had resigned his position, so NASIRC is actively working with another contact at the center to collect further information. The unsuccessful login failures occurred twice in a period of 1 week. NASIRC suggested installing a firewall-type machine in front of the router with a TCPwrappers to log the attempts.

Incident # : 950016 Date Opened: 3/20/95 Status: 4/7/95 Impact: low - \$250

An hacker bulletin board was found to be running on a NASA system, in the anonymous ftp account. NASIRC spoke with the center IG, and due to the lack of a clear trail as to who was involved, he said to go ahead and close this. The system was cleaned up.

Incident # : 950017 Date Opened: 3/20/95 Status: closed 4/24/95 Impact: Low - \$700

A system was sniffed from Jonns Hopkins University. The system was checked

and determined to be clean.

Incident # : 950018 Date Opened: 1/31/95 Status: closed - 3/21/95 Impact: Low - \$2,500

There was a false instance of the "DA BOYS" virus noticed. It was missing the "installer" portion. It was analyzed and determined not to be a true threat.

Some weeks later the actual "DA BOYS" virus did infect a NASA center machine and propagated around the center. It was then contained and cleaned up.

Incident # : 950020 Date Opened: 4/10/95 Status: closed 4/18/95 Impact: Iow - \$350

A nacker bulletin board was discovered at a NASA center, and the intruder had apparently gained root access. The system was taken off-line, cleaned up, and the incoming ftp area was set to write-only. TcpWrappers were installed.

Incident # : 950021 Date Opened: 4/6/95 Status: closed 4/11/95 Impact: Iow - \$300

NASIRC received notification that a sniffer at Lawrence Berkeley Labs has grabbed a password for a system at a NASA center. The center was notified, and the user was told to change the password. The system subsequently checked out clean.

Incident # : 950022 Date Opened: 4/11/95 Status: closed 4/12/95 Impact: Iow - \$100

Several failed attempts to log into a NASA center computer as "test" and "guest" were recorded. The offending site would not reply to our queries, but no more occurrences were subsequently reported.

Incident # : 950023 Date Opened: 4/1/95 Status: closed 5/10/95 Impact: low - \$100

A report was received from Auscert that a NASA system had run through a sniffer. The system is an open system, and the password was public knowledge, so no damage was suffered.

Incident # : 950024 Date Opened: 4/11/95 Status: Closed 4/25/95 Impact: low - \$300

A report came in from columbia.edu that 2 NASA machines had passwords sniffed for one user on each. Both the users and ITS managers were notified, and the password was changed at one site-the other site was an unpassworded account. NASIRC supplied information to help the administrators better secure the unpassworded account.

Incident # : 950025 Date Opened: 4/19/95 Status: closed 4/24/95 Impact: Iow - \$550

A password was sniffed at a center from ann.ee.uh.edu (Univ. of Houston). It appears that the account sniffed was the anonymous ftp account, and was therefore still secure. The system checked out clean.

Incident # : 950026 Opened: 4/19/95 Status: closed 5/11/95 Impact: Iow - \$450

An email probe was reported from a NASA center, that apparently came from NCSA. NASIRC contacted NCSA, and also contacted the sender, but was unable to accurately determine the origin. The sender denied ever sending the message, and speculated that he had been email spoofed. While this is a possibility, the sender was running a racey web page, and sounded as though he might be affiliated with hacker-types. No more messages were received.

Incident # : 950027 Opened: 4/20/95 Status: closed - 5/10/95 Impact: low - \$350

The password was sniffed on a NASA center system from hut4.pha.jhu.edu, and then the account was broken into. The intruder appeared to be looking for classified and secret files, but there weren't any, so he logged out. The password was apparently grabbed when a NASA user logged into his account from his JHU account. The passwords have been changed, and the system checked out clean.

Incident # : 950028 Opened: 4/24/95 Status: closed 5/26/95 Impact: Iow - \$100

A report came in from NSIOPS that a NASA center system was being used to access an unadvertised web site. This turned out to be a case of employee misuse, and was handled internally by the contractor's company. It was recommended that the user have his internet access revoked, since he doesn't need it to perform his job.

Incident # : 950029 Date Opened: 5/3/95 Status: closed 7/13/95 Impact: low - \$625

A NASA system administrator reported that an intruder managed to telnet in from panda.uiowa.edu as root. Upon further inspection, it was discovered that the system had been misconfigured for the DECNET/TCP/IP gateway. This was then used to start a connection from an unregistered DECNET host that passed through panda.uiowa.edu. The system was apparently uncompromised, and the gateway was subsequently disabled.

Incident # : 950030 Date Opened: 5/3/95 Status: closed 5/8/95 Impact: low - \$150

A NASA system administrator reported a scanning attack picked up by Gabriel software from another system at the same site. NASIRC checked with the contractor doing development work on the offending NASA system to see if they were doing anything that might be causing this. They were not, but the attacks did not continue.

Incident # : 950031 Date Opened: 5/3/95 Status: closed 8/10/95 Impact: low - \$6500

A sniffer was found running at Stanford.edu with the logged file having been found on kudu.ru.ac.za (South Africa). From this sniffer file, some NASA systems had their user names and passwords sniffed. NASIRC notified all centers that were passed on to them from the logs to change their passwords and secure their machines. The intruders apparently came from several different sites, tracing back to South Africa and to the East Coast. The most systematic attacks were against Stanford, RIACS and NASA. Passwords on NASA systems were subsequently changed, and the systems were checked and cleaned up, where necessary.

Incident # : 950032 Date Opened: 5/5/95 Status: Closed 5/4/95 Impact: Iow - \$300

The virus, NYB, was reported at a NASA center. It was discovered on a floppy disk using McAfee, but was eradicated using Norton Utilities.

Incident # : 950033 Date Opened: 5/10/95 Status: Closed 5/15/95 Impact: Iow - \$400

The Anti-EXE virus was reported on 7 systems at a NASA center, apparently having been spread by an infected floppy. It was removed with F-prot.

Incident # : 950034 Date Opened: 5/17/95 Status: Closed 7/25/95 Impact: Low - \$2150

A sniffer found to be running at hpc.org sniffed machines at several centers. NASIRC received this notice from CERT, and all system administrators for the sniffed machines were subsequently notified by NASIRC to secure their machines and to have all passwords changed. This covered several centers. Accounts appeared to have been sniffed, but not compromised.

Incident # : 950035 Date Opened: 5/25/95 Status: Closed 5/25/95 Impact: Iow - \$100

A NASA system was reported to be pinging some cmich.edu systems (15000 attempts). The attacker turned out to be an employee who was previously a student at that site, and found that his account was disabled. He was fingering sites to find some of his friends to get his account reactiviated. He was told to stop this activity.

Incident # : 950036 Date Opened: 6/6/95 Status: Closed 6/12/95 Impact: Low - \$1150

A Center system administrator reported a possible system penetration. The NASA system logs contained 2 logins as root from virgo.acc.iit.edu and tcpgate.advantis.com. NASIRC provided assistance to review and analyze the system logs. Although the system administrator's log had shown the 2 logins, no trace remained of any out-of-the-crdinary activity.

This was further complicated by the system administrator's choice to announce that an intruder was suspected to be on the system, and that system monitoring might be taking place in the login banner. NASIRC felt that this probably warned the intruder sufficiently to cover his/her tracks and exit the machine. NASIRC provided software to monitor the system (a modified version for their Ultrix machine), but the system administrator was unable to compile it. No intruders or modified files were found and the case was closed.

Incident # : 950037 Date Opened: 6/16/95 Status: closed 7/10/95 Impact: Low - \$2400

A NASA system was penetrated from an intruder at netcom20.netcom.com. This seemed to result from a previously unexploited, but known vulnerability in sendmail. The account that was penetrated belonged to a graduate student at Arizona State University. Both netcom20 and Arizona State were temporarily disellowed access to the NASA center systemCenter C system by the system administrator. It was suspected that the initial access was provided by the account being sniffed from Arizona State. NASIRC notified Arizona State that they might have sniffers running on their machines.

Incident # : 950038 Date Opened: 6/26/95 Status: closed 7/25/95 Impact: Low - \$1300

A NASA system was penetrated from lida.lbl.gov, through a system located at llnl.gov. The NASA system was running an old version of Sendmail, which may have provided easy access for the intruder. The intruder then installed a fake "root" account on this machine. The Sendmail was upgraded, and the user passwords were changed, and the machine cleaned up. NASIRC assisted Center personnel in analyzing this penetration and coordinated communication with the external organizations.

Incident # : 950039 Date Opened: 6/26/95 Status: closed 6/26/95 Impact: Low - \$3150

A number of microcomputers located at a NASA center were infected with the Cascade virus. The virus was detected by vshield. This virus causes all the characters on the screen to fall into a pile at the bottom of the screen. It executes when a user logs into a Novell Netware file server to obtain his email. The virus was most likely loaded into the system via an infected floppy, or by downloading software from an Internet site and not scanning for viruses. A total of 13 systems were infected, but more than 70 had to be checked. The virus was isolated and was eradicated from the infected systems.

Incident # : 950040 Date Opened: 7/7/95 Status: closed 7/11/95 Impact: Iow - \$350

A NASA center reported finding the Anti-CMOS virus on 5 PCs. This was detected and eradicated using antiviral software. If the software had been run on the disk prior to loading, the spread would have been limited to one machine, or prevented altogether. On two of the five machines the virus was easily eradicated with software. The other 3 had to have the operating systems reloaded.

Incident # : 950041 Date Opened: 7/10/95 Status: closed 8/30/95 Impact: low - \$300

A center reported constant unauthorized login attempts from trader.com. The NASA system was running with C2 level security active and successfully challenged and rejected all of the trader.com attempts. Trader.com said that they found the culprit, and that they would ask him to stop.

Incident # : 950042 Date Opened: 7/11/95 Status: closed 7/20/95 Impact: low - \$850

A NASA center reported that one of their systems was broken into from a site in

Germany. NASIRC enlisted the help of DFN-CERT to identify the system administrator of the german machine. Once that information was obtained, NASIRC contacted the system administrator to clear up the situation. He said that his logs did not have any information for the time period in question, and that his computer resided in a medical facility, where the users had very limited skills. It is possible that the address was spoofed, but in any case, the information was dt a dead end, and the case was closed after the NASA system was cleaned up.

Incident # : 950043 Date Opened: 7/13/95 Status: closed 10/11/95 Impact: Iow - \$350

A center reported that a site in the UK had tried to access several of their computers, and succeeded in getting into one. The center tried to contact the postmaster of the probing machine, but got no response. NASIRC contacted the postmaster and got him to agree to check the log entries for the time in question. He reported back that he had no record of the attempts, but that he would see if he could get the phone records pertaining to the time period. He was unsuccessful, and the center agreed to close the incident.

Incident # : 950044 Date Opened: 7/13/95 Status: open Impact: medium - currently at \$31,000 + IG time (estimated at \$9000+, and NSIOPS and other centers time, estimated at \$2500+)

A NASA center reported probing taking place against several systems, coming from fas.harvard.edu. Notice was then received from the Navy that several NASA systems had been attacked and possibly penetrated. A sniffer was found on one of the penetrated systems. This incident relates directly to 950004 and 950045, and other offending sites included mit.edu and umass. The FBI is currently investigating and seeking prosecution.

Incident # : 950045 Date Opened: 7/18/95 Status: closed 8/28/95 Impact: Iow - \$1000

A center reported that sarin.seritel.it scanned a range of IP addresses at the center on 2 different dates. NASIRC contacted the system administrator at sarin to determine who had done this, and what they may have wanted. The sys admin reported that their machine had been hacked from finchley.media.mit.edu, but they didn't know what user was responsible. The machines at the NASA center were not penetrated. Scans were also seen from fas.harvard.edu and chewie.wookie.net, and from master.towson.edu.

Incident #: 950046 Date Opened: 8/9/95 Status: closed 8/25/95 Impact: Iow - \$100

The MBDF virus was found on 3 Macintosh systems at a center. It was

detected with Central Point virus checking software, and does not cause permanent damage according to the information available on that virus.

Incident # : 950047 Date Opened: 8/11/95 Status: closed 11/30/95 Impact: low - \$50

A center reported sequential pinging attacks to public and non-public IP addresses from 192.48.154.51. The attack site appears to be an SGI site. Repeated attempts to follow-up with the center have yielded no further information, so NASIRC elected to close this case.

Incident # : 950048 Date Opened: 8/17/95 Status: closed 10/2/95 Impact: Iow - \$2500

A NASA center reported a password file being mailed to an iup.edu site from their system. The file went to theubab@avocet.ma.iup.edu. There is a possibility that the hacked machine did not have all of it's up-to -date patches installed. The machine was taken off-line for clean-up and investigation. A subsequent attempt by the hackers to telnet to the NASA machine was not successful. The university was cooperative in trying to contain and identify the hacker.

Incident # : 950049 Date Opened: 8/24/95 Status: closed 10/12/95 Impact: low - \$1400

An affiliate of a NASA center reported that a machine was broken into from gandalf.rutgers.edu and from er6.rutgers.edu. There was apparently a bug in sendmail that was exploited. The machine had several files corrupted, including the password file. All users were instructed to change passwords, and connections to trusted machines were discontinued during the cleanup effort, as well as the users on the trusted machines being asked to change passwords. Rutgers feels they may have figured out who the culprit is, but won't give NASIRC that information. They have, however, disabled that person's accounts on all machines, and the activity should have stopped. The center affiliate had disabled all connections from Rutgers.edu as best they could, but the router is controlled by another organization, and they can't be forced to block IP addresses.

Incident # : 950050 Date Opened: 9/5/95 Status: Closed 9/5/95 Impact: Iow - \$200

This WinWord.concept virus was spotted and eradicated at 2 NASA centers. Apparently one center gave it to the other. The WVFIX.ZIP file was used to fix the infected systems.

Incident # : 950051

Date Opened: 9/5/95 Status: Closed 9/5/95 Impact: low - \$150

The WinWord.concept virus was spotted and eradicated at a NASA center. The center used a "workaround" patch to fix the system.

Incident # : 950052 Date Opened: 10/6/95 Status: closed 10/31/95 Impact: Iow - \$3500

A center had a system penetration as root from several sites. This was noticed when the system crashed unexpectedly, causing the system administrator to investigate. The intruder was apparently trying to compile some C code that caused the system to crash. NASIRC was able to reach several of the sites, some of which were internet providers who identified the person and disabled him. Due to the lack of serious damage caused by the intruder, the IG has not opted to obtain court orders to gain the person's identity.

Incident # : 950053 Date Opened: 10/16/95 Status: closed 10/31/95 Impact: low - \$150

A center reported the ms-word macro virus at a contractor site (supporting that center). Two machines were involved and Scanprot.cot was used to clean the machines.

Incident # : 950054 Date Opened: 10/6/95 Status: closed 10/16/95 Impact: low - \$3350

A center reported 3 machines hacked from another machine on that center. The offending machine appeared to be hacked from oydport7.elron.net (Isreal). All four machines were cleaned up, and the attacking system had the operating system reinstalled and upgraded. The Isreali site was contacted, but they said that their machine had very little logging capabilities and were unable to match up a user. They said that they did close an account that they found had suspicious activity. NASA system administrators could not datermined the method used by the intruder to gain entry.

Incident # : 950055 Date Opened: 10/12/95 Status: closed 10/12/95 Impact: Iow - \$450

A user at a center reported that he was unable to riogin to the server. Upon inspection, it was found that the root password had been modified, and a new account had been added. Further reseach indicated that an employee who was making modifications to another machine, and had several windows on his terminal opened, accidentally made the modifications to this machine. The system administrator for the system cleaned up the modifications, changed the root password, and restricted the trusted hosts to only those he is in charge of, and checked for null passwords.

Incident # : 950056 Date Opened: 10/16/95 Status: closed 10/26/95 Impact: low - \$2500

A center reported that their machine was broken into from CWRU. Apparently the user resided at CWRU and at the NASA, and his password was sniffed at CWRU and used to gain access to the NASA system. NASIRC suggested using Skey as an added security precaution for the user at CWRU. There was also another computer compromised from CWRU. The first compromised system was also used to try to get the password file from a third system at the center, but was unsuccessful. 15 machines also had to be checked out because they were listed in the .rhosts file.

Incident # : 950057 Date Opened: 10/12/95 Status: closed 10/31/95 Impact: low - \$6300

A center computer was penetrated from oydport11.elron.net, an Isreali Internet provider. From the logs, we were unable to determine how the intruder got access to the system, but the password could have been sniffed or an NFS hole may have been exploited. The intruder was noticed during a period of "odd" ftp and web activity. The system was switched over from SunOS to Solaris 2.4, with all of the available patches installed, and a topwrapper.

Incident # : 950058 Date Opened: 10/20/95 Status: open Impact: high - \$45,000 + (does not include 18000 hours of computer down-time, usually calculated at \$50/hour = \$900,000)

A center reported a compromised machine that turned out to have a sniffer running on it, and a large sniffer log. Upon further inspection, the entire rib appeared to have been sniffed, and sniffers/logs resided on at least 6 machines. The rib was temporarily disconnected from the Internet, as the hackers repeatedly tried to reaccess. Once the rib was back online, and after a period of 1 week, a packet monitor was installed on the originally hacked system, in the hopes that the hacker(s) would return. The hackers did not return. The investigation is not yet closed per the IG's office.

Incident #: 950059 Date Opened: 11/1/95 Status: Closed 11/9/95 Impact: Iow - \$3600

A center reported that one of their systems had been penetrated. Further inspection turned up a sniffer and a trojanned login. Several systems within that center had passwords grabbed, and a few outside the center were grabbed as well. All were notified. The original system was loosely configured and did not have the most current operating system installed. It can't be upgraded, due to the fact that the project software is tightly integrated into the existing operating system. Plans to secure it include moving it to it's own LAN and taking it off the Internet.

Incident # : 950060 Date Opened: 11/9/95 Status: closed 11/20/95 Impact: low - \$350

Probes to a center system from std.cpc.ku.ac.th and ems.mut.ac.th were recorded. NASIRC had contacted someone at both sites, but never received a response. A backfinger indicated that these were students, possibly in a class at the time. The coordinators for the sites in question were notified, and they said they would see what they could do. This activity occurred again in January, right about when a new semester would start. NASIRC was again unable to reach anyone at the site to research this.

Incident # : 950061 Date Opened: 11/9/95 Status: closed 12/4/95 Impact: Iow - \$150

A report came in from one NASA center that an employee at another center was using his computer to conduct Internet Relay Chat sessions where he was asking for pornographic material. This was forwarded to the Center ITS manager for review and instruction. The system involved turned out to be in an open area, with many people having access. It was not possible to determine the exact user, so a memo to the group regarding this type of activity was to be distributed.

Incident #: 950062 Date Opened: 11/9/95 Status: closed 12/9/95 Impact: low - \$150

A center reported a scanning of one of their systems from core.exp.interop.net. Apparently when the scanning was noticed, the user fingered the machine and noticed that root was logged in from Italy. He then started up a talk session with them. NASIRC contacted the coordinator, jim@interop.net, but got no response.

Incident # : 950063 Date Opened: 11/14/95 Status: Closed 11/14/95 Impact: Iow - \$20,775

Function/Sensitivity level of compromised machines: 5 at level 0, 8 at level 2 (benefits and compensation, and salary data), one of the eight being a Novell Netware Server.

A center reported 13 PC systems infected with the Three Tunes virus. This virus is capable of infecting the .exe, .com, .vsd, .dll and various

software application files. It is also self-encrypting, making detection more difficult. The center was able to detect it using Viruscan V2.2.54.

Incident # : 950064 Date Opened: 11/14/95 Status: Closed 11/14/95 Impact: Iow - \$2050

A center reported a system penetration with root access, and a sniffer installed. The system was rebooted, however, before any sniffer information was logged, due to a hardware problem. The penetration came from nntp.vassar. edu., and gained entry via a known hole in Sendmail. They gained root by exploiting a hole in the loadmodule program. All passwords were changed and the sendmail service was removed.

Incident #: 950065 Date Opened: 11/27/95 Status: closed 11/29/95 Impact: low - \$150

The SMEG virus reported at a NASA center. It was found on a PC running Windows NT using McAfea, but McAfee could not eradicate it. Microsoft recommended rebooting the system from a clean floppy with DOS and the DOS-based anti-virus application be executed. This appeared to work.

Incident #: 950066 Date Opened: 11/27/95 Status: closed 1/29/96 Impact: low - \$200

A center received an email threat from a captive account (open for outside users). The threat indicated that it might be from the Uni-bomber, but the general feeling is that it is not authentic due to several factors, including the misspelling of "uni-bomber", the brevity of the message, and the idea that the uni-bomber has not yet been known to use email as a communication tool. This was referred to the FBI, and is closed at the center level.

Incident # : 950067 Date Opened: 11/29/95 Status: closed 12/4/95 Impact: low - \$100

A center experienced an intrusion from bermuda.io.com and eos.kub.nl to a Mac system, and 1.5MB were uploaded to that machine. Further research indicated that the system was not compromised, but that the user had accessed the bermuda.io.com site and had grabbed a file, unaware that it was listed as a hostile sites.

Incident # : 950068 Date Opened: 12/1/95 Status: closed 12/1/95 Impact: low - \$150 been hacked, and suspected 2 machines at a NASA center may have had a root compromise. The 2 machines were found to be clean and uncompromised, leading the ITS Manager to consider that he had been IP spoofed. 2 other centers also had systems that ran through sniffer related to the temple sniffer, but those systems checked out clean (that sniffer apparently was related to PSU as well.)

Incident #: 950074 Opened : 12/18/95 Status : closed 12/29/95 Impact : low - \$3250

A center reported a compromised machine-all log information that would lead to identifying the attacking site was wiped out, as the hacker had gained root access. NASIRC helped the user research the intrusion and provided information to aid the user in setting up a more secure environment for the operating system.

Incident #: 950075 Opened : 12/18/95 Status : closed 1/23/96 Impact : low - \$3000

A center reported a compromised machine-all log information that would lead to identifying the attacking site was wiped out, and the hacker had gained root access. NASIRC helped the user research the intrusion, but was unable to determine if there was an actual intrusion, or if there were just some messed up files.

Incident #: 950076 Opened : 12/18/95 Status : closed 12/18/95 Impact :low - \$100

A center reported that they had a range of machines scanned from biris.chem.lsu.edu. LSU is checking things out on their end, and the center didn't find any penetrated systems.

Incident #: 950077 Opened : 12/18/95 Status : closed 1/16/96 Impact : low - \$100

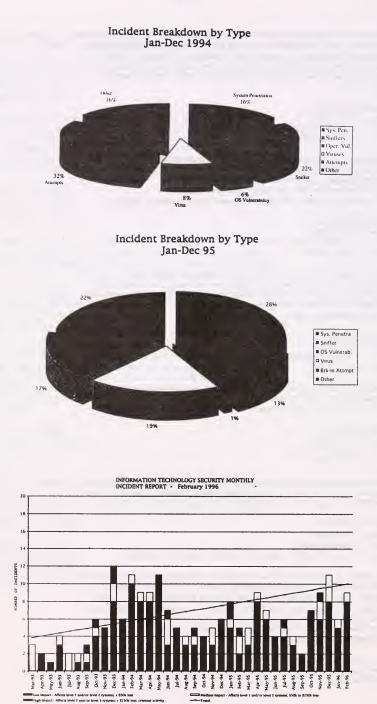
A NASA center system was reported to be fingering and attempting to telnet to nps.navy.mil. It turned out to be a Navy person who was granted an account on the NASA system who was fingering his own system at the .mil site.

Incident #: 950078 Opened : 12/21/95 Status : closed 2/9/96 Impact : low - \$10,670 + (security personnel's time not included)

Four systems at a NASA center were penetrated, possibly using an unpassworded LP account provided with IRIX operating systems. The intruder modified password files, and set up several user accounts for him/herself on various machines. The first 3 machines had a shared home user directory, and were accessed from biris.chem.lsu.edu, baasgi.cs.columbia.edu, and from several aol.com sites. NASIRC issued an alert on this vulnerability. The machines were cleaned up by center personnel.

*****Other reported items*******

Centers reported viruses that cost approximately \$10,000 in clean-up effort, at \$30/hour.



Central Intelligence Agency



wan D.C. 205(15

Senate Permanent Subcommittee en Investigations

EXHIBIT # 19

27 June 1996 rovd. 7181%

The Honorable Sam Nunn United States Senate Washington, D.C. 20510

Dear Senator Nunn:

During yesterday's hearing on foreign information warfare capabilities you asked a rather indelicate question: "What does 'cyber' mean, anyway?" I must admit that your query caused a great deal of discomfort here. While everyone had used the term, no one had heretofore felt any need to know precisely what it meant. In light of my promise to keep Congress fully and currently informed, I pressed for an answer.

Central Intelligence Agency's (CTA) research revealed that the term "cybernetics" was coined by the Father of Cybernetics, Norbert Wiener, in 1948. In Mr. Wiener's words, "We have decided to call the entire field of control and communication theory, whether in the machine or the animal, by the name cybernetics, which we form from the Greek kybernetes or 'steersman'."

• Department of State concurred with CIA's findings, but wished to point out that the Greek kybernetes is related to the Latin gubernator, meaning "steersman" or "governor."

The Defense Intelligence Agency is not yet ready to make a judgment, and is exploring the possibility that "cyber" may have come from the Greek Kybisteter or "diver," from which we also derive the word "cybister" or "a genus of large diving beetles."

I hope this clears up any confusion.

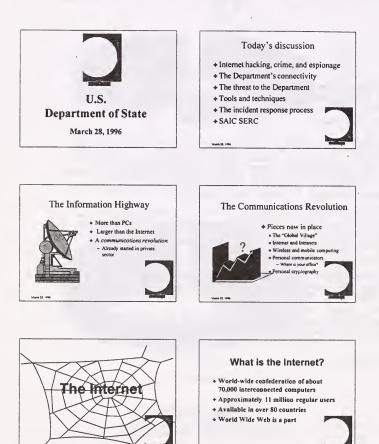
Sincerely, John Deutch Director of Central Intelligence

* nit

Senate Permanent Subcommittee en Investigations

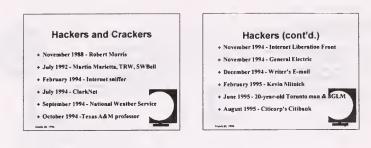
1

EXHIBIT # _____ 20

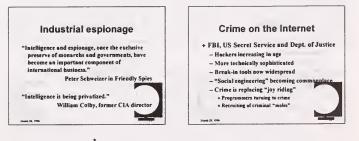


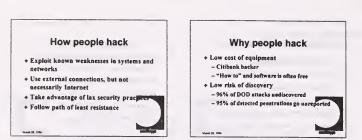
March 28, 1998

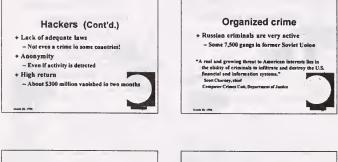


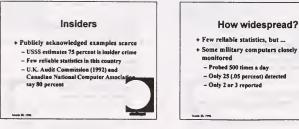














DEPARTMENT OF THE AIR FORCE OFFICE OF THE CHIEF OF STAFF UNITED STATES AIR FORCE WASHINGTON DC 20330 Senate Parmanent Subcommittee on Investigations

EXHIBIT # ____24

16 July 1996

HQ USAF/CC 1670 Air Force Pentagon Washington, DC 20330-1670

Honorable Sam Nunn Ranking Minority Leader Permanent Subcommittee on Investigations United States Senate Washington, D.C. 20510-6250

mator Nunn Dear

I appreciate your providing me a copy of the Senate staff report on Security in Cyberspace. I was interested to note that the report's findings are consistent with the results of previous Air Force vulnerability assessments.

As we have discussed, the Air Force is very concerned about the vulnerabilities associated with interconnected computer systems in today's hi-tech environment. In fact, protection of our data systems from unauthorized intrusions and other Information Warfare (IW) techniques is one of our highest priorities. Therefore, we are implementing several programs to address these threats.

The IW Technology Demonstration you recenity observed here in the Pentagon highlighted some of our efforts to protect the Air Force Base Information Infrastructure. Our Combat Information Transport System (CITS) program is funded to provide network management and information protection at 108 different installations by FY01. The CITS program provides a single focal point, the Base Network Control Center (BNCC), to manage and protect information for our fixed forces. All Air Force information systems, including combat operations, supply, logistics, and intelligence, will eventually migrate to the BNCC and be afforded the efficiency of single point network management and protection.

The Theater Deployable Communications program will carry our concept of single point management and protection of computer networks to our tactically deployed forces. One of the key roles of our new information warfare squadron is to be ready to rapidly deploy overseas to defend vital Air Force information systems in the event of a crisis or conflict. The squadron will work with both fixed and deployed network management activities to assist in the protection of our information systems and data bases.

The Air Force has already implemented a number of initiatives to train large numbers of our people on defensive IW, to deal effectively with unauthorized intrusions, and to standardize log-on banners on our systems to support prosecution of unauthorized intruders. We are continuing to evaluate the vulnerability of our service information infrastructure. We are assessing the potential threat posed by imbedded information processing components in our weapon systems. And we are working with the Office of the Secretary of Defense (OSD) to develop department-wide concepts for information system policies and procedures, for emergency responses to intruders, and for tailored responses to incidents.

I applaud your efforts to highlight the challenges we face in safeguarding the information systems that our nation has become so dependent upon. The Air Force will continue to work closely with the other services, Congress, and OSD to provide the maximum protection possible for our weapon systems and integrated information collection, processing, and communication systems. Your efforts in this area will help drive the formulation of a comprehensive strategy to protect Department of Defense and commercial systems. I look forward to continuing our dialogue on efforts to examine and improve the security of America's national information infrastructure.

RONALD R. FOGLEMAN

RONALL R. FOGLEMAN General, USAF Chief of Staff

As you know we ART working THIS HARD .- BUT HAVE A LONG WAY TO GO. THANK AGAIN FOR COMING TO SOTE OUR Bispay. R

Senate Permanent Subcommittee on Investigations

EXHIBIT # 25

SUPPLEMENTAL QUESTIONS FOR THE RECORD

HONORABLE JOHN P. WHITE DEPUTY SECRETARY DEPARTMENT OF DEFENSE

HEARINGS ON

SECURITY IN CYBERSPACE JULY 16, 1996

Question from Senator Nunn: "Could both of you address or either of you address when we will have a formal threat assessment in response to the Kyl Amendment to, I believe it was, the Authorization Act last year?"

A: During his testimony before the committee on June 25, Dr. John Deutch, the Director, Central Intelligence, stated that he has a major effort underway to bring together all parts of the community involved in security and intelligence to produce a National Intelligence Estimate on this subject. Dr. Deutch stated then that he expected the estimate to be completed by December of this year. We have confirmed with the National Intelligence Council that the assessment will be complete on December 1, 1996.

Senator Nunn: "Could you furnish for the record a general budgetary analysis of how much in the way of resources we are submitting to this area [protection of information systems], anything you can in an unclassified form -- and then if necessary, a classified section?"

A: I have asked the Defense Information Systems Agency and the C4I Integration Support Activity to compile the requested data and expect to provide it to your committee by September 30, 1996.

Senate Subcommittee on Governmental Affairs Permanent Subcommittee on Investigations

July 16, 1996

Subject: Security In Cyberspace

Question from Senator Nunn: "Could you furnish for the record a general budgetary analysis of how much in the way of resources we are submitting to this area [protection of information systems], anything you can in an unclassified form and then if necessary, a classified section?"

Answer: As requested by Mr. Dan Gelber, the resources depicted below constitute Information Systems Security Program Budget and Budget Estimate Submission resources (by appropriation) for the periods indicated The percentages displayed are rounded to the nearest whole percent.

						FY96-99
	FY 1996	<u>FY 1997</u>	<u>FY 1998</u>	FY 1999	TOTAL	CHANGE
Army						
RDT&E	3.455	3.161	9.681	3.843	20.140	+11%
Proc	10.647	10.678	21.221	24.163	66.709	+127%
0&M	16.500	17.300	25.403	24,626	83.829	+49%
MILPAY	3.000	3.324	3.200	3.269	12.793	+9%
TOTAL	33.602	34.463	59.505	55.901	183.471	+66%
Navy						
RDT&E	23.938	26.936	21.158	25.490	97.522	+6%
Proc	24.962	42 606	39.370	56.866	163.804	+128%
0&M	20.173	19.687	18.610	18.225	76.695	-10%
MILPAY	8.377	9.713	9.822	10.089	38.001	+20%
TOTAL	77.450	98.942	88.960	110.670	376.022	+43%

S in Millions

						FY 96-99
	FY 1996	<u>FY 1997</u>	FY 1998	FY 1999	TOTAL	CHANGE
Air Force						
RDT&E	10.388	6.900	10.219	8.623	36.130	-17%
Proc	52 260	42.640	39.682	42.819	177.401	-18%
0&M	27.306	34.812	45.294	56.045	163.457	+105%
MILPAY	6.066	7.405	9.282	9.951	32.704	+39%
TOTAL	96.020	91.757	104.477	117.438	409.692	+22%
<u>DIA</u>						
0&M	.271	.282	.301	.312	1.166	+15%
MILPAY	099	.100	.109	.110	.418	+11%
TOTAL	.370	.382	.410	.422	1.584	+14%
DISA						
RDT&E	0	0	0	0	0	0%
Proc	23.250	17.136	19.680	18.871	78.937	-19%
0&M	23.152	78.827	91.920	81.365	275.264	+251%
MILPAY	1.600	1.648	1.697	1.748	6.693	+9%
TOTAL	48.002	97.611	113.297	101.984	360.894	+112%
NSA						
RDT&E	211.640	239.155	228 564	227.248	906.607	+7%
Proc	27 459	21.231	20.720	29 620	99.030	+8%
0&M	221.031	225,427	228.364	235.832	910.654	+7%
MILPAY	18.768	19.297	19.297	19.297	76.659	+3%
TOTAL	478.898	505.110	496.945	511.997	1,992.950	+7%
Summary						
RDT&E	249.421	276.152	269.622	265.204	1.060.399	+6%
Proc	138.578	134.291	140.673	172.339	585.881	+24%
0&M	308,433	376.335	409.892	416 405	1,511.065	+35%
MILPAY	37.910	41.487	43.407	44.464	167.268	+17%
TOTAL	734.342	828.265	863.594	898.412	3,324.613	+22%

Senate Permanent Subcommittee en Investigations

EXHIBIT # 26

National Security Telecommunications Advisory Committee

September 18, 1996

Honorable Sam Nunn United States Senate Washington, DC 20515

Dear Senator Nunn:

On behalf of the President's National Security Telecommunications Advisory Committee (NSTAC) and its Industry Executive Subcommittee, thank you for this opportunity to contribute to the hearings on "Security in Cyberspace," which have brought much-needed attention to an issue the NSTAC considers extremely important -- information assurance. The NSTAC has defined information assurance, related to national security and emergency preparedness (NS/EP) telecommunications and information systems, as "protecting key public and private elements of the National Information Infrastructure (NII) from exploitation, degradation, and denial of service." The NSTAC shares your concerns and looks forward to continuing its relationship with the Government to ensure that the vision of an NII can be achieved while sustaining the robustness, reliability, and security of those information systems supporting our Nation's most critical infrastructures.

Over the years, the NSTAC has worked extensively with the Government to assess the security of the Public Switched Network. During that time, the NSTAC's focus has broadened as telecommunications and information systems have converged. More recently, it has examined the security of the NII and other critical national infrastructures that depend on information systems. The NSTAC principals emphasized their concerns about NII security in a March 20, 1995, letter to the President (See Enclosure 1, Appendix A). The Presidential response, dated July 7, 1995, asked that "the NSTAC's principals — with input from the full range of users of the NII -- to provide me with your assessment of national security emergency preparedness requirements for our rapidly evolving information environment" (See Enclosure 1, Appendix B). In addition to addressing these challenging issues, the NSTAC is examining a number of related NS/EP issues, including the implications of the Telecommunications Act of 1996 and the feasibility of establishing a private, nonprofit Information Systems Security

Enclosed you will find information highlighting NSTAC's history and endeavors to meet the challenges summarized above. If you require further information, please contact me at (703) 607-6101.

Sincerely,

lane D. Diane Fountaine

D. Diane Fountaine Chair Industry Executive Subcommittee

Enclosure: Information on the President's NSTAC

Information on the President's National Security Telecommunications Advisory Committee

Provided to

The U. S. Senate Committee on Governmental Affairs Permanent Subcommittee on Investigations

September 12, 1996

Enclosure 1

INTRODUCTION

The U.S. Senate Permanent Subcommittee on Investigations' recent hearings on "Security in Cyberspace," and the establishment of the President's Commission on Critical Infrastructure Protection and the Infrastructure Protection Task Force,¹ have brought muchneeded attention to an issue of national importance— information assurance.² It is evident from the testimony received thus far that the national defense and vitality of our national economy are closely tied to technology, especially communications and information technologies. Government and industry have leveraged and exploited leading-edge information technologies for competitive advantage, whether it be on the battlefield, in the corporate boardroom, in pursuit of new research and development opportunities in industry and academia, or in empowering citizens in their efforts to profit from the accessibility provided by the National Information Infrastructure (NII).

These benefits to the Nation, however, are not without costs. Entrance into the Information Age has resulted in a greater dependence on telecommunications and information systems than ever before, and the Nation's ability to protect those systems is the key to safeguarding both national security and socio-economic interests. This fact is made even more critical given the growing reliance of the Nation's infrastructures' on information systems. For these reasons, the security of the NII and, for that matter, the Global Information Infrastructure (GII) are of utmost national importance. The President's National Security Telecommunications Advisory Committee (NSTAC) commends the Subcommittee for holding these hearings and shares its desire to explore what private industry is doing to ensure that the vital services dependent on the NII and the information stored on it are afforded the appropriate level of protection. Furthermore, the NSTAC stands ready to advise the President, who has communicated his concerns regarding the security of the NII with the NSTAC directly,⁴ on information assurance matters and to leverage our considerable experience in this area to assist the President's Commission on Critical Infrastructure Protection and the Infrastructure Protection Task Force in their efforts to grapple with these complex issues.

²Defined by the NSTAC's Information Assurance Task Force as "protecting key public and private elements of the National Information Infrastructure from exploitation, degradation, and denial of service."

³E.O. 13010 identifies eight critical infrastructures: telecommunications, electric power, banking and financial services, oil and gas, water supply, transportation, emergency services, and continuity of government.

⁴Letter from President Clinton to the President's NSTAC dated July 7, 1995.

l

¹Both entities established by Executive Order (E.O.) 13010, Critical Infrastructure Protection, July 15, 1996.

BACKGROUND

This is the second time the NSTAC has been asked to provide testimony to Congress on security issues. On June 27, 1991, the chair of the NSTAC's Network Security Task Force (NSTF) testified before the U.S. House of Representatives Committee on Science, Space, and Technology, Subcommittee on Technology and Competitiveness, about the actions the NSTAC and the National Communications System (NCS) had taken in response to Government concerns about the potential disruption of national security and emergency preparedness (NS/EP) telecommunications' through network software manipulation. Since that time, the NSTAC and the NCS have addressed issues related to information systems security and, more recently, the NII. These experiences have increased both knowledge of, and concern about, the Nation's growing dependence on information systems. Over the years, the NSTAC has worked with the U.S. Government to address the security of the Public Switched Network (PSN) and more recently has turned to consider the security of other critical national infrastructures. Through the unique relationship fostered by the NSTAC process, the U.S. Government and the telecommunications industry have been able to derive significant value in terms of characterizing threats to and identifying vulnerabilities of telecommunications and information systems. By discussing these matters directly with senior officials from the Government and among industry representatives, the NSTAC provides a forum through which concerns about network security and information assurance may be addressed. Before discussing joint industry-Government efforts and activities, however, it may be helpful to provide some background information on the NSTAC and the NCS.

National Security Telecommunications Advisory Committee

Established by President Ronald Reagan in 1982 in anticipation of the divestiture of AT&T and the Federal Communications Commission's deregulation proceedings, the NSTAC is a high-level industry advisory group that provides advice to the President on NS/EP issues relating to telecommunications and information technology. Membership in NSTAC is limited to 30 presidentially appointed industry leaders who are senior executives (often chief executive officers) representing the major carriers, information system providers, manufacturers, electronics and aerospace firms, system integrators, and, more recently, the financial services industry. (See Appendix C for complete NSTAC principals list.) Over its 15 years, NSTAC has

⁵NS/EP telecommunications services are "the telecommunications services used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that does or could: cause injury or harm to the population; cause damage to or loss of property; or degrade or threaten the NS/EP posture of the United States." (National Communications System Manual 3-1-1, *Telecommunications Service Priority (TSP) System for National Security Emergency Preparedness Service User Manual*, National Communications System, July 9, 1990)

evolved to mirror the dynamic changes occurring in the telecommunications industry. As information systems have become more critical in the day-to-day operation of telecommunications and computing networks, for example, the NSTAC has broadened its focus to consider the potential NS/EP implications. In addition, and in keeping with the National Security Strategies articulated by Presidents Bush and Clinton, the NSTAC has considered the economic security dimensions of telecommunications and information system issues.

The 30 principals appoint executives from their respective firms to the Industry Executive Subcommittee (IES) of the NSTAC, which addresses issues on a continuing basis with NSTAC principals every 9 to 12 months. The IES members in turn call on subject matter experts from within their respective companies as required. Currently, the IES and its subordinate bodies are examining a number of issues, including network security, information assurance, the feasibility of establishing a private, nonprofit Information Systems Security Board (ISSB), and the NS/EP implications of the Telecommunications Act of 1996. In addition to participation in these subordinate groups, representatives from some of the NSTAC member companies work directly with officials from the U.S. Government in an operational, emergency response framework known as the National Coordinating Center (NCC) for Telecommunications. The NCC was formed "as an authoritative entity to coordinate initiation and restoration of NS/EP telecommunications services . . . [and] to provide the framework for the operating relationship between the telecommunications industry and the Federal Government in coordinating the initiation and restoration of NS/EP telecommunications services."6 It also "provides for the rapid exchange of information and expedites NS/EP telecommunications responses . . . [and] has the capability to support responses to a broad spectrum of emergency or crisis situations."7

National Communications System

The Manager, NCS, serves as the designated Federal official for the NSTAC under the Federal Advisory Committee Act. Through the NCS, the NSTAC coordinates its activities with the Federal Government. An interagency group created in 1963 initially to address the results of communications failures during the Cuban missile crisis, the NCS was rechartered in 1984 to plan and coordinate NS/EP telecommunications supporting recovery from any crisis or disaster. Its membership consists of 23 Federal departments and agencies, including the Department of Defense (DoD) and agencies from the intelligence community as well as civil government agencies such as the Departments of Commerce, Energy, Transportation, Treasury, the Federal Communications Commission, and the Federal Reserve Board. The Office of the Manager, NCS (OMNCS) provides the means for joint industry-Government planning through the

7Ibid.

⁶National Coordinating Center Operating Charter, National Communications System, October 9, 1985.

executive support of the NCS members and the President's NSTAC. The OMNCS includes the NCC which is a joint industry-Government operations center for coordinating the provisioning and restoration of telecommunications services during natural disasters and military operations.

GOVERNMENT/NSTAC NETWORK SECURITY ACTIVITIES

The NSTAC first addressed network security issues in 1990 in response to a request from the Manager, NCS. The Manager had been asked by the National Security Council (NSC) to determine what actions were needed from Government and industry to ensure the availability of NS/EP telecommunications considering the vulnerabilities of telecommunications to the "hacker" threat. In response, the NSTAC established the Network Security Task Force (NSTF) to study the threats and vulnerabilities of the Public Switched Network to intrusions into information systems that support its operations. This remains crucial because the PSN provides the backbone for the Nation's telecommunications and data transmission services, including services provided by the Internet and the NII. In its deliberations, the task force addressed three key issues:

- Establishing a mechanism for exchanging network security information among telecommunications service providers and between the telecommunications industry and the Government
- Network security research and development (R&D) for commercially applicable products
- Network security standards.

Joint Industry-Government Network Security Information Exchanges

The centerpiece of the joint industry-Government network security activities has been the Network Security Information Exchange (NSIE) process. The NSTAC and Government NSIEs are separate but closely coordinated bodies established to provide a working forum to identify issues involving penetration or manipulation of software and databases affecting NS/EP telecommunications. The NSTAC and the Government NSIEs each have their own process for determining the membership of their respective group. The NSIEs meet jointly to identify lessons learned about processes and procedures, and to exchange information and views on threats, vulnerabilities, and their remedies. They share information about specific network security events and discuss general interest topics that may impact the PSN and the information systems supporting it. This exchange of intrusion information and data is facilitated by the use of nondisclosure agreements, which all representatives are required to sign before participating. Since their establishment, the NSIEs have gradually and successfully built an unparalleled level of trust between competitors in the telecommunications industry and between representatives from industry and from Government. Perhaps as important as the exchange of information have been the relationships fostered between the security practitioners that compose the NSIE.

The NSIEs also endeavor to share lessons learned about network security with a broader audience through workshops and analytical reports. In 1993, for instance, they examined the deficiencies in Federal computer crime laws and developed recommendations for correcting them. NSTAC presented these recommendations to the President. NSIE-sponsored workshops have addressed specific issues, such as the security of digital cross-connect systems, network firewalls, and advanced authentication techniques. Another workshop addressing the security of data networks is planned for September 1996.

Periodically, the NSIEs conduct risk assessments of the PSN. In the most recent assessment, dated December 1995, NSIE representatives expanded their focus from the PSN to the Public Network (PN)⁸ and stated the overall risk to the PN is greater now than it was perceived to be during the last formal risk assessment conducted in 1993. The NSIE representatives gave the following reasons for their conclusions:

- The threat is growing, primarily because of the increasing sophistication of the intruders and their more advanced methods of attacks.
- Deterrent capabilities, such as law enforcement and security awareness, are improving and require continued commitments of resources, as well as enhanced industry and Government coordinated efforts, but deterrent capabilities have not kept pace with the threat.
- The overall vulnerability is an increasing concern because computer intruders continue to exploit well-known vulnerabilities, while new technologies and the restructuring of the industry are introducing new vulnerabilities.
- Protection mechanisms are improving but have not kept pace with new and emerging vulnerabilities and the increasing capabilities of computer intruders.

The risk assessment further noted that Government and the telecommunications industry recognize the importance of protecting the PN, particularly as society moves towards increased use of the capabilities and services offered by the emerging NII. Consequently, Government and industry have taken actions, both independently and jointly, to make the PN more secure. They are taking advantage of available protection measures and continuing research into improved methods and tools to strengthen PN security. In addition to the tried and true methods (for example, intensive security evaluations and audits, improving security staff skills, and controlling proprietary information), Government and industry are pursuing new tools, such as advanced authentication mechanisms and internal network partitioning.

⁸The PN includes any switching system or voice, data, or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless services, and signaling networks).

⁵

Clearly, the NSIE process is a unique forum through which industry and Government address network security. Based on our experience in this forum, the NSTAC has drawn the following conclusions:9

- Technology alone will not solve the problem. To a great extent, security is a people problem, requiring both full attention and support of management and the continued vigilance of systems users and administrators.
- Protecting the PN and the NII is a continuous, dynamic, and growing process. Measures such as training and audits are not one-time efforts, and there is no guarantee that current measures will continue to be effective in the future.
- Security is everybody's problem. Service providers and equipment vendors are responsible for protecting the network components over which they have control. However, as customers gain access to network components that allow them to have greater control over their own services, they must also take responsibility for protecting those network components.
- The changing business environment should prompt periodic reviews of security programs. Efforts to reduce operating expenses frequently entail workforce reductions. Terminated employees have the knowledge, and may have the motivation, to attack the resources of their former employers; retained employees may become disgruntled or may simply be unable to devote as much time and attention to security-related activities as is needed. Companies that outsource their work or embark on joint ventures may be exposed to the vulnerabilities of their vendors and partners. Changes in how people do their work, such as telecommuting and the increasing use of laptops, create new vulnerabilities.
 - There is no silver bullet. Protecting the information systems that support telecommunications and other critical national infrastructures will require addressal of issues on a number of different levels and from multiple perspectives.

Network Security R&D

In 1991, the NSTF held a series of meetings in which the Government and industry shared information on network security R&D efforts and requirements. The purposes of these meetings were to identify what network security areas needed further R&D, determine what was already being addressed by Government, and make recommendations to the Government with

⁹Extracted from An Assessment of the Risk to the Security of Public Networks, U.S. Government and NSTAC Network Security Information Exchanges, February 8, 1996.

respect to R&D. The following areas were identified as needing further R&D: mechanisms for easy, portable control of access to a network element; a development to introduce an appropriate level of "suspicion" among trusted elements of the PSN; solutions for reliable recovery from damage to software and databases; means to adequately partition memory, or otherwise isolate network element software from databases that are more broadly accessed; means to analyze all events in a network and highlight questionable situations; and tools to plan an architecture toward a long-term, more secure network. Following submission of final recommendations to the NSTAC for presentation to the President, the NSTAC established the Network Security Group as a permanent body that, among other activities, continues to identify and assess network security R&D efforts and initiatives. In September of this year, the Network Security Group is sponsoring an R&D exchange to facilitate communication between the Government and industry about network security R&D issues. This R&D exchange will focus on issues of authentication, intrusion detection, and access control, from the capabilities management perspective.

Network Security Standards Oversight Group

In the past, security standards have not been a high priority (relative to other standards areas) and have been focused primarily on individual components of the network rather than the network as a whole. In an effort to increase awareness within the standards community of the importance of comprehensive, integrated standards, the NSTF created the Network Security Standards Oversight Group (NSSOG), which investigated standards and identified gaps in standards for network security. It was composed of individuals with design and operations expertise and standards awareness. The NSSOG did not develop or propose standards; rather, the members worked with the standards community to actively foster the development and adoption of a single consistent set of network security standards for the PSN that embraced architecture, design, operations, interfaces, and assurance. The NSSOG published its findings in October 1994. The NSTAC provided this report to various standards.

NATIONAL INFORMATION INFRASTRUCTURE ACTIVITIES

In February 1993, the President released *Technology for America's Economic Growth: A New Direction to Build Economic Strength*, which articulated his administration's vision and objectives for the NII. That document called for increased investment in information and communications technologies that together would compose the NII. Today, by undergirding much of the critical infrastructure on which the national economy rests, the NII is playing an increasingly prominent role in our economic and national security. However, the value derived from the development of the NII will be lost if we as a Nation cannot be assured that its resources are available when needed most. This concern was the primary impetus for the establishment of the NSTAC's NII Task Force.

NII Task Force

In March 1993, Dr. John Gibbons, Director of the Office of Science and Technology Policy, asked the NSTAC to advise the President on several NII-related issues, such as security, interoperability, standards, spectrum, and dual-use applications. In response, the NII Task Force was formed in August 1993 and began to study the effect of the evolving NII on NS/EP services. The task force was further guided in its efforts by *The National Information Infrastructure: An Agenda for Action*, released by the administration in Septem¹-er 1993. That document called for the NSTAC to continue offering advice to the President on NS/EP telecommunications issues, work with the Federal Communications Commission's Network Reliability Council, and complement the work of the U.S. Advisory Council on the NII.

The NII Task Force worked closely with the administration's Information Infrastructure Task Force and its committees and working groups on the following actions:

- Identified the policy implications of NS/EP concerns in the context of privacy and security for the NII. The task force also advised the Government on policy and regulatory issues that would accelerate commercialization of a nationwide highspeed network available to NS/EP users.
- Investigated potential NII applications that could serve both NS/EP needs and non-NS/EP Government needs. The task force identified the highest priority dual-use projects and areas worthy of increased emphasis by the Government.
- Analyzed industry trends and NS/EP issues that would arise as the NII evolved, specifically in the areas of interoperability and standards. The task force also examined technical, architectural, regulatory, and policy issues associated with the development of the NII.

Based on that work, the task force synthesized its findings into broader key issues and forwarded its recommendations to the President. More recently, the NII Task Force provided guidance to the Government on additional NS/EP issues stemming from its previous work. The task force undertook the following actions, which resulted in findings and recommendations to the President:

- Determined the NS/EP implications of the GII
- Completed an assessment of emergency health care information issues.

In addition, the NII Task Force determined the need to examine the feasibility of an NII Information Systems Security Board. NSTAC directed the task force to continue to explore an ISSB model that could work with recognized testing laboratories and commercial security consulting services to enhance the security component of the NII and identify the details of the ISSB's formation, operation, and funding. In addition, the task force was tasked to explore linkages with Government that may be essential to the ISSB and to ascertain support of the concept through outreach to appropriate industry, government, and other organizations, associations, and institutions.

Information Systems Security Board

Because information systems security issues have become increasingly important and national in scope, the NII Task Force is now concentrating its efforts on investigating the feasibility and advisability of establishing an industry-run ISSB as a potential mechanism for improving the security of the NII. In developing the ISSB concept, the task force identified potential information security functions that such an entity might perform. The task force then surveyed a sample of private companies, associations, universities, and Government agencies known to have significant information security programs to determine which functions were being addressed by those organizations. They discovered that many of the functions were being addressed either by the Government or for the Government by contractors, but not for the private sector. In addition, the task force researched organizational models that might provide a conceptual framework for an ISSB and subsequently proposed a model for the ISSB structure to achieve both institutional independence and accomplish those functions necessary to perform its mission. Specifically, the ISSB mission would be twofold: improve the common understanding of the nature and purpose of information systems security, and promote generally accepted information systems security principles and standards to improve the reliability and trustworthiness of the Nation's information infrastructure, services, and products. The task force is currently ascertaining the potential for broad support for the ISSB concept in the appropriate industry, Government, and academic organizations. As a next step, the task force will further examine the ISSB concept and provide final recommendations to the NSTAC for consideration. The NSTAC will forward its recommendations to the President.

NSTAC'S INFORMATION ASSURANCE ACTIVITIES

The NSTAC's experience identifying electronic threats and network vulnerabilities—and subsequent efforts to assess the NS/EP implications of the NII and GII—led directly to its most recent initiative, information assurance. As noted previously, the NSTAC considers information systems important because critical national infrastructures increasingly depend on these systems for the real-time exchange and processing of information. To an ever increasing degree, critical national infrastructures like financial services, electric power distribution, and transportation are using information systems and applications, perhaps best exemplified by the explosive growth and use of the Internet, that transit the PN to streamline their business processes and operations. As these infrastructures grow more dependent on the NII—and as the NII grows more reliant on

them—the risks to the national defense, the national economy, and society at large correspondingly increase. The need to provide information assurance in each of those critical infrastructures is based on the following:

- The current trend toward increased network interconnection, which has profound
 implications for all telecommunications and information networks. Security
 programs are often widely inconsistent both within and across network
 domains—allowing attacks to propagate from networks with weak security to
 networks with relatively solid security postures.
- The ambiguous nature of the threat. Although the effects of an attack on an information system may be apparent, the source and objective of the attack are not easily determined. The threat posed could be an adolescent motivated by curiosity or a foreign agent intent on sabotaging a vital system.
- Limited information sharing with respect to threat data. Although there is a great amount of information available within the intelligence community about the threat, this data is not generally shared within the intelligence community, nor is it shared with the elements of the private sector responsible for protecting critical, although unclassified, systems.
- Applicability of lessons learned. The lessons learned about information systems supporting the telecommunications infrastructure, as described in the NSIEs' 1995 risk assessment, are applicable to other infrastructures.
- The potential impact of the Telecommunications Act of 1996, which will likely result in the reconfiguration of the telecommunications infrastructure. For example, provisions in that act allow new types of service providers into the market, including the power companies, and allow greatly increased access to the PSN.

Information Assurance Task Force

In January 1995, the Director of the National Security Agency briefed the NSTAC on threats to U.S. information systems and the need to improve the security of critical national infrastructures. The NSTAC principals discussed those issues and subsequently drafted a letter in March of that year to the President stating that "[t]he integrity of the Nation's information systems, both government and public, are increasingly at risk from intrusion and attack ... [and that] other national infrastructures ... [such as] finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk."¹⁰ The President replied to the NSTAC letter in July 1995, stating that he would "welcome NSTAC's continuing effort to work with the Administration to counter threats to our Nation's information and telecommunications systems."¹¹ The President further asked "the NSTAC's principals—with input from the full range of users of the NII —to provide me with your assessment of national security emergency preparedness requirements for our rapidly evolving information environment."¹²

In May 1995, the NSTAC formed the Information Assurance Task Force (IATF) to work closely with the U.S. Government to identify critical national infrastructures and their importance to the national interest. Following several meetings with elements of the national security community, civil departments and agencies, and the private sector, the task force determined that electric power, financial services, and transportation were the most critical of the infrastructures. The task force recommended that those infrastructures be studied to assess—and to make them more aware of—how their dependence on information and information systems puts them at increased risk.

IATF Risk Assessments

The task force scheduled the three infrastructures identified above for assessment. The status of each of these assessments is summarized below:

- Electric Power Distribution. The IATF is currently assessing the risk to electric power distribution systems, specifically examining the associated systems that manage and control distribution. To provide a coherent picture of the whole, the assessment will also identify and describe the various elements of the utilities industry and the role each element plays in the overall infrastructure. Thanks to the willingness of that industry to cooperate with the NSTAC's efforts, the risk assessment will be completed in October of this year.
- Financial Services. An assessment of the financial services infrastructure has been initiated and will be completed in early 1997.
- Transportation Services. An assessment of the transportation services infrastructure is also under consideration and would be completed by the end of

¹²Ibid.

¹⁰Letter from Mr. William Esrey, Sprint Corporation and Chair of the President's NSTAC, to the President of the United States dated March 20, 1995.

¹¹Letter from the President of the United States to the NSTAC dated July 7, 1995.

Clearly, these activities complement those undertaken by the President's Commission on Critical Infrastructure Protection and the Infrastructure Protection Task Force, which were established by E.O. 13010 to examine threats and vulnerabilities to the Nation's most critical infrastructures. In addition to providing these bodies with NSTAC's experiences with respect to the information infrastructure and its interdependencies with other infrastructures, the IATF expects three outcomes from its effort:

- Based on the findings derived from the risk assessments, the IATF will propose high-level policy recommendations for NSTAC approval and presentation to the President. The IATF expects these recommendations to focus on the interdependencies of these critical infrastructures and how Government NS/EP requirements can best be achieved.
- The process of collecting and sharing information between infrastructures will heighten the awareness of information assurance threats and vulnerabilities. By sharing the lessons the NSTAC has learned about critical information systems, it is hoped that the companies composing other critical infrastructures will benefit from NSTAC's experience and become more aware of the vulnerabilities of the information systems on which their industries and, therefore, American citizens depend.
- The process will also demonstrate the value of the unique industry-Government relationship facilitated by the NSTAC-NCS process to address broader issues within the NII. An outcome from this effort might be the consideration on the part of all infrastructures to establish similar processes and constructs in their own respective domains to address information assurance issues and concerns.

A key consideration, and a point highlighted in the Subcommittee's minority report on "Security in Cyberspace," is the need to make threat information available to those infrastructures at risk from attack. The Subcommittee's recommendation that "the Director of Central Intelligence complete an NII threat estimate . . . [and] should have an unclassified version that can be made available to private industry" is in concert with the NSTAC's standing position on and interest in the ongoing National Intelligence Estimate and the need to heighten awareness of the IA threats in other critical national infrastructures and key end-user communities.¹³

¹³1996 NSTAC Industry Executive Subcommittee Working Plan.

Information Assurance Gaming Activities

As a resource to the Government, the NSTAC has been called on to analyze and examine information assurance and other commercial telecommunications issues in gaming and simulation environments. This is because NSTAC is a unique focal point for NS/EP issues relating to telecommunications and information systems, and its members are able to access a wide range of subject matter experts familiar with technical, policy, and strategic issues. In the past two years, representatives from the NSTAC have participated in the "Day After in Cyberspace" games sponsored by the DoD. Those games analyzed national-level concerns with respect to hostile information assurance/warfare actions against several of the Nation's most critical infrastructures. During these games, NSTAC representatives interacted with key decision makers in Government to surface high-level issues, including interdependencies among infrastructures; the need for a strategic indications, warning, and assessment capability; and the need for organizational clarity at the national level with respect to information assurance. Since 1991, representatives from the NSTAC member companies have also participated in the Global Games, an annual series of wargames sponsored by the U.S. Naval War College (NWC). The Global Games are designed to examine and challenge U.S. policies, strategies, and military doctrines in the context of global and regional military and geopolitical trends. For the past several years, the Global Games have addressed information assurance/information warfare issues to an increasing degree. This past year, the NCS and NSTAC developed information assurance scenarios that were incorporated into game play. These scenarios addressed potential attacks against those critical national infrastructures supporting defense operations.

NSTAC OUTREACH ACTIVITIES

The purpose of the NSTAC's outreach effort is to elevate the awareness of selected industries about the vulnerability of and threats to the Nation's critical infrastructures. This NSTAC outreach is a continuation and enhancement of previous outreach efforts and has two components: the Principal's Outreach Initiative and the ongoing IES outreach activities. The proposed Principal's Outreach Initiative is intended to address executive-level meetings of organizations and associations (i.e., the Business Roundtable, boards of directors, management councils, chambers of commerce, and industry associations) to raise the information assurance issue with other industry leaders at every opportunity. As described previously, this is an issue of national importance, and the NSTAC principals provide a conduit to heighten awareness outside of the traditional NS/EP venues. In addition to these efforts, several of the NSTAC groups and task forces are actively seeking to reach out to other industries and to the Government to address topics related to information assurance, network security, and other issues associated with telecommunications and information systems. These efforts ensure that the NSTAC will continue to provide the President with timely recommendations with respect to telecommunications and information systems, information assurance, and other critical NS/EP matters as the Nation moves ahead into the Information Age.

CONCLUSION

The NSTAC was created to help Government address NS/EP telecommunications issues arising from the dramatically altered marketplace resulting from the divestiture of AT&T. It was formed in response to the realization that the telecommunications infrastructure was an essential component of deterrence and recovery in the event of a major attack on the Nation. During its tenure, the joint NCS-NSTAC process has provided the President with advice as the industry has diversified, moved toward information systems composed of both telecommunications and computer networks, and reacted to a changing threat environment. Over time, NSTAC has become a model for industry-Government cooperation in addressing critical NS/EP issues affecting those information systems that support the NII and the Nation's other critical infrastructures in a rapidly changing environment. The lessons learned from the NSTAC experiences are generic and thus clearly applicable to the information systems supporting critical infrastructures. The emerging NII, and the dramatic changes likely to result from the implementation of the Telecommunications Act of 1996, give rise to significant new issues for the Government to address. The NSTAC hopes to continue to serve the Government by studying these issues and making recommendations to the President on ways to ensure that the vision of an NII can be achieved while sustaining the robustness, reliability, and security of those information systems supporting the Nation's critical infrastructures.

APPENDIX A

Letter from Mr. William Esrey, Chairman of the President's NSTAC, to the President of the United States

- Cristing

National Security Telecommunications Advisory Committee

March 20, 1995

The President The White House Washington, DC 20500

Dear Mr. President

We appreciated the opportunity to meet with you and the Vice President in January, and to discuss our mutual concerns facing the National Information Infrastructure on which our national security and economy are so dependent. The integrity of the nation's information systems, both government and public, are increasingly at risk from intrusion and attack by vandals, terrorists, foreign commercial interests, and potential adversaries. Other national infrastructures supporting American society, finance, air traffic control, power, etc., also depend on reliable and secure information systems, and could be at risk. Pursuant to your guidance, we are addressing these issues in conjunction with the National Communications System and will report back to you in October 1995 at the next National Security Telecommunications Advisory Committee (NSTAC) meeting.

In the interim, the Committee suggests two additional actions to further efforts in dealing with these threats to our national security. First, we recommend a senior administration policy official be designated as the focal point on issues affecting the information infrastructure's security. Second, we recommend a review and validation of national security and emergency preparedness (NS/EP) requirements for our nation's information infrastructure. Your Administration's focus on the economic dimensions of national security suggests the need to modernize NS/EP planning for continuity of operations across the spectrum of crises, including protection and recovery of the information infrastructure. The NSTAC is prepared to assist and invite representatives of other industries to join in contributing to this review.

Given the pace of the information revolution, the window of opportunity for cost effective and timely integration of measured security and protection into the National Information Infrastructure may not be open for long.

Confidence in and support for the protection of the Nation's vital information infrastructure is our goal. Your leadership in this area, combined with the efforts of the Federal and private sectors will make this a reality.

Sincerely,

Bill Bry

William T. Esrey Chairman

APPENDIX B

Letter from the President of the United States to Mr. William Esrey, Chairman of the President's NSTAC

THE WHITE HOUSE

July 7, 1995

Dear Mr. Esrey:

Thank you for sharing the concerns and vision of the National Security Telecommunications Advisory Committee (NSTAC) in your recent letter to me. I wholeheartedly agree with your views on the importance of the National Information Infrastructure (NII) to our nation's prosperity and security, and I welcome the NSTAC's continuing effort to work with the Administration to counter threats to our nation's information and telecommunications systems, particularly those used to meet our defense needs.

I agree high-level focus on our information infrastructure security needs is required. Several offices within the White House are working on various aspects of this problem, including the National Security Council, the Office of Science and Technology Policy and the Office of Management and Budget. For the near term, while we determine how better to address our information assurance policy needs, the National Security Council will serve as your point of contact, as it does now for other NSTAC activities.

I would ask you, as Chair of the NSTAC, to look to the NSTAC's principals -- with input from the full range of users of the NII -- to provide me with your assessment of national security emergency preparedness requirements for our rapidly evolving information environment. Your experience and insight will help us find efficient and innovative ways to protect government-critical information systems and networks.

2

I will look forward to your progress report on these issues at the NSTAC's October meeting.

Sincerely,

Bin Curton

5.

Mr. William T. Esrey Chairman and Chief Executive Officer Sprint Corporation Post Office Box.11315 Kansas City, Missouri 64112 539

APPENDIX C



THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC) FACT SHEET (June 6, 1996)

PURPOSE: The NSTAC provides advice and information, from the industry perspective, to the President and the Executive Branch regarding policy and enhancements to national security and emergency preparedness (NS/EP) telecommunications.

BACKGROUND: The President created the NSTAC by Executive Order 12382 in September 1982 to advise him on matters regarding NS/EP relecommunications. Four issues provided impents for the sessibilisment of the NSTAC: (1) The divestitute of AT&T, (2) Increased government reliance to commercial communications (95% of government communications travels) over the Public Networks), (3) Potential impact of new technologies on NS/EP telecommunications, and (4) Growing importance of command, control, and communications (3) to military and disaster response modernization. The NSTAC has been validated beinnially, most recend yb E.O. 1274, September 29, 1995. Membership is limited to 30 presidentiallyappointed industry leaders. Currently, the NSTAC is comprised of 29 senior executives (see reverse) representing major carriers, telecommunications and information settivities, and rowide recommediations to the President. Its most recent upwork provide recommediations to the President. Its most recent meeting, NSTAC XVIII, was held February 28, 1996.

LEADERSHIP: Assisting the President in NSTAC matters are: Vice President Gore; the National Security Advisor, Mr. Anthony Lake; the Secretary of Defense, William J. Perry [also designated as the Executive Agent, National Communications System (NCS)]; the Assistant to the President for Science and Technology, John H. Gibbons; and the NSTAC's Executive Secretary, Li Geo Albert J. Edmonds, Manager, NCS, and Director, Defense Information System Saperoy (DISA). The NSTAC chairmanabip, a rotating position, is currently held by William T. Esrey, Chairman and CED of Sprint Corporation. The vice chairman is Charles R. Lee, Chairman and CEO of GTE Corporation.

DUSTRY EXECUTIVE SUBCOMMITTEE (ES): The IES, principal working body of the NSTAC, consists of representatives appointed by each NSTAC Principal. It meets formally twice between each NSTAC meeting and informally as needed. The IES overses five permanent subgroups, Issues Group, Legislative and Regulatory Group (LRG), Network Security Group (NSG), NSTP Group, and Standards Llaison Group SLO). The Issues Group scopes potential issues for further IES consideration; the LRG examines legislative, regulatory, and policy issues; the NSG overses all network security activities; the NSTP Group examines issues related to our autio's NSTP posture; and the SLG works standard is sues: The IES also oversees two task forces working issues for the NSTAC, the National Information Infrastructure (RIU) Task Force and the Information Assurance Task Force (LATF). The majority of the NSTAC's work is done by these individual subgroups and task forces that address issues brought to the NSTAC from the President, his staff, or the NCS through the Office of the Manager, NCS (OMNCS).

Manager, NCS (DMNCS): NATIONAL COMMUNICATIONS SYSTEM: The NCS, an interagency group of 23 Federal departments and agencies, coordinates and plans NS7F telecommunications to support any crisis or disaster. Originally created with six members in 1960 as a testul of CJ failures during the Cuban Missite Disis, members of Agriculture, Commerce, Defons, Energy, Heald and Human Services, Interior, Justice, State, Transportation, Tressary, and Veterans Affairs, Central Intelligence Agency, Federal Communications Commission, Federal Energency Management Agency, Federal Reserve Board, General Services, Administration, National Security, and Veterans Information Administration, Nuclear Regulatory Commission, U.S. Information Administration, Nuclear Regulatory Commission, U.S. Information Agency, and U.S. Postal Service. Each NCS member organization is represented on the NCS committee of Principals (COP) and is subordinate Council of Resentations to the NCS on NS/EP telecommunications, participate and recommendations to the NCS on NS/EP telecommunications, participate in joint industry-government planning, and request advice and information from the NSTAC through the OMNCS. The OMNCS Customer Service Branch provides the means for joint industry-government planning through technical and executive support of the NCS COP and COR, as well as the President's NSTAC and its Subordinate groups.

NSTAC ISSUES: The President's NSTAC, working jointly with the Government, is addressing or has addressed the following issues:

ACTIVE ISSUES

 National Information Infrastructure (NII)
 Standards

 Wireless Services
 Threat Assessment

 Network Security
 Information Assurance

 Interoperability
 Telecommunications Legislation

PREVIOUSLY ADDRESSED ISSUES

Energy National Telecommunications Management Structure Assured Accounts International Diplomatic Telecommunications Ilectromagnetic Pulse Enknred Call Completion Underground Storage Tanks Service Priority Funding of NSTAC Initiatives Wirteless Low-Bit Digital Services National Coendinating Mechanism Dual Use Applications Dual Use Applications

ACCOMPLISHMENTS AND ACTIVITES: May activities of the NSTAC's subordinate groups result in technical regords, recommendations to the President, and operational programs. For example, the National Coordinating Center for Telecommunications (NCC), a joint industrygovernment operations center for planning, coordination, and exercise of NS/EP telecommunications, is the direct result of an NSTAC recommendation. Also, the Telecommunications Management Structure (NTMS), one NSTAC issues, are now operational programs. Much of the Government's National Level Program (NLP) for survivable and robust NS/EP telecommunications is a result of the President's NSTAC actions and recommendations. Separate industry and government Network Security to counter the threat of hackers and software disturbances to the PN. In December 1995, NSTAC approved their latest report, "An Assessment of the Risk to the Security of Public Networks." On February 28, 1996, the emerging global information Infrastructure (GU), and entry entry access Services. A primary Nots of NSTAC's most recent work has been the emerging global information Infrastructure (GU), and Centular Priority Access Services. A primary Nots of NSTAC's most recent work has been the examination of the emerging national security implications of IA. IA is force is activities, and the emerging antional security implications of IA. IA is normation infrastructure from exploitation, and denial of service. With the growing societal dependence on the information infrastructure, and its importance in meeting national economic and security interests, protecting key public and private elements of the nation's information infrastructures that perform critical national functions (e.g., electric power distribution, financial services, and the NIT and other information infrastructures that perform critical national functions, (e.g., electric power distribution, financial services, and transportation).

540

The President's National Security Telecommunications Advisory Committee (NSTAC) Membership (August 15, 1996)

Chairman, President & CEO, Electronic Data Systems (EDS) Mr. Lester M. Alberthal, Jr. Mr. Robert E. Allen Chairman & CEO, AT&T Ms. Betty C. Alewine (Pending) President & CEO, COMSAT Corporation Mr. C. Michael Armstrong Chairman & CEO, GM Hughes Electronics Corporation Mr. Stanley C. Beckelman President, Information Services, Boeing Chairman & CEO, Science Applications International Corporation (SAIC) Dr. J. Robert Beyster Mr. Bobby A. Boaldin Chairman, U. S. Telephone Association (USTA) President & CEO, Executive Security & Engineering Technologies, Inc. (ESET) Ms. Margo H. Briggs Executive Vice President & COO, Lockheed Martin Corporation Dr. Vance D. Coffman Chairman, President, & CEO, ITT Industries, Inc. Mr. D. Travis Engen Chairman & CEO, Sprint Corporatioo Mr. William T. Esrey (NSTAC Chairman) Mr. Louis V. Gerstner, Jr. Chairman & CEO, International Business Machines Corp. (IBM) Mr. Joseph T. Gorman Chairman & CEO, TRW, Inc. President & CEO, Bell Communications Research, Inc. (Bellcore) Dr. George H. Heilmeier Chairman, Advanced Digital Technologies Company (ADTC) Mr. William J. Hilsman President & COO, MFS Communications Company, Inc. Mr. Royce J. Holland Mr. Van B. Honeycutt President & CEO, Computer Sciences Corporation (CSC) Group Vice President, Lockheed Martin Federal Systems Mr. Arthur E. Johnson Chairman & CEO, GTE Corporation Mr. Charles R. Lee (NSTAC Vice Chairman) Mr. Craig O. McCaw Chairman, Teledesic Corporation Mr. Richard D. McCormick Chairman, President, & CEO, U S WEST, Inc. President & COO, Aerospace & Defense, Rockwell International Corporation Mr. John A. McLuckey Mr. John F. Mitchell Vice Chairman, Motorola, Inc. Chairman & CEO, MCI Communications Corporation Mr. Bert C. Roberts, Jr. Mr. Charles E. Robinson Chairman, President, & CEO, Pacific Telecom, Inc. (PTI) Mr. Donald J. Schuenke Chairman, Northern Telecom Inc. (NORTEL) Vice Chairman, BankAmerica Automation and Support Services, Mr. Martin A. Stein BankAmerica Corporation Mr. James A. Unruh Chairman & CEO, Unisys Corporation President & CEO, WorldCom Network Services, WorldCom Inc. Mr. Roy A. Wilkens Mr. Paul E. Wright Chairman, Chrysler Technologies Corporation (CTC)

APPENDIX D

Office of the Manager, National Communications System Plans, Customer Service and Information Assurance Division



NATIONAL COMMUNICATIONS SYSTEM (NCS) PLANS, CUSTOMER SERVICE, AND INFORMATION ASSURANCE DIVISION INFORMATION ASSURANCE BRANCH FACT SHEET (August 13, 1996)

PURPOSE: The Information Assurance (IA) Branch was established within the Plans, Customer Service, and Information Assurance Division to combine the network and information security imitiatives of the National Communications System (NCS) under a common program to increase their efficiency and effectiveness, apply a coordinated direction, and increase the general awareness of the importance of network security and information assurance to the NCS government and industry community. The IA Branch serves as a focal point within the NCS for network security and information assurance related activities of the Defense Information System Agency's (DISA) Center for Information Systems Security (CISS), the National Institute of Standards and Technology (NIST), and the General Services

BACKGROUND: In an April 23, 1990, memorandum, the National Security Council (NSC) tasked the Manager, NCS, to determine what actions are needed from the government and industry to protect national security and emergency preparedness (NS/EP) telecommunications on the Public Switched Network (PSN) from the "hacker" threat. In response to this tasking, the Manager, NCS, requested the President's National Security Telecommunications Advisory Committee (NSTAC) to work with the government to provide industry's perspective. The Manager and NSTAC identified several areas in which action was needed. The first was the need for a forum in which government and industry could exchange information important to the security of the PSN. In 1991, the Manager, NCS, and NSTAC established separate but closely coordinated Network Security Information Exchanges (NSIEs) to identify issues and share information about enetration or manipulation of software and databases affecting NS/EP telecommunications. A second area was the need for security related standards for telecommunications. In 1992, NSTAC established the Network Security Standards Oversight Group (NSSOG) to meet this need. In 1994, the evolution of the National Information Infrastructure (NII) elicited concerns about the security of information infrastructures supporting functions important to the national interest, such as telecommunications. The concern was that an adversary - a foreign nation, terrorist group, or organized crime - could wage an electronic attack on these infrastructures. In late 1995, in response to those concerns and the NCS interest in addressing them, the Information Assurance Branch was established within the OMNCS to address related security issues regarding a broader spectrum of information systems

LEADERSHIP: LIGEn Albert J. Edmonds is the Manager, NCS, and Director, Defense Information Systems Agency (DISA), and also serves as the NSTAC'S Executive Secretary. Ms. Diane Fountaine is the Deputy Manager, NCS, and is responsible for the day-to-day operations of the staff in OMNCS. Within the OMNCS, Chuck Caputo is the Director of the Plans, Customer Service, and Information Assurance Division and Fred Herr is the Chief of the Division's Information Assurance Branch and chair of the Government NSIE. Tim Tuttle, GTE, serves as chair of the NSTAC NSIE, and Randy Schulz, Bellcore, serves as the vicechair.

NATIONAL COMMUNICATIONS SYSTEM: The NCS, an interagency group of 23 Federal departments and agencies, coordinates and plans NS/EP telecommunications to support any crisis or disaster. Originally created with 5 members in 1963 as a result of command, control, and communications (C3) failures during the Cuban Missile Crisis, the NCS was expanded by E.O. 12472 to the current 23 members: Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Interior, Justice, State, Transportation, Treasury, and Veterans Affairs, Central Intelligence Agency, Federal Communications Commission, Federal Emergency Management Agency, Federal Reserve Board, General Services Administration, The Joint Staff, National Aeronautics and Space Administration, National Security Agency, National Telecommunications and Information Administration, Nuclear Regulatory Commission, U.S. Information Agency, and U.S. Postal Service. Each NCS member organization is represented on the NCS Committee of Principals (COP) and its subordinate Council of Representatives (COR). The COP and COR meet to provide advice and recommendations to the NCS on NS/EP telecommunications, participate in joint industry-government planning, and request advice and information from the NSTAC through the OMNCS. The OMNCS Plans, Customer Service, and Information Assurance Division provides the means for joint industry-government planning through technical and executive support of the NCS COP and COR, as well as the President's NSTAC and its subordinate groups

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC): The NSTAC provides advice and information, from the industry perspective, to the President and the Executive Branch regarding policy and enhancements to NS/EP telecommunications. The President created the NSTAC by Executive Order (E.O.) 12382 in September 1982 to advise him on matters regarding NS/EP telecommunications. Four issues provided impetus for the establishment of the NSTAC: (1) The divestiture of AT&T; (2) Increased government reliance on commercial communications (95% of government communications travels over the PSN); (3) Potential impact of new technologies on NS/EP telecommunications; and (4) Growing importance of C3 capabilities to military and disaster response modernization. The NSTAC has been validated biennially, most recently in September 1995 by E.O. 1274. Membership is limited to 30 presidentiallyappointed industry leaders. There are a number of NSTAC working groups and task forces that work closely with the government on telecommunications issues important to NS/EP.

NETWORK SECURITY INFORMATION EXCHANGES (NSIEs): The NSIE process was established to exchange information about the security of the PSN with the goal of improving each member's total knowledge and understanding of the problem. Members of the Government NSIE represent agencies that have research, standards, regulatory, law enforcement, or intelligence functions related to the PSN, or are major telecommunications users. NSTAC NSIE members include representatives from telecommunications service providers, equipment vendors, systems integrators, and major users. The NSIEs meet jointly approximately every 2 months to exchange information and views on threats and incidents affecting the PSN's software elements, and vulnerabilities and their remedies. In addition, the NSIEs periodically conduct an assessment of the risk to the PSN from electronic intrusion. In 1995, because of the evolving nature of the PSN' the NSIEs changed the description of their area of interest to the Public Network (PN), which better reflects the increasing diversity of communications alternatives, such as the Internet, used by the general public.

PRODUCTS AND ACCOMPLISHMENTS: Although membership in the NSIEs has been kept at a manageable size to promote trust and faciliate information exchange among representatives, the NSIEs have taken steps to share lessons learned in this forum with a broader audience. They have invited representatives from non-member or ganizations to attend NSIEsponsored workshops and symposia and have distributed NSIEdeveloped documents to organizations interested in improving the security of their networks. In early 1994, the NSIEs sponsored work hetwork Security Symposium to share information on the NSIEs' findings, conclusions, and recommendations from the experience gained and lessons learned over the first 2 years of the NSIE process. They have also sponsored workshops focused on topics such as firewalls and packet switched networks. NSIE documents include a Digital Cross-connect System Security Evaluation Aid and risk assessments of the PSN, with the most recent one completed in December 1995. The NSIEs also addressed the issue of legislative deficiencies in Federal computer ortine laws and made complementary resommendations to the President, through the OMNCS and the NSTAC, to correct those deficiencies. In addition to their collaboration in the NSIEs, government and industry also worked together to address the issue of network security standards. In 1992, NSTAC established the Network Security standards Oversight Group (NSSOG) to increase awareness within the standards for network security NIST participated in the NSSOG, having been designated by the President to serve as the government's focal point for network security standards. In 1994, the NSSOG produced a report identifying 12 major network security issues that need to be addressed. In October 1994, OMNCS issued a report focused on threat, *The Electronic Intrusian Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document. This document was updated in December 1995.*

INFORMATION ASSURANCE FOCUS: In 1994, with the evolution of the NII, concerns were expressed about the security of the infrastructures that comprise the NII. The telecommunications infrastructures (e.g., energy distribution) rejv on telecommunications to fulfill their functions. The government is also eager to apply lessons learned about the security of the PSN's OAM&P systems to other infrastructure elements. The OMNCS has established the Information Assurance Branch to improve awareness of the need to protect the critical information systems on which the NII relies. Joint government-industry efforts to address network security in the telecommunications industry have provided a model for government-industry information assurance issues within other segments of the NII.

FURTHER INFORMATION: For additional information, refer to the NCS Information Assurance Home Page: http://www.disa.mil/ncs/ncshome.html or http://164.117.147.223, or send inquiries to: Chief, Information Assurance Branch, National Communications System, Plans, Customer Service, and Information Assurance Division, 701 South Court House Road, Arlington, Virginia 22204-2198.

GOVERNMENT NSIE MEMBERSHIP

Central Intelligence Agency (CIA)

Defense Intelligence Agency (DIA)

Federal Bureau of Investigation (FBI)

Federal Communications Commission (FCC)

National Institute of Standards and Technology (NIST)

National Security Agency (NSA)

Department of Defense (DoD)

Office of the Manager, National Communications System (OMNCS)

United States Secret Service (USSS)

NSTAC NSIE MEMBERSHIP American Telephone and Telegraph Company (AT&T) BankAmerica Bell Communications Research, Inc. (Bellcore) Boeing Information Services GTE Corporation (GTE) Lockheed Martin Corporation MC1 Communications Corporation (MCI) Northern Telecom Inc. (NTI) Sprint Corporation To appear in the Journal of Criminal Justice Education, 1995 Senate Permanent Subcommittee on Investigations

EXHIBIT # 28a.

Crime and Crypto on the Information Superhighway

Dorothy E. Denning Georgetown University

December 13, 1994

Although the information superhighway offers many benefits to individuals and to society, it also can be exploited to further crimes such as theft and sabotage of data, embezzlement, fraud, child pornography, and defamation. Thus, a challenge in designing and using the information superhighway is to maximize its benefits while minimizing the harm associated with criminal activity. Three types of mechanisms that help meet this challenge are information security tools, ethics, and laws.

One information security tool that is particularly useful against crime is encryption, the scrambling of data in such manner that it can be unscrambled only with knowledge of a secret key. Encryption can protect against espionage, sabotage, and fraud. But it is a dual edged sword in that it also can enable criminal activity and interfere with foreign intelligence operations. Thus, the role of encryption on the information superhighway poses a major dilemma. This dilemma has been the topic of considerable dialogue and debate ever since the Clinton Administration announced the Clipper Chip, a special purpose encryption chip designed to meet the needs of individuals and society both for communications security and privacy protection and for law enforcement and national security. The outcome of the debate is likely to have considerable implications for criminal justice. In order to put the debate in context, we will first describe some of the criminal activities made possible by computer networks and how cryptography fits into a range of information security tools. We will then review the encryption dilemma and Clipper controversy.

Criminal Activities

Eavesdropping, espionage, and theft of information. In the best selling book The Cuckoo's Egg¹, Cliff Stoll tells the fascinating story of how he traced a 75¢ accounting error on the Lawrence Berkeley Labs computer system to a espionage ring in Germany selling information to the KGB. The German "hackers" were after military secrets, and they had penetrated dozens of computer systems by exploiting common system vulnerabilities, including default or poorly chosen passwords, and security holes in system software. None of the systems held classified information, but the case heightened concerns about the threat of government and corporate espionage to sensitive information stored on computer systems.

System break-ins are a common and serious threat. Once on a system, intruders are often able to

exploit additional vulnerabilities in order to attain privileged status, with access to all files stored on the machine. They then can browse through the files or download them to their own computer, and they can modify system files to ensure future entry and to cover up their tracks. If the computer is on a local area network, they might install a "password sniffer" program that intercepts network traffic and extracts passwords. If the computer is a workstation with a builtin-microphone, they might listen in on conversations taking place in the room. Information transmitted over computer networks is also vulnerable to interception while it passes through physically unprotected connections, particularly wireless, or is routed through untrustworthy hosts.

Credit card numbers and telephone calling card numbers are the target of many intrusions. In one case, up to \$140 million in unauthorized long-distance calls could have resulted from the theft and sale of thousands of telephone calling card numbers by an international ring of computer hackers, who obtained the numbers from suppliers in the United States, some of whom worked for the telephone companies². Many hackers ride the information superhighway for free, stealing long distance codes and services on computers and networks. It is like using turnpikes, tunnels, or bridges without paying the toll; or riding buses, subways, trains, and airplanes without paying the fare.

Cellular "bandits" use scanners to intercept the phone and serial numbers which identify cellular phones and are transmitted with each call. The numbers are used to make and sell "cloned" phones, which bear the same numbers as the legitimate phones. Cellular phone fraud costs the cellular industry an estimated \$1 million per day³. The problem is so serious in the New York City area that Cellular One temporarily suspended their roaming service in that area in December, 1994.

Because it is so easy to copy and distribute information electronically, computer networks present a serious risk to intellectual property. Commercial software is frequently uploaded onto bulletin boards and made available for free downloading in violation of copyrights and software licensing agreements. In October, 1994, hackers broke into a University of Florida computer and set up an invisible directory with test versions of OS/2 and Windows 95⁴. The Software Publishers Association has identified 1600 bulletin boards carrying bootleg software and estimated that \$7.4 billion worth of software was lost to piracy in 1993; by some industry estimates, \$2 billion of that was stolen over the Internet⁵. Documents, music, and images are similarly distributed over computer networks. Playboy Enterprises won a suit against the owner of a bulletin board for allowing postings of copyrighted images taken from *Playboy* magazine on the board⁶. In that case the images were not already on-line, but had to be scanned into a computer. Many organizations are struggling with the question of how to make their publications available electronically without suffering financial loss.

In the future, as the information superhighway looks more like an electronic marketplace, "digital cash" might be vulnerable to theft. "Burglars" might be able to break into a computer and download cash, and "muggers" might be able to rob intelligent agents that have been sent out on

the network with cash to purchase information goods.

Sabotage of data. System penetrators often damage files and records. Recently, a colleague reported that an intruder broke into their system and trashed a partition on one of their disks. Although they eventually recovered most of the lost data from backups, the restoration did not run smoothly and the disruption was considerable. Their experience was not uncommon. Even when an intruder does not overtly damage user data files, recovery from a break-in is disruptive since the system administrators must check for corrupted files and restore system files that were altered in order to allow for re-entry.

System penetrators have damaged sensitive and sometimes life critical information. In one case, a nurse broke into a hospital computer and altered patient records⁷. He changed prescriptions, "scheduled" an X-ray, and "recommended" discharge of a patient. In another, a prison inmate broke into a computer and altered the date for his release so that he could be home in time for Christmas⁸. There have been several reported cases of students who gained access to school records and altered their grades or the grades of classmates. Employees of banks and other companies have misused their computer privileges to embezzle money from their institutions by creating false accounts, changing accounting records, and inserting payroll records for bogus employees. In June, 1994, a hacker pled guilty to breaking into the computer systems of radio stations in order to rig promotional contests. He "won" two Porsches, two trips to Hawaii, and \$20,000 in cash⁹.

Malicious code. Malicious code can come in a variety of forms¹⁰. Computer "viruses" are fragments of code that attach themselves to the boot sector of a disk or to executable files on the disk. They are activated whenever the boot sector or host-file is loaded into memory and executed, and spread from one computer to another through floppy disks and computer networks. Some viruses re-format the hard drive, destroying all files in the process. Others print messages, play tunes, or cause congestion that slows down the machine.

"Worms" are active programs that spread through computer networks, potentially causing considerable damage. One of the most famous worms was launched on the Internet in 1988 by a graduate student at Cornell¹¹. The Internet worm eventually infected and shut down thousands of computers on the Internet.

A "logic bomb" is any form of malicious code that "detonates" in response to some event. A "time bomb"goes off at a particular time. Before quitting, one disgruntled employee left behind a time bomb disguised inside a "Cleanup" program¹². Had it not been caught in time, it would have destroyed a computer program used to build missiles. Some viruses behave as time bombs, hiding their presence and destructive nature until they have had a chance to spread. The Michelangelo virus is triggered on the artist's birthday, March 6.

A "letter bomb" is an electronic mail message which causes unexpected and harmful effects when the message arrives, is read, or is loaded into memory and executed. Joshua Quittner, journalist

and co-author of a forthcoming book on computer hackers, reported that he was mail bombed with thousands of pieces of unwanted mail that jammed his mailbox and eventually shut down his Internet access on Thanksgiving weekend, 1994¹³. In an unrelated incident occurring a few weeks later, a virus alert spread throughout the Internet warning of an e-mail message labelled "Good Times," which purportedly carried a virus that would wipe out the hard drive. Although the act of reading an e-mail message cannot cause code contained within the message to execute unless the system supports self-executing messages (most do not), an unsuspecting user might follow directions to store the message in a file and then execute it explicitly. The alert turned out to be hoax.

A "Trojan horse" is a program containing hidden malicious code, for example, a time bomb such as in the aforementioned Cleanup program. One of the ways that hackers acquire passwords is by replacing the login program on a computer with one that surreptitiously captures the passwords typed by users.

Electronic Mail Fraud and Anonymity. On many systems, it is easy to send an e-mail message that appears to come from someone other than the actual sender. Several years ago when I was interviewing hackers, I frequently received messages from them that appeared to be from myself. They did this to conceal their actual identity and location. More recently, while I was teaching my class how to send electronic mail, a student asked me how he could spoof a message from his roommate. He wanted to play a joke!

E-mail forgery is quite common. At Dartmouth, a student spoofed an e-mail message from the department secretary cancelling an exam. Half the students did not show up. At the University of Wisconsin, someone forged a letter of resignation from the Director of Housing to the Chancellor. In another case, a New Jersey housewife discovered that a Chicago man was sending obscene messages in her name. E-mail fraud could become a serious problem as the information superhighway evolves into a major system of electronic commerce, with million dollar contracts being negotiated and transacted through electronic mail.

On the Internet, it is possible to send or post an anonymous message by directing the message through an anonymous re-mailer that strips off the message headers, thereby hiding the true origin. While sending anonymous messages is not a crime and indeed has many benefits for privacy, it can be used in the furtherance of other crimes, for example, defamation and child pornography. Anonymous re-mailers have been used to send death threats to the President.

Sex crimes and sexual harassment. One of the dark sides of the computer revolution has been the use of bulletin boards and networks to distribute child pornography and find victims for child molestation. Many people are drawn into intimate relationships over computer networks, and pedophiles have taken advantage of this to befriend juveniles. In one case, a fourteen-year-old Boston boy disappeared after running away to meet a man in Texas who had sent him on-line love letters and airline tickets.

Networks also provide a tool for sexual harassment. A fourteen-year-old New Jersey girl reported that she was forced off the network after continuing to receive unwanted computer-generated sexual images of young boys. One woman joined an on-line service to discuss the joys and pitfalls of raising children, but found herself the target of an elusive "cyberstalker" who threatened her life, sent her pornographic e-mail, and may be following her around the country.

Defamation. A former Australian professor won \$40,000 in a defamation suit against an anthropologist who defamed him on a computer bulletin board distributed worldwide¹⁴. The message had said that his career and reputation were based on "his ability to berate and bully all and sundry," and suggested that he had engaged in sexual misconduct with a local boy. The suit did not implicate any operators of the bulletin board or network. In another case, Cubby, Inc. sued CompuServe, an on-line information service, for defamatory statements that appeared in one of their forums¹⁵. The court dismissed the case on the grounds that management of the forum had been contracted out to an independent firm, Cameron Communications, and that CompuServe was serving as a distributor rather than publisher, with little or no editorial control over content.

Information Security Tools

In order to better understand the role of encryption in protecting against some of the activities described above, we will first give a brief overview of three equally important types of security tools: access controls and monitoring, user authentication, and trusted systems and operational controls¹⁶.

Access controls and monitoring. Access controls are used to prevent outsiders from gaining access to a system through dial-up or network connections. They also can enable limited outside access to public files on a system, while prohibiting access to private files. For example, a site could make part of its file system available on the world wide web, using access controls to allow outsiders to retrieve web files, but not perform other functions on the system. By limiting the information that users can view or modify and the software and transactions they can run, access a system, but not everything on it.

Access controls are implemented with file system monitors, "firewalls," and other types of security monitors that control what operations can be performed and what information can be accessed. Some security monitors use artificial intelligence techniques and statistical profiling to determine whether a particular activity is likely to be indicative of an intrusion or other violation of security policy. Firewalls are computer gateways that monitor the flow of all traffic between a single computer or internal network and an outside network. They can be used to limit connections and the contents of traffic going in or out of the protected system. While not a panacea, they can be effective in protecting against network threats, including system penetrations. Anti-viral tools are monitors that check for and assist the user recover from computer viruses. Although they are not usually classified as access controls, their effect is to prevent malicious code from accessing and potentially damaging information.

Access controls are the primary mechanism for implementing a security policy on a system. However, they have several limitations. First, they cannot prevent an eavesdropper from intercepting traffic on an unprotected medium. Encryption is the only mechanism that addresses this threat. Second, they are ineffective without mechanisms that authenticate the identity of users and ensure the authenticity of software and data. Third, they can be subverted if the operating system or applications software has security holes, or if a system is not configured securely. Trusted systems and operational controls help mitigate this threat, but are not usually foolproof. Finally, they cannot prevent authorized users from misusing their privileges, for example, to commit fraud or to leak company secrets. Indeed, no security tool can prevent this. Worse, encryption can be used to conceal such activity as well as activity resulting from security breaches.

User Authentication. The most common method of user authentication is passwords that remain fixed for a period of time, sometimes indefinitely. Although passwords can provide an adequate level of security in many environments, systems that rely on fixed passwords are vulnerable to poorly chosen passwords that can be guessed or determined by systematic attack with "password crackers," and to capture by Trojan horse programs and password siffers. Frequent changes of passwords help protect against these threats, but a higher level of security can be obtained with "one-time passwords" and "challenge-response protocols" that use a different authentication value each time the user logs into the system. The authentication value may be generated by a special device (e.g., smart card or PCMCIA card) or software program that computes the next password in sequence or the response to the challenge. Cryptographic techniques are used in the process.

Biometrics, for example, thumb prints, voice prints, and retinal patterns, offer another method of user authentication. However, these approaches require special scanning equipment and are subject to false positives and negatives. But when combined with another form of authentication, they can provide a very high level of security.

Trusted systems and operational controls. A system may have reasonable access controls and authentication mechanisms, but use default passwords or security settings that are readily exploited, or have security weaknesses that allow an insider or outsider to circumvent the access controls. "Trusted systems," which are designed under strict criteria in order to provide a high level of protection against security breaches, are one line of defense. Operational controls, which include security checks, management of access privileges, system configuration, auditing, use of anti-viral tools, backups, and security awareness training, are another. Operational controls can help ensure that technical safeguards are used correctly and effectively, that the opportunities for users to misuse their privileges are minimized, that backup mechanisms are in place to protect against accidents or acts of sabotage, that.audit mechanisms are turned on, and that any discovered security weaknesses are appropriately handled. Separation of duties and two person control can minimize the possibility of a single user compromising information or engaging in fraudulent or destructive activity.

Most commercial systems are not "trusted," and it is not uncommon for security holes and

weaknesses to be discovered after they have been on the market for several months or years. Often, the discovery is made only after some security incident in which the vulnerability is exploited. In order to facilitate and coordinate responses to such incidents, a Computer Emergency Response Team (CERT) was established in 1988 to serve the Internet community. CERT reported that in 1993, there were 111 new incidents a month involving 1 to over 65,000 sites, and that in1994, the number of incidents increased by 77% and the number of sites affected by 51%¹⁷. The incidents involved malicious code, intrusions resulting from bypass of authentication mechanisms, exploitation of security holes in network services, password sniffers, insider attacks, and espionage.

Cryptography. A cryptographic system is a set of functions that are parameterized by keys and used for the purpose of secrecy or authenticity¹⁸. An encryption system is a special type of cryptosystem consisting of an encrypt function which scrambles (encrypts) data and an inverse decrypt function which restores the data to its original form. Encryption conceals data from anyone not knowing the secret key needed for decryption. It provides security and privacy protection for information that is vulnerable to eavesdropping or unauthorized access, for example, information transmitted over unprotected communication channels or stored on unprotected media. Cryptographic authentication mechanisms are used to protect against modifications to data, for example, insertion of malicious code into a standard program, and masquerading of users and host computers.

Historically, encryption has been used primarily by governments to protect classified communications. It has only been within the past decade or two that encryption has come into much use elsewhere, most notably in the banking industry to protect electronic transactions. Today, it is widely recognized as an essential tool for the information superhighway, although its use is still relatively low.

There are two types of cryptosystems: single key and public key. With single key cryptography, a common secret key is used both for encryption and decryption. The Data Encryption Standard (DES), which was adopted as a federal standard in 1977, is a single key system. Normally, a different "session key" is used with each communication, and each party to the communication must acquire a copy of the session key. In addition, each user may have a long-term key that is shared with a trusted server and employed by the server to authenticate the user and to distribute session keys. The Kerberos system, developed at MIT to protect their network from intrusions and unauthorized use, employs DES and a trusted server in this way to implement authentication and secrecy services on UNIX TCP/IP networks. Single key cryptography also can be used to compute "message authentication codes" for the purpose of authenticating information.

Public key cryptography uses a pair of keys, one public and one private. Typically, each user has a personal key pair, and the user's public key is used by other persons to send encrypted messages to the user, while the private key is employed by the user to decrypt messages received. Some public key cryptosystems implement "digital signatures" instead of or in addition to encryption. In that case, the private key is employed by the user to "sign" documents, while the public key is

used by the recipients to verify the signature. The RSA cryptosystem is a public key system with both encryption and signature capabilities. The Digital Signature Standard (DSS) is a public key signature-only system. Digital signatures provide strong authentication with non-repudiation, protecting against forgenes of documents and messages.

Because of their mathematical structure, public key systems are several orders of magnitude slower than most single key systems, making them less attractive for encrypting real-time communications or large files. However, they can provide a convenient method for establishing a session key for single key encryption. Thus, they are typically used only for key establishment and digital signatures. Current implementations of Privacy Enhanced Mail (PEM), an Internet standard for protecting electronic mail, use DES for data encryption and RSA for key establishment and digital signatures. Pretty Good Privacy (PGP), which is also used on the Internet, uses the single key algorithm IDEA with RSA.

Cryptographic techniques can be used to implement digital cash that is protected from duplication, alteration, and counterfeiting. They can be used to implement untraceable cash and anonymous, untraceable transactions. While such services can offer many privacy benefits, they also could facilitate money laundering and fraud.

Cryptography supplements and helps enforce access controls, authentication mechanisms, and operational controls. However, it is not a complete "security solution." If a system has security holes, an intruder might be able to penetrate the system, circumventing encryption and authentication mechanisms. They might then be able to obtain access to cryptographic keys or put a Trojan horse in encryption software. Encryption also cannot prevent insiders from misusing their access privileges.

y

The Encryption Debate

The Dilemma. By providing a mechanism for secrecy and authentication, cryptography can help protect against many of the criminal activities described earlier, including eavesdropping and espionage, system penetrations leading to sabotage, malicious software, and fraud. It can also be used to conceal crimes and malicious code. Employees can use encryption to leak company secrets, hide an embezzlement scheme, cover up a fraud, or hold information for ransom. Organized crime and terrorist groups can use it to protect their communications and computer files from lawful interception and search by the government.

By rendering communications and stored records immune from government access, encryption thus threatens investigations that depend on wiretaps or computer records for evidence. Already, investigations of child pornography cases have been hindered because seized computer files were encrypted with PGP and could not be broken. If encryption comes into widespread use on the information superhighway, this could seriously jeopardize law enforcement and the public safety. Encryption is also a threat to foreign intelligence operations, and thus can affect national security.

550

In considering the societal threat posed by cryptography, it is important to recognize that it is only encryption's role in providing secrecy that presents a problem. The use of cryptography for authentication does not threaten law enforcement and national security. Indeed, by strengthening the integrity of evidence and sources, cryptographic tools for authentication aid criminal investigations. Because different cryptographic methods are employed for secrecy and authentication, it is, therefore, possible to place safeguards on the former but not the latter. Indeed, this is the approach taken in the key escrow encryption initiative. Key escrow ties into encryption's role in providing communications secrecy on the information superhighway, but not its role in providing digital signatures and other authentication services, which help protect against system penetrations, malicious code, and forgeries.

Key escrow encryption and the Clipper Chip. In order to maximize the benefits of encryption to individuals and organizations, while minimizing its threat to public safety and law enforcement, the Clinton Administration developed and announced a key escrow approach to encryption designed to promote security and privacy on the information superhighway, while allowing government decryption of lawfully intercepted communications. The approach was first realized in the Clipper Chip, a tiny microelectronic chip that encrypts data using the SKIPJACK encryption algorithm, a classified single key algorithm designed by the National Security Agency. Prior to transmitting any encrypted data, the Clipper Chip transmits a Law Enforcement Access Field (LEAF), which contains the session key used for encryption and decryption. The session key is protected under two layers of encryption, and cannot be determined without a special decrypt processor, a common family key, and the device unique key for that particular chip. To obtain the device unique key, an authorized government official must get two key components, each of which is held by a separate key escrow agent (currently, these are the National Institute of Standards and Technology and the Automated Systems Division of the Department of Treasury). These components are combined inside the decrypt processor, where they enable decryption of the session key and thus decryption of the data. The chip and associated key escrow system have been designed with extensive safeguards to protect against any unauthorized use of keys¹⁹.

Clipper's general specifications were adopted in February, 1994, as the Escrowed Encryption Standard (EES), a voluntary government standard for encrypting sensitive but unclassified telephone communications, including voice, fax, and data²⁰. A standard for high-speed computer networks such as the Internet has not yet been proposed. The first product to use the Clipper Chip is the AT&T 3600 Telephone Security Device, which plugs into an ordinary telephone between the handset and base-set. Both parties to a conversation must have a device, but the party at either end can initiate a secure conversation by pushing a button. Once this is done, the security devices use public key cryptography to establish a one-time secret session key for the conversation, which is then encrypted and decrypted by the Clipper Chips at each end.

Criticisms of Clipper. Ever since its announcement, Clipper has been the target of blazing guns. Calling it "Big Brother in a chip," Clipper's strongest opponents have portrayed it as an Orwellian tool of oppression that will cripple privacy. They believe that citizens have the right to use strong encryption that evades government surveillance, and that exercising this capability is one way of

Clipper also has been criticized for being developed in secrecy without prior public review and for using a classified algorithm that is not open to public scrutiny. Critics argue that encryption standards should be developed by an open process, with input from industry, academia, privacy groups, and other interested parties. They argue further that Clipper products will have a limited foreign market as long as the algorithms are classified and the U.S. holds the keys, and that Clipper will not serve the needs for secure international communications.

Some of the criticism has been aimed not at the principle of key escrow encryption, but its particular instantiation with Clipper. Clipper is implemented in special tamper-resistant hardware in order to protect the classified SKIPJACK algorithm and to ensure that it cannot be used without the law enforcement access feature. Some vendors have stated that they would prefer a software approach, mainly because it would be cheaper, but also because it could be integrated readily into software applications. The selection of escrow agents has been criticized, with critics arguing that at least one should be outside the Executive branch, either in the Judiciary or private sector.

Some people have criticized Clipper for not going far enough and providing a mechanism whereby individuals and organizations can obtain emergency access to their own encrypted data through some sort of commercial key escrow system which would be managed by the private sector. Encryption poses a threat not only to public safety and law enforcement, but also to information security since encrypted data can become inaccessible if the keys are ever lost, destroyed, or held for ransom. Commercial key escrow could mitigate this threat, while also serving law enforcement needs.

Since Clipper is voluntary, many people argue criminals will not use it. They conclude that it will be waste of taxpayer money while needlessly introducing the risks associated with escrowed keys. In fact, cryptography without key escrow is spreading, and the government could very well find itself locked out of many communications and stored files.

Response and future directions. In adopting a new encryption standard, the government recognized that if it adopted a strong algorithm that precluded government access, the standard would almost certainly be used by criminals to the detriment of society. This outcome was considered unacceptable, and key escrow was seen as the best solution. Although no system is 100% risk free, Clipper's key escrow system has been designed with extensive safeguards that parallel those used to protect some of the country's most sensitive information. In my assessment, the risks associated with the compromise or misuse of keys will be negligible. Thus, key escrow will not degrade encryption's capability to protect against crime on the information superhighway, only its capability to conceal crime.

While these proposals are promising, I do not see them as replacements for Clipper, but rather as alternative options that may be better suited for some applications. Clipper offers excellent security, indeed the best security on the market. The SKIPJACK algorithm is considerably stronger than DES, and hardware generally provides greater security for keys and greater protection against sabotage or malicious code than software. Even for computer networks, the Capstone Chip, which is a more advanced version of Clipper that includes algorithms for the Digital Signature Standard and key establishment, is an attractive option for applications such as secure electronic mail and electronic commerce. Capstone has been embedded in a PCMCIA crypto card, called Fortezza, for use in the Defense Messaging System.

Although criminals may in fact not use Clipper, it is conceivable that over time, market forces could favor escrowed encryption. Organizations might require key escrow for their own protection, and vendors could favor it for its export advantage. The government will be ordering key escrow products, and demand for interoperability could lead to its proliferation. Criminals could choose key escrow because it is more readily available, to communicate with the rest of the world, or to allow their own emergency access.

Nevertheless, despite its benefits to organizations and to society, key escrow is highly controversial and vehemently opposed by some proponents of encryption. Thus, its widespread adoption is by no means assured. If it is rejected, the implications for criminal justice could be profound. As the information superhighway continues to expand into every area of society and commerce, court ordered wiretaps and seizures of records could become tools of the past, and the information superhighway a safe haven for criminal and terrorist activity.

Endnotes

¹Clifford Stoll, The Cuckoos Egg, Simon and Schuster, 1989.

²Bill Miller, "Ringleader Pleads Guilty in Phone Fraud," The Washington Post, Oct. 27, 1994.

³Mike Mills, "Cellular One Suspends a Service in N.Y. Area," *The Washington Post*, Nov. 29, 1994, p. C1.

⁴Michael Meyer with Anne Underwood, "Crimes of the 'Net'," *Newsweek*, Nov. 14, 1994, pp 46-47.

^{5.}Id.

⁶Playboy Enterprises Inc. v. George Frena et al., 839 F. Supp. 1552, U.S. Dist. Ct., M.D. Fla., Dec. 9, 1993. See also Dorothy E. Denning and Herb Lin, eds., *Rights and Responsibilities of Participants in Networked* Communities, Computer Science and Telecommunications Board, National Research Council, National Academy Press, 1994, box 3.9, p. 49.

⁷John Jones, "Hacker nurse makes unauthorised changes to prescriptions," *RISKS-FORUM Digest*, Vol. 15, No. 37, Jan. 3, 1994; reported from *The Guardian*, Dec. 21, 1993.

⁸Peter G. Neumann, Computer Related Risks, Addison-Wesley, 1994, p. 176.

⁹Elka Worner, "Hacker Pleads Guilty to Fraud," United Press International Newswire, June 14, 1994.

¹⁰. See Peter J. Denning, ed., Computers Under Attack: Intruders, Worms, and Viruses, ACM Press, Addison-Wesley, 1990; Robert Slade, Computer Viruses, Springer-Verlag, 1994.

¹¹. United States v. Morris, 928 F. 2d 504, 2d Cir. 1991. See also Peter J. Denning, supra note 10, pp. 191-281.

¹²William M. Carley, , "In-House Hackers: Rigging Computers for Fraud or Malice is Often an Inside Job," *The Wall Street Journal*, Aug. 27, 1992.

¹³.Philip Elmer-Dewitt, "Terror on the Internet," Time, Dec. 12, 1994, pp 44-45.

¹⁴. Margot Lang, "Computer Libel Wins Academic \$40,000;" The West Australian, Apr. 2, 1994.

¹⁵. Cubby Inc. v. CompuServe, 776 F. Supp. 135, S.D. N.Y., 1991. See also Denning and Lin, supra note 6, box 3.5, p. 45.

¹⁶For more information about information security tools, see Zella G. Ruthberg and Harold F. Tipton, eds., *Handbook of Information Security Management*, Auerbach, 1993; Charles P. Pfleeger, *Security in Computing*, Prentice Hall, 1989.

¹⁷L. Dain Gary, presentation at National Computer Security Conf., Oct. 12, 1994.

¹⁸. For more information on cryptography and the techniques and systems mentioned here, see Denning, D. E., "Cryptography and Escrowed Encryption," in *the Handbook of Information Security Management: 1994-95 Yearbook*; Zella G. Ruthberg and Harold F. Tipton, eds., Auerbach, 1994, pp. S-217-235; Denning, D. E., *Cryptography and Data Security*, Addison-Wesley, 1982; Bruce Schneier, *Applied Cryptography*, Wiley, 1994.

¹⁹ For more information about Clipper, its key escrow system, and how it is used, see Dorothy E. Denning, "Data Encryption and Electronic Surveillance," *SEARCH Technical Bulletin*, Dorothy E. Denning and Miles Smid, "Key Escrowing Today," *IEEE Communications*, Vol. 32, No. 9, Sept. 1994, pp. 58-68; Geoffrey R. Greiveldinger, "Digital Telephony and Key-Escrow Encryption Initiatives," *Federal Bar News & Journal*, Vol. 41, No. 7, Aug. 1994, pp. 505-510.

^{20.}"Escrowed Encryption Standard (EES)," Federal Information Processing Standards Publication (FIPS PUB) 185, National Institute for Standards and Technology, Feb. 9, 1994.

Senate Permanent Subcommittee on Investigations

EXHIBIT # _____28b.

Protection and Defense of Intrusion

Dorothy E. Denning

Georgetown University Computer Science Department, Reiss 225 Washington DC 20057 voice: 202-687-5703; fax: 202-687-1835 denning@cs.georgetown.edu http://www.cosc.georgetown.edu/~denning

March 5, 1996

This paper gives a brief overview of information system security vulnerabilities and countermeasures. It outlines why systems are vulnerable to intrusion, common methods of attack, and tools the attacker can draw upon. It summarizes information security technologies, including a new authentication technology based on geodetic location, and international efforts to address the societal conflict raised by powerful encryption programs. The paper is based on a talk given at the conference on National Security in the Information Age at the US Air Force Academy, Colorado Springs, February 28 - March 1, 1996.

Attacks and Vulnerabilities

The Automated Systems Security Incident Support Team (ASSIST) of the Defense Information Systems Agency (DISA) tested the vulnerability of 12,000 DoD host computers in the unclassified domain. They found that 1-3% of the systems had exploitable front doors and that 88% could be penetrated by network trust relationships. Only 4% of the penetrations were detected and, of those, only 5% reported. The 3rd Annual *Information Week/*Ernst &Young security survey found that one in five of the 1,290 companies responding reported network breakins. Two-thirds said they were hit by a virus.

Why Systems are Vulnerable. There are many reasons why systems are vulnerable to attack:

Security is hard and expensive. It is not easy to design systems that resist penetration, particularly in today's world where they are connected to open networks. It requires considerable skill and investment of resources, often involving dozens of engineers and scientists and years of work. Consequently, many systems have vulnerabilities which allow an intruder to bypass the security controls. In many cases, the security controls themselves introduce weaknesses. Security is a bottomless pit. It is often said that the only way to make a system secure is to pull the plug. It is not practical, and usually impossible, to achieve 100% security. Not only is it too expensive, it is unachievable because not all weaknesses and attacks can be anticipated. Vulnerabilities can be found in even carefully designed products.¹ New methods of attack are continually being discovered.² Thus, one settles for something less than perfect, say a 90% solution aimed at preventing the simplest and most common attacks. However, this brings me to the next observation:

Security is complex and fuzzy. We speak about information security as though it were welldefined and quantifiable. In fact, it is neither of these. Security policies are often complex, imprecise, sometimes conflicting, and subject to human judgement.³

Organizations are willing to take risks. Organizations generally do not demand perfect security for their systems and information. They are willing to take risks, as they do with other assets and technologies, in order to save time and money, to enjoy the benefits of the Internet and new services, to boost productivity, and to ensure that their employees and customers are not denied legitimate access. Many organizations connect to the Internet knowing fully well that they may be vulnerable to attack. Access to people, organizations, and information world-wide is considered well worth the risk. Security is about risk management, not absolute prevention.

Developers and users have limited resources. System developers have limited resources to spend on product development, and those resources have competing demands, including functionality, performance, and customer support. Decisions are based on factors such as marketability and profitability. Similarly, organizations have limited resources. Funds for security management, products, and training are balanced with other needs of the organization. In many organizations, the senior management do not view security as very important.⁴

New technology is constantly emerging. New technologies, for example, to support World Wide Web applications, bring forth new forms of vulnerabilities. In the rush to bring products to market and increase connectivity, the security implications are not always thoroughly researched and understood. Weaknesses are not discovered until after the products have been on the market. Security engineering lags behind the product development curve.

Security involves humans. Human beings are responsible for designing, configuring, and using systems with security features. They make mistakes in judgement and in implementation. They take shortcuts. They do not anticipate all possible failures. They can be conned by those wishing to intrude.

Lack of cryptographic infrastructure. In order to realize the full potential of cryptography for information security, a global public-key infrastructure must be developed. The infrastructure must offer high assurance that public keys are bound to particular individuals and organizations. It must provide services in support of confidentiality and authentication.

Export controls. Inadequate security is often blamed on export controls over strong encryption technology. The argument is that if there were no controls, strong encryption would be integrated into applications and networks, thereby making them secure. However, the situation is not so simple as security involves much more than unbreakable encryption algorithms. Thus, while export controls may have inhibited the integration of strong encryption into systems, the preceding factors seem much more significant. Moreover, cryptographic methods of authentication, which are largely exempt from export restrictions, play a larger role in preventing intrusions than methods of confidentiality protection.

Hackers often justify their cracking activities with the argument that systems should be secure; they are merely exposing flaws that never should have appeared in the first place and should be fixed. This argument falls apart, however, in the context of the preceding analysis. Networked systems will always have vulnerabilities, just as our streets, homes, and other public infrastructures do. Breaking into a computer system, without authorization to do so, is no more ethical than breaking into a house to demonstrate its physical vulnerabilities.

Methods of Attack. The following are some common methods of attack:

Insider misuse. Some of the most serious breaches of security are performed by insiders misusing their access authorizations. This is another reason why total security is unachievable. Although a user's access rights can be contained, they can never be so constrained as to preclude any misuse.

Social engineering. The attacker uses lies and deception to con the victim into providing information (e.g., passwords) that facilitates an attack. Strong technical safeguards can be useless against this form of attack.

Password cracking. Many passwords are easily guessed or vulnerable to systematic attack. These attacks are typically launched with the aid of a dictionary and password cracking program. First the attacker acquires a file of encrypted passwords. Then the cracking program is used to encrypt all of the words in the dictionary along with commonly chosen passwords until a match is found in the encrypted password file.

Key cracking. If encryption keys are not sufficiently long, they can be systematically broken by trying all possible keys until the correct one is found. Even keys that are long enough to withstand a brute force attack can be cracked if the random number generator used to create keys is not sufficiently good or if the cryptosystem has protocol failures or other weaknesses. In some cases, keys have been broken within a few minutes.⁵

Sniffers. "Sniffer" programs, installed on network nodes, intercept packets traversing the network and ferret out login IDs and passwords, credit card numbers, or messages containing certain keywords.⁶ This information is stored in a file, where it can be read by or transmitted back to the owner of the program.

IP Spoofing. This involves forging the Internet Protocol (IP) address of a trusted host in order to establish a connection with a victim machine. One method floods the trusted host with connection requests and then, while the host is recovering, sends packets that forge the node's IP address. The forged packets may contain data that allow the attacker to gain privileged access on the victim machine.

Injecting viruses, Trojan horses, time bombs, and other malicious code. Malicious code is injected into a target system through a disk or computer network. The code could alter or destroy data or cause other types of mischief.

Exploiting weaknesses in operating systems, network protocols, and applications. In general, any system vulnerability can be exploited to form an attack.⁷ Depending on the weaknesses, such attacks may effectively circumvent access controls and encryption, allowing access to plaintext data without the need to crack passwords or encryption keys. An intruder may be able to download tens of thousands of credit or calling card numbers at a time. Weaknesses are often found in configuration settings and parameter checking.

The Attacker's Toolkit. The attacker has many tools to draw upon. These include:

Programs and scripts. A variety of programs and scripts are available to locate system vulnerabilities and launch attacks. These include password crackers, key crackers, cryptanalytic tools, vendor utility and diagnostic programs, Trojan horse system utilities, special hacker tools (e.g., RootKit⁸), and graphical network sweepers (e.g., SATAN). A Trojan horse system utility is a program which resembles a real utility to the unsuspecting user but performs some subversive function. The attacker replaces the real utility with the Trojan horse, which is then executed whenever the utility is invoked. Network sweepers are programs that check the nodes on a network for poor configuration settings and other vulnerabilities. Many programs and scripts that are developed to aid the system administrator check for weaknesses are also useful to the attacker becomes easier. Sophisticated attacks can be launched by persons with only modest technical expertise.

Delivery mechanisms. Malicious code can be injected into a target system through a variety of delivery mechanisms, including floppy disks, network protocols, electronic mail, and web browsers. It can be concealed in the low order bits of images or in macros attached to documents, and then activated when the image or document is opened and processed. A web browser or other Internet application may download and execute software without the user's knowledge.

Publications and forum. Information and software tools that facilitate attacks are exchanged and distributed through a variety of media including electronic bulletin boards, Internet web pages and news groups, Internet chat services, electronic and paper magazines, conferences and meetings, and e-mail distribution lists. The Internet has greatly facilitated the spread of knowledge about

vulnerabilities and the distribution of tools, both to the attackers and to those who are responsible for defending against intrusion.

Massive computing resources. This includes powerful workstations and supercomputers, but also the Internet as a massive distributed computing system. The Internet lends itself particularly well to any task that can be broken into independent pieces, for example, breaking encryption keys.⁹

Anonymity and invisibility. Attackers use a variety of mechanisms to hide their identity, activities, and location. These include masquerading as legitimate users (after first acquiring their passwords) and hosts (IP spoofing), disabling audit programs, looping, sending messages through anonymous remailers, and encrypting electronic mail and files. Looping involves logging into a target system via a lengthy path that goes through many intermediate systems, using multiple carriers and passing through multiple jurisdictions. The objective is to make it extremely difficult to trace the connection back to the attacker. Anonymous remailers allow an attacker to send email or post messages that cannot be traced to the source.

Technologies of Defense

Information security is about risk management, not absolute security, and involves application of both technical and non-technical countermeasures. Non-technical defenses include formulating a security policy for the organization and educating users about that policy.

The following gives a brief description of the main technologies of defense and some of their potential vulnerabilities. In describing vulnerabilities, I do not mean to suggest that the technologies are riddled with holes or useless, only that they may not be foolproof. Particular attention is given to two recent technologies, location-based authentication and key escrow encryption.

Authentication. These technologies are used to determine the authenticity of users, network nodes, and documents. They are typically based on knowledge of secret information such as a password, PIN, or cryptographic key; possession of a device such as an access token or crypto card; and biometrics such as a thumb print or iris pattern. While all of these methods are valuable, they also have limitations. Secret information may be vulnerable to guessing and cracking, hardware tokens to theft, and biometrics to false positives, false negatives, and replay. In addition, authentication controls are potentially vulnerable to subversion or by-pass.

Location-based authentication. International Series Research, Inc. of Boulder, Colorado, has developed a new technology for authentication, called CyberLocatorTM, which uses space geodetic methods to authenticate the physical locations of users, network nodes, and documents.¹⁰ This is accomplished through a location signature sensor, which uses signals from the Global Positioning System's worldwide satellite constellation to create a location signature that is unique to every location on Earth at every instant in time. This signature is used to verify and certify geodetic location to within a few meters or better. Because the GPS observations at

any given site are unpredictable in advance (at the required accuracy.level), constantly changing, and everywhere unique, it is virtually impossible to spoof the signature.

The CyberLocator technology is not vulnerable to many of the techniques in the attacker's toolkit, in part, because it does not rely on any secret information and it is not readily forged. In addition, it counters one of the attacker's most powerful tools, anonymity. Because the exact location of the intruder is revealed, it defeats looping and masquerading. It would be a strong deterrent to many potential intruders, who would be unwilling to make their locations known.

Location-based authentication would normally be used in combination with another method of authentication. Its value added is a high level of assurance against intrusion from any unapproved location regardless of whether the other methods have been compromised. In critical environments, for example, military command and control, nuclear materials handling, telephone switching, air traffic control, and large financial transactions, this extra assurance could be extremely valuable. Location-based authentication also has applications besides access control, for example, implementation of an electronic notary function or enforcement of transborder data flows (e.g., export controls).

Cryptography. Various cryptographic techniques provide confidentiality protection (encryption) and authentication, which includes data integrity; user, host, and message authentication; and digital signatures. They are used to protect both communications transmitted over open networks and data stored in computer files. Cryptographic systems can be implemented as stand-alone products or they can be integrated into applications and network services, where they may be transparent to the user. They are potentially vulnerable to weaknesses in algorithms, protocols, key generation, and key management.

The encryption conflict. Encryption is essential for protecting classified national security information, unclassified but sensitive business and government information, and individual privacy. At the same time, in the hands of foreign adversaries, it interferes with signals intelligence. Terrorists, drug dealers, and computer intruders can use it to conceal their activities and stored records. Law enforcement agencies are concerned that as encryption proliferates worldwide, it could seriously imperil their ability to counter domestic and international organized crime and terrorism. It could cut off valuable sources of foreign intelligence. Even within an organization, encryption can cause problems. If keys are lost or damaged, valuable data may become inaccessible.

Because of its significance to national security, encryption is classified as a munitions and subject to export controls. These controls have come into conflict with the need for strong encryption on the global information infrastructure to support secure international communications and the desire of industry to compete in the global encryption market.¹¹

While it is beyond the scope of this paper to discuss the encryption conflict in any depth,¹² I shall briefly summarize international efforts aimed at accommodating the different interests. The

Organization for Economic Cooperation Development (OECD) is addressing the issues through its Committee for Information, Computer, and Communications Policy (ICCP). An ad-hoc group of experts on cryptography policy held an initial meeting in December 1995, and is expected to meet again in spring 1996 after being officially established by the ICCP. The December meeting was immediately followed by a Business-Government Forum on Global Cryptography Policy sponsored by the OECD, the International Chamber of Commerce, and the Business and Industry Advisory Committee to the OECD. At that meeting, representatives from the international business community and member governments agreed to work together to develop encryption policy guidelines based on agreed upon principles that accommodate their mutual interests. Statements of principles were issued by the INFOSEC Business Advisory Group (IBAG), an association of associations representing the information security interests of users, and a quadripartite group consisting of EUROBIT (European Association of Manufacturers of Business Machines and Information Technology Industry), ITAC (Information Technology industry Association of Canada), ITI (Information Technology Industry Council, U.S.), and JEIDA (Japan Electronic Industry Development Association), which accounts for more than 90% of the worldwide revenue in information technology.¹³ In addition to the above OECD-related efforts, the International Cryptography Institute, sponsored by the National Intellectual Property Law Institute and chaired by myself, brought together people from all over the world to address the encryption conflict at its meetings in September 1994 and 1995.14

One approach that has received considerable attention uses trusted parties as key holders. The keys held by these parties are not normally the same as the ones used for data encryption, but they allow access to the data encryption keys. This approach, sometimes called key escrow or emergency data recovery, can accommodate access by the owners of data who have lost their keys as well as by government officials operating under a court order or other lawful authorization¹⁵. Many existing encryption products have data recovery capabilities to accommodate user needs; some have integrated it into their key management services. Data recovery could be a service provided by an international network of trusted parties accredited to offer services that support digital signatures, notarization, confidentiality, and data integrity. This effectively puts key escrow in the public-key infrastructure. The European Commission is proposing a project to establish such a European-wide network. X/Open is drawing up plans for a public-key infrastructure project that would create specifications and possibly operating manuals for use in conformance testing and site accreditation. The U.S. government plans to finalize criteria for exporting software encryption with key escrow in early 1996.¹⁶

The objectives of business regarding encryption with trusted parties are articulated in the IBAG principles. Businesses and individuals would lodge keys with accredited trusted parties, which could be independent entities or entities within a company. The trusted parties would be liable for any loss or damage resulting from compromise or misuse of keys. Keys would be available to businesses and individuals on proof of ownership and to governments under due process of law. The principles call for industry to develop open voluntary, consensus, international standards and for governments, businesses, and individuals to work together to define the requirements for those standards. The standards would allow choices about key holder(s), algorithm, mode of operation,

key length, and implementation in hardware or software. Products conforming to the standards would not be subject to restrictions on import or use and would be generally exportable.

Access controls. These technologies are used to control access to networks, computers, applications, transactions, and information according to a security policy. Policies can be based on individual users, groups, or roles and on time of day or location. Access controls rely on authentication mechanisms to confirm the identity of users attempting access. They are typically integrated into both applications and systems software. Access controls are potentially vulnerable to bypass, failure to correctly implement the security policy, and ill-defined policies.

Firewalls. A firewall is a trusted computer system that monitors all traffic into and out of a protected network. It is frequently placed between an organization's internal network and the Internet with the objective of keeping intruders out and proprietary or sensitive data in. The firewall examines each incoming or outgoing message to determine whether it should be allowed to pass. Decisions can be based on protocol, source or destination address or port number, and message contents. Firewalls are potentially vulnerable to subversion, to malicious code that enters the firewall in a seemingly legitimate message, and to ill-defined or incomplete policies.

Audit. Audit logs record security relevant activity, for example, successful and unsuccessful logins, execution of system commands and applications, and access to files and database records. Auditing can be performed at both the system level and the application level. Audit mechanisms are potentially vulnerable to being disabled or bypassed; audit records to tampering or deletion.

Intrusion detection/monitoring. Intrusion detection systems actively monitor a system for intrusions and unauthorized activity. They typically inspect audit records, either after the fact or in real-time. They can look for particular events or event sequences, or for behavior that is abnormal. They are normally run under the direction of a security officer who specifies the events of interest and evaluates the results. Monitoring is analogous to the use of guards to keep watch over the physical premises of a protected site, either through direct surveillance or through video cameras. It is potentially vulnerable to false positives and false negatives, to being disabled, and to incomplete or false knowledge about misuse scenarios.

Anti-viral tools. These include scanners, which look for specified patterns; disinfectants, which remove viruses; and integrity checkers, which check for modifications to files and code. Potential vulnerabilities include failure to detect unknown viruses or to adequately protect checksums.

Vulnerability assessment tools. These are the same tools described earlier under the attacker's toolkit. They are potentially vulnerable to failure to detect a weakness or to misuse.

Trusted systems design. Good engineering, based on sound security models, is the bedrock for all trusted systems (complete systems or components). It can increase assurance that the systems meet their specifications and do not have certain weaknesses. It is integral to the development of high assurance systems. Trusted system development does not, however, guarantee perfect

Conclusions

The encryption conflict is an instance of a broader conflict between the defensive use of information security technologies and offensive operations against foreign adversaries, criminals, and terrorists. To the extent that the systems and communications of our adversaries are secure, they preclude penetration or signals intelligence. The central question facing us is how best to accommodate the need for government access. Should national policy promote or require approaches that ensure access by the government? This will be the topic of much debate for at least the near future.

Notes and References

1. As an example, in February 1996, the COAST (Computer Operations, Audit, and Security Technology) Laboratory at Purdue University reported an unexpected weakness in version 4 of Kerberos, a system that provides authentication and encryption services for distributed systems. Kerberos was developed in the mid-1980's at MIT and had been regarded as very secure.

2. For example, Paul Kocher recently demonstrated a new method of cryptanalysis based on timing estimates. See Paul Kocher, "Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attacks," Dec. 7, 1995.

3. See Hilary Hosmer, "Security is Fuzzy: Applying Fuzzy Logic to the Multipolicy Paradigm," Computer Security Journal, Vol. XI, No. 2, Fall 1995, pp. 15-24.

4. The 3rd Annual *Information Week*/Ernst & Young survey found that only 24% of information security managers reported that senior management perceives security as extremely important. 32% reported it as somewhat important, 39% as important, and 5% as unimportant.

5. The Kerberos vulnerability involved a poor random number generator that allowed session keys to be cracked in just a few minutes. A similar weakness was found (and corrected) in Netscape. See Steven Levy, "Wisecrackers," *Wired*, Mar. 1996, pp. 128+.

6. Many security papers and books discuss these attacks. For an award-winning paper on this topic, see E. Eugene Schultz and Thomas A. Longstaff, "Internet Sniffer Attacks," *Proc. 18th National Information Systems Security Conf.*, Oct. 1995, pp. 534-542.

7. See William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994, for a good discussion of system vulnerabilities and countermeasures.

9. For example, the Internet was used to help break a 129-digit secret RSA key between September 1993 and October 1994. The attack, which required factoring a 129-digit public key, was carried out with the assistance of 1,600 machines that sent partial results to a computer at MIT. See Steven Levy, "Wisecrackers," *Wired*, Mar. 1996, pp. 128+.

10. See Dorothy E. Denning and Peter F. MacDoran, "Location-based system delivers user authentication breakthrough," *Computer Security Alert*, No. 154, Jan. 1996, pp 1+.

11. See the Computer Systems Policy Project report, "Perspectives on Security in the Information Age," Jan. 1996 for the views and recommendations of representatives of the U.S. computer systems industry regarding export controls.

12. For a balanced discussion of the issues, see Susan Landau et. al, *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy*, ACM, June 1994. For my personal perspective, see Dorothy E. Denning, "The Future of Cryptography," presented at the joint Australian-OECD Conference on Security, Privacy, and Intellectual Property Protection, Canberra, Feb. 7-8, 1996. http://www.cosc.georgetown.edu/~denning/crypto/Future.html.

13. The IBAG and EUROBIT-ITAC-ITI-JEIDA statements are available at http://www.cosc.georgetown.edu/~denning/crypto.

14. Information about the ICI is available at http://www.cosc.georgetown.edu/~denning/crypto.

15. For a general description of key escrow and the U.S. government's proposal for exporting software encryption with key escrow, see Dorothy E. Denning and William E. Baugh, Jr., "Decoding Encryption Policy," *Security Management*, Feb. 1996, pp. 59-63. For a more detailed description of key escrow systems, see Dorothy E. Denning and Dennis K. Branstad, "A Taxonomy for Key Escrow Encryption Systems," *Communications of the ACM*, Vol. 39, No. 3, Mar. 1996.

16. Draft Software Key Escrow Encryption Export Criteria (11/95 version) and Key Escrow Agent Criteria," draft, Dec. 1, 1995. Available through http://csrc.ncsl.nist.gov/keyescrow.

LEHRSTUHL FÜR STRAFRECHT. STRAFPROZESSRECHT UND RECHTSPHILOSOPHIE UNIVERSITÄT WÜRZBURG 97070 W Ü R Z B U R G DOMERSCHULSTRASSE 1 6 TELEFON 0 9 31 - 31 23 04 TELEFAX 0 9 31 - 31 27 97 EMAIL sieber Øjura.uni-wuerzburg de

> Senate Permanent Subcommittee on Investigations

EXHIBIT # 30a.

Computer Crime and Criminal Information Law

- New Trends in the International Risk and Information Society -

Statement

by

Professor Dr. Ulrich Sieber University of Würzburg, Germany

for the

Hearing on Security in Cyberspace

of the

United States Senate

Permanent Subcommittee on Investigations

Committee on Governmental Affairs

on

July 16th, 1996

Computer Crime and Criminal Information Law

- New Trends in the International Risk and Information Society -*

Computer crime and criminal information law are relatively young phenomena. A first historical analysis indicates that each new development of computer technology was followed by a corresponding adaptation of crime as well as by legislative changes. A short overview - using the example of Germany - illustrates this adaptation of crime and information law to the new information technologies. It also indicates that this process started gradually at first, but then continued at an increasing pace:

- From the beginning of the 1950s computers were introduced in industry and administration to control routine processes. As late as 20 years after that time, the first cases of computer manipulation, computer sabotage and computer espionage became known. Only in 1986 did the German legislator react with the Second Act for the Prevention of Economic Crime.
- On the other hand, the mass processing of personal data in electronic data banks since the 1960s was soon regarded as a danger to privacy. In Germany, the first law that took this development into account was enacted in 1970.
- The open networks of the 1970s soon led to corresponding misuses in the form of ,hacking", which the Law Committee of the German Parliament could still consider in the Second Act for the Prevention of Economic Crime in 1986.
- The mass phenomenon of program piracy came along simultaneously with the spreading of personal computers in the 1980s, forcing the legislator to carry out different reform measures from 1985 onwards.
- The use of automated teller machines in the 1980s, too, was immediately followed by new ways of code card misuses, which already represented criminal offenses due to the reforms of the Second Act for the Prevention of Economic Crime.
- Today, electronic post services, mailboxes, ISDN as well as the development of close links between data processing and telecommunication are used by neo-nazi groups, perpetrators in the field of economic crime and organized criminals: Computer technology and telecommunication have not only become part of general life, but also of general crime. The changes that these new technologies caused in criminal procedural law do therefore not only concern traditional computer offenses, but all kinds of crime.

Updated and extended version of an article in the German language published in Computer und Recht (CR) 1995, pp. 100 et seq.

Starting from this historical background the first part of this paper will give an overview on the relevant forms of offenses and changes in computer crime. The second part deals with the corresponding reactions of the law. The third part asks for the change of paradigms and future prospects of the legal development. In the end, the analysis will show that the multitude of computer-related offenses has led to four waves of computer-specific reform laws in all countries, which are marked by the fundamental changes of our society.

I. Current Forms of Offenses

In most countries, the discussion about computer misuse began in the 1960s with the endangerment of privacy, which was discussed under the catchword of "data protection" and was at first not seen as a part of "computer crime" (see infra A). In the 1970s, scientific research concentrated on computer-specific economic crimes, especially computer manipulations, computer sabotage, computer espionage and software piracy (see infra B).¹ Further research demonstrated rapidly that - along with the advance of information technology into new areas of life - criminals can use computers for almost all offenses and that - from a phenomenological point of view - homogeneous computer crime does not exist any more (see infra C).² Today changes and differentiations that are characterized especially by the innovations of telecommunication technology are ascertainable in all areas mentioned.

A. Infringements of Privacy

The 1960s saw the beginning triumph of computers, and in many Western countries it was realized that the collection, storage, transmission and connecting of personal data endangers the personality rights of citizens. *Orwellian* visions and the mistrust of the revolting youth of the late sixties inspired the discussion about the dangers of the "Big Brother". However, today the old paradigm of the computer as an exotic instrument in the hands of the powerful became at the latest obsolete with the massive spreading of personal computers.

According to official statistics, data protection offenses are only of limited importance today.³ The cases that became known show different degrees of endangerment: The misuse of "STASI" documents, i.e. the documents of the Ministry for State Security of the former GDR, or the possible blackmailing of AIDS-infected patients prove that in the information society of the 20th century, data protection has become a central matter of concern. The storing of information about defaulting debtors by credit investigation agencies or the transmission of data within criminal prosecution authorities also show, however, that the ascertainment of infringements of privacy in

¹ Cf. Sieber, Computerkriminalität und Strafrecht, 1st edition 1977, 2nd edition 1980, pp. 1/39 et seq., 2/97 et seq. (Japanese translation by Noriyuki Nishida and Atsushi Yamaguchi, 1986 and 1988).

² Cf. Sieber, The International Handbook on Computer Crime, 1986, pp. 26 et seq. (French translation "La délinquence informatique" by Sylvie Schaff and Martine Briat, 1990); Sieber, The International Emergence of Criminal Information Law, 1992, pp. 6 et seq.

³ In Germany, the share of data protection infringements compared with the total number of computer crime cases registered by the police just amounted to about 1 % in 1993. Cf. Federal Criminal Agency (ed.), Police Criminal Statistics of 1993, 1994, table appendix 01, sheet 18, key figure 7280 as well as Möhrenschlager, in: Sieber (editor), Information Technology Crime, 1994, p. 200.

numerous cases depends on a difficult assessment and evaluation of conflicting principles: The underlying discussion on values does not only have to deal with the protection of privacy, but also with the freedom of information, which is the driving force of the cultural, economic and political development of an "open society".⁴

"Clear" infringements of privacy became known especially in the area of traditionally protected (also by criminal law) professional secrets, especially concerning official secrecy as well as the requirement of confidentiality for officials, doctors, lawyers and banks. Such data constituted the object of the offense in a South-African case, in which the offender - presumably through theft of magnetic tapes - obtained medical data of persons which had undergone an AIDS-test; the data were passed on to the employers of the persons affected.⁵

Another clear case of infringement of traditional regulations on protection of secrets happened in 1989 when two employees of one of the biggest Swiss banks helped the French tax authorities to decode magnetic tapes containing customers' data for a compensation of 500,000 FF.

In contrast, difficult problems on evaluation and assessment with regard to the ascertainment of infringements of privacy are illustrated by an Italian case. In 1986 IBM was accused that its security system RACF represented an inadmissible control over employees.⁶

B. Economic Offenses

Since the 1970s, the discussion about computer misuse was not only marked by data protection crime but also by computer-related economic crimes, which today are regarded as the central area of computer crime and which were at first exclusively characterized by that term. In this field, the central offenses are those of computer manipulation, computer sabotage, computer extortion, hacking, computer espionage, as well as software piracy and other forms of product piracy.

1. Computer Manipulations

Computer manipulations were at the starting point of the discussion about computer-related economic offenses. During the time of the large mainframe computers, computer manipulations constituted a uniform group of crimes. Because of the diversification of computer systems in the 1980s, today the term computer manipulation describes a spectrum of different cases within the field of economic crimes.⁷

a) Among the "classic" large-scale computer manipulations, invoice manipulations concerning the payment of bills and salaries of industrial companies as well as the manipulations of account balances and balance sheets at banks are the predominant offenses. In the course of the recession of the last years, an extension of manipulations to increase the inventory could be perceived.

In Germany, a complicated invoice manipulation was committed as early as 1974 by a programmer who carried out salary manipulations of over 193,000 deutschmarks (DM) through changes of salary data as well as the book-keeping and balance sheet programs of his company.

Among the balance sheet manipulations, especially the case of the German Herstatt Bank of 1974 must be mentioned, in which balances totalling over one billion deutschmarks were manipulated.⁸

⁴ Cf. already John Stuart Mill, On Liberty, 1859; Popper, The Open Society and Its Enemies, 2 vol., 1945.

⁵ Cf. for this case van der Merwe, in: Sieber (editor), Information Technology Crime, 1994, p. 423.

⁶ Cf. for the last two cases Sieber, The International Handbook on Computer Crime, 1986, pp. 23 et seq.

⁷ For computer manipulations outside economic crime cf. infra I C.

⁸ Cf. for the last two cases Sieber, Computerkriminalität und Strafrecht, 2. ed. 1980, pp. 58 et seq., 61 et seq.

An example for a typical account balance manipulation is the terminal-input of a Japanese bank accountant who put in a deposit of 1,800 million yen and withdrew 50 million yen in cash and cheques amounting to 80 million yen from a subsidiary of the affected Sanwa-Bank in 1981.⁹

In 1994, a Russian group of offenders showed that these manipulations could also be carried out via data networks by external perpetrators. Operating from St. Petersburg, the group succeeded in making an American bank transfer over ten million dollars to them.¹⁰

b) Numerous *misuses of ATM-cards* and similar means of payment have been added to these "big" manipulations since the end of the eighties. Even though these misuses often lead only to small sums of damage, statistics show that the misuses of cards surpass the number of classic manipulations by far and meanwhile constitute the most frequent computer crime cases.¹¹ The protection of the respective cards - above all by chip technology - is gaining more importance in particular for the point-of-sales-systems, which are already common in Japan and which are being introduced in Europe at the moment. Suitable methods of protection are important especially because of the fact that meanwhile, the relevant classic credit card crimes are committed mostly by organized groups of criminals.

Today the forms of committing misuses of ATM-cards range from the simple use of stolen cards and the manipulation of cards with the help of computers to the independent manufacturing of card copies. Apart from the ATM-cards other magnetic cards are manipulated, e.g. phone cards or cards for horse betting.¹² The offenders get the PIN-code necessary for the use of the cards often by a phone call trick, by preparing the keyboard, by false keyboards or - as in a Japanese case - by bugging data telecommunication lines.¹³ A Hungarian case was particularly remarkable due to a high sum of damage. Within one month, the respective maximum amount of approx. 250 US \$ was withdrawn by the help of the copy of a single card in 1,583 cases.¹⁴

c) The *misuse of the telephone network*, in the field of which considerable qualitative changes have occurred in recent years, is currently also becoming a "mass crime": In the 1960s, offenders only wanted to avoid expenditures for their own phone calls. Since the end of the 1980s, the techniques originally developed by young hackers were also used by "companies" which - in often changing apartments or with the help of mobile telephones - offered conversations especially in intercontinental telecommunications. In the 1990s, even financial manipulations resulting in the transfer of money were made possible by the telephone companies when the insufficiently protected telephone network, which was not developed for this purpose, was used in an incautious way for the accounting of services.

Blue boxing was already developed in the sixties and is based on the fact that in the traditional analogous telephone network, control tones for establishing a link are transmitted through the same line as the information and can therefore be manipulated with the help of the so-called "blue box". By using a telephone number free of charge (in Germany a 0130-number), e.g., an operator of an American telephone company is called. Then the conversation is ended with the help of a "break tone" and the free line is held with the help of a "seize tone". After the input of certain control impulses it is possible to dial the desired number in the USA free of charge. However, especially as a consequence of installed frequency blockers,

⁹ Cf. for this case Yamaguchi, in: Sieber (editor), Information Technology Crime, 1994, p. 307.

¹⁰ Cf. for this (1995) "Datenschutzberater", vol. 10, p. 23.

¹¹ In Germany, the number of card misuses was five times bigger than the number of traditional manipulations in 1993, card misuses thus being responsible for more than two thirds of the computer crimes. In Japan, 1,081 cases of card misuses were counted in 1990 compared to 77 cases of other computer crimes. Cf. for this *Federal Criminal Agency* (ed.), Police Criminal Statistics of 1993, 1994, table appendix 01, sheet 10, code figure 5163 and 5175; as well as *Möhrenschlager* and *Yamaguchi*, in: *Sieber* (ed.), Information Technology Crime, 1994, p. 200 et seq., 305 et seq.

¹² Cf. Yamaguchi, in: Sieber (ed.), Information Technology Crime, 1994, p. 307.

¹³ Cf. for the Japanese case Yamaguchi, in: Sieber (ed.), Information Technology Crime, 1994, p. 307.

¹⁴ Cf. for this case Kertész / Pustazai, in: Sieber (ed.), Information Technology Crime, 1994, pp. 251 et seq.

the blue boxing technique now only works in a limited way, i.e. in telecommunications between certain countries only.

This is why young telephone hackers today predominantly use manipulation techniques which allow phone calls at the expense of other network participants. This is made possible by breaking into badly protected voice-mail-systems, the direct-dialing functions of which are exploited. A widespread form of manipulation is also the trade with foreign "calling card" numbers, which, e.g., are given away by insiders of the telephone companies, are obtained with the help of trick phone calls from the card holders, are "hacked" by intruding a computer or are found out by listening in on phone calls. Some of the phone calls are carried out at the expense of other users with the help of modified walkie-talkies or home-made devices.

Apart from that, phonecards for public phone-boxes are faked or manipulated. These manipulations can easily be effected in countries where only magnetic strip systems are used. In other countries as in, e.g., Germany, the telephone companies use phonecards with integrated chips which are especially secured against "recharging" by hardware protections. However, German youths are currently working on a copy of phonecards. They decode the signals of the cards with adapter cables and small computers and then simulate the signals with their own "intelligent" cards. According to reliable sources, the first successful "copying" of a phonecard with integrated chip which can be recharged after using it is said to have been completed in Germany in 1994. This card could therefore be used permanently.

Against the background of these forms of misuse one could foresee that the use of the telephone network for the accounting of services had to lead to a new wave of manipulations in the 1990s. In Germany, especially the "sex telephones" and "party lines" were used for this purpose, which can be called under the area code of 0190. Out of the 1.15 DM per minute to be paid to Deutsche Telekom, 52% remain with Deutsche Telekom whereas 48% go to the providers of the services (where they are divided between the provider of the service and the provider of the content); for foreign numbers, the revenue per minute amounts to over 3 DM. The perpetrators set up - partly with the help of specialized agencies corresponding service numbers which were then called at the expense of Deutsche Telekom and of some clients by young telephone hackers who shared the profits. In doing this, they used the whole range of possibilities of misuse described above. Moreover, Deutsche Telekom got harmed worst when whole private offices were rented for the exclusive purpose of calling chargeable service numbers during a twomonth period with the help of numerous (in a particular case up to 400) telephone connections and by using telephone computers before Deutsche Telekom claimed the outstanding invoices. Employees of Deutsche Telekom also misused telephone connections not yet given to clients by switching off the meter. Furthermore, clients of Deutsche Telekom were also charged when so-called "dialers" (i.e. electronic dialling machines, about the size of a cigarette box and distributed at 150 DM) were arbitrarily connected to some switchboxes, local telephone exchanges or wires, which called pre-programmed numbers especially at night at the expense of the affected telephone connection.

The first larger inquiries of telephone misuses were carried out in Germany in March 1994, when the apartments of 60 suspects were searched in nine German regions at the same time and four persons were arrested. In December 1994 and in January 1995 further searches were carried out at the request of the state attorney's office of Cologne (among others the head office of Deutsche Telekom at Bonn was searched) and some arrests because of financial manipulation in the field of service numbers were made. Two employees of Deutsche Telekom were arrested who are suspected of having collaborated with foreign organized groups of criminals. It is estimated that more than 80% of the turnovers off all sex-phones result from such manipulations. According to their own reports some youths obtained monthly commissions of more than 100,000 DM. The total damage for Deutsche Telekom and its harmed clients is estimated at more than 100 million DM for 1994.¹⁵

¹⁵ Cf. "DIE WELT" of March 19, 1994, p. 12., as well as "Frankfurter Allgemeine Zeitung (FAZ)" no. 289 of December 13, 1994, p. 22 and no. 5 of January 6, 1995, p. 4; "Focus" no. 50 of December 12, 1994, pp. 244 et seq. The German Telekom reacted to the shown cases with measures of public security of which the essential parts are individual invoicing, special warning reports in case of an increase of the telephone costs and the setting up of a center for network security in Darmstadt; cf. for this "Computer Zeitung", no. 3 of January 19, 1995, p.6.

2. Computer Sabotage and Computer Extortion

a) Today in the field of *computer sabotage*, a similar "popularization" as in the field of computer manipulations occurs: Beside the formerly predominant major cases of sabotage¹⁶ which only rarely appear in the today's statistics, there are massive damages to personal computers caused by virus programs and worm programs.¹⁷ These programs are spread especially through illegally copied software or in networks, and therefore constitute a considerable share of the total number of computer crimes.

Computer viruses are programs which spread in other programs of a computer system and - possibly with a delay of time - often cause damages. The number and the variety of viruses in circulation has increased in recent years. In some cases, the original software as issued by the producing company was already infected with a virus.

While viruses only spread in "host programs", worm programs attack foreign computer systems independently. Widely known became the "Internet-worm" of an American student, which blocked approx. 6,000 computers of the Internet network within a few days in 1988.¹⁸

The above mentioned merging of computer and telecommunication systems leads to the fact that acts of sabotage are increasingly being directed against telephone lines and other data lines. In the field of computer sabotage, the same development as in the sphere of the above mentioned manipulations and in the cases of hacking and espionage (which are to be examined in more detail below) is occurring.

The latest example for sabotage in the field of data lines is an attack on the network of Deutsche Telekom in February 1995: The offenders cut seven underground glass fibre cables and thus interrupted approx. 7000 telephone and data lines around Frankfurt/Main airport. In a letter a group called "Keine Verbindung e.V." claimed responsibility and declared that they had wanted to disturb the deportation of persons seeking political asylum.¹⁹

b) The cases of computer sabotage constitute a serious problem especially due to the fact that the economy, the administration and frequently also the individual citizen depend to a high degree on the functioning of modern computer and communication systems.²⁰ This dependency of the information society on computer systems makes *computer extortion* a dangerous form of attack. The victim is threatened with the destruction or the sabotage of his computer systems and data stocks.

An example for such a computer extortion is the case of an American scientist who distributed more than 20,000 floppy disks which supposedly contained information about the AIDS-virus, but encoded the user's hard disk when calling the stored programs. By a corresponding announcement on the screen, the users were asked to transfer an amount of at least 189 US \pm to a bank account in Panama in order to obtain the code for decoding the hard disk.²¹

¹⁶ In the German statustics of 1991, only 1-2% of all the cases of computer crime registered were cases of computer sabotage. Cf. Federal Criminal Agency (ed.), Police Criminal Statistics of 1993, 1994, table appendix 01, sheet 14, code figure 6742; and Möhrenschlager, in Sieber (ed.), Information Technology Crime, 1994, pp. 200 et seq.

¹⁷ In the Netherlands, statistics for computer viruses reveal that these cases of sabotage amount to almost a third of the total number of computer crimes. Cf. *Kaspersen*, in: *Sieber* (ed.), Information Technology Crime, 1994, p. 347 (with explanations about the groups of crimes on p. 345).

¹⁸ Cf. for this case Hafner / Markor , Cybe. punk, 1991, pp. 251 et seq.

¹⁹ Cf. for this "FAZ" No. 28 of February 2, 1995, p. 1 and No. 29 of February 3, 1995, p. 1.

²⁰ This dependency also leads to the high total damages which in different statistics are described as a consequence of computer breakdowns. Thus the total damage which occurred in Austria for private enterprises due to computer breakdowns in 1988 amounts to 1,500 million schilling, cf. Schick / Schmölzer, in: Sieber (cd.), Information Technology Crime, 1994, p.22. In France the corresponding total damage adds up to 10,400 million francs in 1991, of which 5,900 millions are caused by wilful damage actions, 2,700 millions are caused by accidents and 1,800 millions are caused by false operations and programmings, cf. Francillon, in: Sieber (cd.), Information Technology Crime, 1994, p.173.

²¹ Cf. for this case Kaspersen, in: Sieber (ed.), Information Technology Crime, 1994, pp. 351 et seq.

3. Computer Hacking

a) The term "computer hacking" traditionally describes the penetration into *computer systems*, which is not carried out with the aims of manipulation, sabotage or espionage, but for the pleasure of overcoming the technical security measures. In practice, this kind of offense can be frequently found.²² As far as damage is concerned, a differentiation must be made: In numerous cases, the attacked computer user is not actually harmed, but only endangered. Contrary to this, considerable damages occur in other cases especially when the perpetrators later use their knowledge for committing espionage and sabotage. In any case the "formal sphere of secrecy" or the integrity of the concerned computer systems is violated.

The most severe case of sophisticated *"hacking"* involved a group of German teenagers. They had managed to get access to various American computer systems and then sold the knowledge obtained in their data-journeys to the former Soviet secret service KGB. The case was discovered because one of the hackers sought help at the author's former Bayreuth chair, and a deal was agreed on with the prosecution authorities: The hacker revealed his knowledge and the investigation against him was suspended. The case was of particular interest because information on new lechniques of computer manipulation was revealed in the course of this proceeding.²³ The resolving of this case confirms the effectiveness of a *"self-revelation"* for cases of hacking already called for before.²⁴

b) Recent developments of telephone and telecommunications technology have led to the fact that nowadays, hacking does not only affect classic computer systems but increasingly also *telephone lines, answerphones and voice-mail-systems.* By using the "blue boxes" and signal devices described above, young "telephone hackers" dial themselves into the local telephone exchanges of the telephone company and are thus able to listen in on the digitally led conversations in the respective part of town.²⁵ In the US, besides other confidential information, especially the numbers of telephone access cards (so-called calling cards) are listened in on, which are then resold. The digital ISDN-network and the combination of telephone and computer technology will make new forms of crimes possible in future.

An example for the new form of telephone hacking is a 1992 case: Young Germans penetrated into the speech computer of the Barclays Bank in Hamburg to which the clients of the bank reported the receipt of their credit cards including the corresponding secret personal identification numbers as well as announcements in case of loss or - by giving the respective secret number - when asking for an increase of their credit limits.²⁶

4. Computer Espionage

a) Computer espionage - only rarely appearing in official statistics²⁷ - constitutes a special danger compared to classic economic espionage, because in computer systems, huge quantities of data are stored in an extremely narrow space, and the data can be copied quickly and easily with

 $^{^{22}}$ In a Dutch statistic of 1991, the cases of hacking amount to approx. one fifth of all computer crimes. Cf. *Kaspersen* in: *Sieber* (cd.), Information Technology Crime, 1994, p. 347 (with explanations about the groups of crimes on p. 345). The twilight zone of hacking is very large, because the respective attempts of getting access often cannot be registered and traced back.

²³ Cf. for this case Hafner / Markoff, Cyberpunk, 1991, pp. 139 et seq.

²⁴ Cf. Sieber, Informationstechnologie und Strafrechtsreform, 1985, pp. 54 et seq.

²⁵ Cf. "Focus" no. 17/1993, p. 106.

²⁶ Cf. "Der Spiegel" No. 34/1992, pp. 206 et seq.

²⁷ In the German statistics of 1991, 1% of the cases of computer crime can be assigned to computer espionage. Cf. *Möhrenschlager*, in: *Sieber* (ed.), Information Technology Crime, 1994, pp. 200 et seq.

the help of modern technology - also via data telecommunication. The objects of the offense are especially computer programs, data of research and defense, data of commercial accounting as well as addresses of clients. As the modus operandi, the simple copying of data is predominant; however, the theft of data carriers, the evaluation of ,,remaining data" or the absorbing of electromagnetic emissions are also effected. Besides young hackers and competing business enterprises, secret services appear which in recent years have increasingly been dealing with economic espionage. The case of the ,,KGB hacking" presented above illustrates the close connection between hacking and computer espionage.

A Japanese case from 1988 shows the possibility of using computer viruses for computer espionage: In this case, a computer virus penetrated into a network of personal computers, collected secret numbers of other network users and then wrote these numbers down on a "black board" of the network in an encoded form for the perpetrators.²⁸

b) With data processing and telecommunication growing together as well as with the digitalization of telecommunication, the line between traditional computer espionage and *telephone monitoring* becomes less clear. In the case of telephone tapping, the criminals today penetrate the telephone exchanges of the telephone companies especially via normal data lines. Car phones, directional radio stations and satellite connections are particularly easy to attack in case of uncoded communication.

In Germany, these techniques of bugging telephones were used especially by the State Security Service of the former GDR: The telephone numbers of politicians, of members of the secret service and of other important bearers of secrets of the Federal Republic were registered as target numbers, so that the telephone communications of these persons were automatically recorded.

Massive measures of listening in on telephone conversations are also carried out by the American National Security Agency (NSA). According to published reports, the NSA is said to run more than 2,000 installations for bugging telephones world-wide, which can supervise up to 54,000 telephone conversations at the same time.²⁹

5. Software Piracy and other Forms of Product Piracy

a) The unauthorized copying and use of foreign computer programs - often called theft of software or software piracy - at first involved, in accordance with the historic development of computer technology, the copying of *individual software* which frequently contains important internal company know-how. Therefore software theft overlaps with computer espionage in many cases.

The German ,,debit collection program case" is an example for the copying of individual software which led to the first decision of the Federal High Court of Justice concerning the possibility of copyright protection: Because of the copying of its central computer program and the following low-price sales by the perpetrator, the enterprise affected got into a situation that threatened its existence.³⁰

Standard software is sold on a massive scale today, and as far as the number of crimes is concerned, presently the predominant offense is the illegal copying of standard software especially for the use in personal computers. Just how wide-spread this phenomenon is can be shown by the fact that in Europe, on average only 0.5 computer programs are sold per personal computer in use.³¹ The industrial organisation "Business Software Alliance" estimates the market share of illegally copied software at, e.g., 40% in the USA, 76% in Germany, 81% in Japan and

²⁸ Cf. Yamaguchi, in: Sieber (ed.), Information Technology Crime, 1994, p. 307.

²⁹ Cf. García, 38 (1991) UCLA Law Review, pp. 1043 et seq. (at p.1055).

³⁰ Cf. Sieber, Computer und Recht 1986, pp. 699 et seq.

³¹ Cf. also Schick / Schmölzer, in: Sieber (ed.), Information Technology Crime, 1994, p. 30.

98% in Thailand.³² Therefore, the total damage of software piracy is - with a rising tendency - very high.³³

A German case from 1994 shows the high resulting damages and also illustrates the careless handling of security measures by program distributors and the proneness of new forms of distribution to misuse: During the biggest German computer fair, a software dealer had distributed 280,000 free copies of a CD-ROM, which contained programs worth more than 100,000 DM. Each program was protected by a code which should only be communicated to the CD-user in the case of concluding a contract. However, young hackers succeeded in "cracking" the code and the program protection of the CD-ROM.³⁴

Software piracy in the field of standard programs does not at all represent just a trivial offense of young PC-users. The software industry now increasingly takes legal action against enterprises that use unlicensed software. In these cases, often only a fraction of the installed programs is licensed. For example, during a police search at a company in northern Germany, the police found that only nine out of 58 installed programs were licensed.³⁵ In this case, 100,000 DM were paid for further licenses and compensation for damages.

In recent years, the distribution forms of software piracy have changed a lot: The illegal sale of computer programs that predominated in the eighties has been considerably reduced due to the corresponding prosecution practice in this field. By now, the predominating forms of distribution are the sale of programs in the so-called "ant trade" at flea markets (that is run and organized by gangs) as well as the proliferation of unauthorized copies via mailboxes (which in Germany partly operate online with more than 15 telephone connections at the same time).³⁶ Moreover, the practice of software piracy is characterized by dealers who produce and sell illegal copies of standard software in large numbers. This software is often distributed as an "extra" to the hardware.³⁷

b) The high value of data in the information society leads to the fact that besides the illegal use of computer programs, also *data banks* and other data collections are increasingly used illegally. Today the illegal copying of data (characterized as "downloading") affects both the hosts of online-data banks and the distributors of off-line-data banks.

In the field of culture, the merging of data processing and data communication as well as the digitalization in the *distribution of cultural products* (e.g. the sale of compact discs with music and films) show the common roots of software, music, video and multimedia piracy in the ,,informatized" society.³⁸ The connections between software piracy and other forms of product piracy become evident with the new devices for playing and producing compact discs which, in the age of ,,multimedia", contain computer programs, data banks, books, music and television films.

The unauthorized copying of *computer chip topographies* in the technical sector is another phenomenon to be mentioned.

³² Cf. "Newsweek" of June 29, 1992, pp. 44 et seq.

³³ E.g. in Austria, the total damage caused by software piracy (without damages caused by violations of semiconductor protection) is estimated at 3000 million schilling: Cf. Schick / Schmölzer, in: Sieber (ed.), Information Technology Crime, 1994, p. 30. In Canada, the losses caused by software piracy are estimated at 200 million dollars: Cf. Piragoff, in: Sieber (ed.), Information Technology Crime, 1994, p. 87. In Germany, the Union of the Software Indu:try estimates a business loss to the extent of 1.5 billion US \$ due to Far Eastern illegal copies; cf. "Handelsblatt" No. 2 of January 3, 1995, p.1. Therefore the share of software piracy in computer crime is very high: In Germany, it amounts to more than 10% in 1991 and to almost 10% in the Netherlands. Cf. for the corresponding statistics Möhrenschlager, in: Sieber (ed.), Information Technology Crime, 1994, pp. 200 et seq.; Kaspersen, loc. cit., p. 347 (with explanations about the groups of crimes on p. 345).

³⁴ Cf. for this von Gravenreuth, CR 1995, p. 122 (at p. 124).

³⁵ Cf. "Handelsblatt" of November 7th, 1994, p.16.

³⁶ Cf. von Gravenreuth, CR 1995, pp.122 et seq.

³⁷ Cf. for Canada Piragoff, in: Sieber (ed.), Information Technology Crime, 1994, p. 87.

³⁸ Cf. for this also Braun, Produktpiraterie, 1993, pp. 11 et seq., and CR 1994, pp. 726 et seq.

C. Communication Offenses

Today, computer crime does not only concern violations of privacy and property, but it is also directed against other objects of legal protection. In recent years, the first cases occurred in which *information glorifying violence or information of racist or pornographic content* was distributed with the help of computers.

In the USA, the Ku Klux Klan, the White Aryan Resistance, skinheads, and other neo-nazi organizations already realized in the eighties that it was much more effective to work with electronic communication than with traditional "newsletters". These groups used electronic communication systems mainly to distribute the names of Jewish, "opponents" and to give advice for the use of violence.

In Germany, right-wing extremist as well as left-wing extremist organizations first used mailboxes and other electronic communication systems at the beginning of the nineties. Right-wing extremist organizations especially used the so-called "Thule-Network", which consists of about 10 mailboxes. In these mailboxes, information about right-wing extremist organizations and corresponding propaganda material is stored. The electronic means of communication are used for the communication within private groups of users as well as for informing the public. Increasingly video games in which the user fights against foreigners and ethnic minorities serve as propaganda material for young people. In the video game "Concentration Camp-Manager" - currently distributed mostly via mailboxes - the player must decide immediately. Left-wing extremist groups (particularly from the anarchistic autonomous scene and from the sphere of the so-called Red Army Fraction) distribute their plans of action especially via the mailbox-network "Spinnennetz (cobweb)", which is included in an international exchange of information via the "European Counter Network (ECN)".³⁹

Law enforcement authorities presently face considerable problems in monitoring these electronic communication systems and in preventing the sale of the above mentioned video games mentioned above. First searches of mailboxes of the "Thule-Network" were carried out by the state criminal agencies of Baden-Württemberg and Hesse at the end of 1994.⁴⁰

The use of information services of the Internet for the dissemination of pornography and National Socialist propaganda was shown by preliminary investigations of the public prosecution authorities of Munich and Mannheim against CompuServe and other service-providers. In these proceedings, the main legal issue is if and to what extent service-providers are obliged to control the content of the data transferred by them.⁴¹

D. Other Offenses

Numerous other cases involve the use of computer technology in traditional crimes. E.g., the computer manipulations described above did not only serve the purpose of gaining pecuniary benefits, but were also used for *attacks on life* - as in the case of the manipulation of a flight control system or of a hospital computer. In the field of organized crime, too, the use of computers gains increasing importance.

An example for the spreading of computer crime in traditional fields of offenses is the manipulation of a British hacker, who in 1994 accessed the information system of a Liverpool hospital because he simply wanted to see "what mess can be caused with the computer". Among other things, he changed the medical

³⁹ Cf. Anti-Defamation League of B''hai B'rith, Hate Groups in America, 1988; Maegerle / Mletzko, Terrorism / Extremism / Organized Crime 1994, no. 5, pp. 1 et seq.; Federal Ministry of the Interior (ed.), Report of the Protection of the Constitution 1993, p.23, pp.147 et seq.; Möhrenschlager, in: Sieber (ed.), Information Technology Crime, 1994, p. 108; Werthebach, NWVBI, 1994, 201 (203); Response of the Parliamentary State Secretary Lintner of April 21, 1994 to questions of the Member of Parliament Böhm, Bundestagsdrucksache 127357; "PC Computing", December 1989, pp.146 et seq.; "Focus" No. 4/1995, pp. 52 et seq.; for the "Thule-Netz" cf. also CHIP no. 3/1994, pp. 82 et seq.

^{40 &}quot;Computer Zeitung" No. 46 of November 17, 1994, p. 20.

⁴¹ Cf. for this as well as for the service-providers' limited actual possibilities of control Sieber, JZ 1996, pp. 429 et seq., 494 et seq.

prescriptions for the patients: A nine-year-old patient who was "prescribed" a highly toxic mixture stayed alive only because a nurse re-checked the prescription.⁴²

In the meantime, the possibilities of computer sabotage have also been recognized in the military

sector. "Strategic Information Warfare" has become a form of potential warfare of its own.⁴³ The dependency of military systems on modern information systems became evident in 1995 when a "ligerteam" of the US Air Force succeeded in sending seven ships of the US Navy to a wrong destination due to manipulations via computer networks.

There is no need to point out possible manipulations in a nuclear power station in order to stress that meanwhile, computer misuse has become a global threat and that the security of modern computer systems has gained central significance for the information society of our days.

E. Summary

Summing up the previous development and especially the recent changes of computer crime, the introductory notion of an accelerated adaptation of crime to information technology is confirmed. Also in taking a look at future developments, three points must be emphasized:

- Today, computer and telecommunication technology have spread into nearly all areas of life. Thus new computer crimes have become possible. In future, this development will go even further: With the backing of the US Federal Government, the Internet is at present being built into an "information superhighway" where pieces of music and movies can be retrieved by private homes. Defense systems, nuclear power stations, traffic control systems and other control systems are increasingly being shaped by computer technology as well. The information society will thus depend even more on information technology. Computer crime has thus become more diverse and more dangerous.
- The computer, which in the 1950s and 1960s was still an exclusive ,,device of power" in the hands of the state or of particular enterprises, became available for every citizen because of the increase in performance and the corresponding price drop of personal computers. This led to changes both on the side of the criminal and on the side of the victim of computer offenses: Computer crimes can nowadays be committed by everybody. They also threaten just as the other dangers of the ,,risk society" every citizen.
- Electronic data processing as a consequence of a permanent "miniaturization" of its components - has grown together with telecommunication. Computer crimes are increasingly committed via telecommunication networks - also from abroad. New patterns of committing offenses developed, such as, e.g., telephone misuse, communication offenses or manipulations via the Internet. Computer crime has thus become more mobile and more international.

Because of this development, the security of computer systems and the prevention of computer misuse have become the central questions of today's information society. The following second part of this article analyzes how the law - and criminal law in particular - has taken up this challenge and how it has adapted to meet the latest developments.

⁴² Cf. for this case "Der Spiegel" No. 9/1994 of February 28, 1994, p. 243.

⁴³ Cf. Arquila / Ronfeldt, Cyberwar is Coming!, Comparative Strategy, vol. 12 (1993), pp. 141 et seq.; Molander / Riddile / Wilson, Strategic Information Warfare - A New Form of War, 1996 (edited by the National Defense Research Institute RAND, Santa Monica/Ca).

II. Legal Developments

In most industrialized countries, the law adapted to the new challenges of the information society by a multitude of new laws. However, throughout the world, the confusing diversity of the new legal regulations can be traced back to six groups of issues, which led to various reform waves: A first reform wave of the 1970s and 1980s concerned the protection of privacy (infra A). A second wave of reforms emerged at the beginning of the 1980s along with the fight against specific forms of economic crime committed with the help of computers (infra B). In the course of the 1980s, a third wave of reforms provided for numerous legal amendments improving the protection of intellectual property in the field of information technology (infra C). In the 1980s and 1990s, the first legislative measures were taken that were dealing with the fight against pornography and other communication offenses in computer networks. For the 1990s, we can perceive the beginning of another wave of reforms in the field of procedural law (infra E). A last body of issues - discussed in particular in the 1990s - concerns the setting-up of requirements for and prohibitions of security measures (infra F).

A. Protection of privacy

In numerous Western legal systems, the first "computer-specific" reforms of law during the 1970s and 1980s concerned the protection of personal rights and privacy in particular. The relevant legislation was a reaction to new challenges to privacy by the increasing possibilities of electronic data processing to gather, store, connect and transfer personal data. The traditional provisions for the protection of secrecy only covered part of the personality right and proved to be far too narrow for a protection against the new dangers.

A differentiation in criminal data protection law which can be found in all countries today results from this historic development: Traditional offenses for the protection of secrecy (e.g. for doctors, lawyers or public officials) can still be found in the core of criminal law, i.e. the Criminal Code. The general data protection laws - which were given rise to by the use of computers - contain criminal provisions that at first only referred to electronically stored data, but which have increasingly been extended to manually processed data in recent years as well. These general provisions are completed by data protection regulations for specific fields, which partly contain special criminal provisions, but which partly only refer to the criminal provisions in the general data protection laws. Personal data receive indirect criminal protection by general criminal provisions that are not limited to personal data.⁴⁴

In the federal system of the Federal Republic of Germany, the first state data protection statute came into force in Hesse in 1970; the other states followed soon after. The Federal Data Protection Act was passed in 1977 and was revised in 1990, extending the criminal provisions. Numerous regulations for specific fields followed, which applied the general principles of data protection law to special fields.

Statutes with important regulations for specific fields were, e.g., the Statistics Act,⁴⁵ the 10th Book of the Social Security Code⁴⁶ and the Framework Registration Act of 1980,⁴⁷ the new Population Census Act of

⁴⁴ Cf. esp. for hacking and for economic espionage infra II B.

⁴⁵ Act on the Statistics for Federal Purposes of 22 January 1987, Federal Law Gazette (BGBI.) 1, p. 462.

⁴⁶ 10th Book of the Social Security Code of 18 September 1980, BGBI, 1, p. 1469; amended by the 2nd Act for the Amendment of the Social Security Code (2, SGBÄndG) of April 26, 1994, BGBI, 1994 I, p.1229.

⁴⁷ Framework Registration Act of 16 August 1980, BGBI. I, p. 1429.

1987,⁴⁸ since 1989 several new Police Acts of the states,⁴⁹ in 1990 the Act Concerning the Federal Agency for the Protection of the Constitution and other laws on the secret services,⁵⁰ in 1991 the Data Protection Regulation on Postal Services, Postal Bank Services and Telecommunications⁵¹ as well as - also in 1991 - the Act Concerning the Documents of the Former East German State Security Service ("STASI").⁵² The Act Against Illegal Drug Trafficking and Other Forms of Organized Crime of 1992⁵³ as well as the Money Laundering Act of 1993⁵⁴ and the Crime Prevention Act of 1994⁵⁵ also contain specific data protection regulations. The "Census-Decision" of the Federal Constitutional Court of 1983 contributed more than anything else to this development, because it stated that any interference with the citizen's right to "informational self-determination" (which was for the first time acknowledged by the decision) required an explicit legal basis.⁵⁶

In other countries, there was a parallel development. Corresponding data protection statutes were mostly passed in the years 1977 to 1981, 1988 and 1992. We can therefore speak of an international wave of reform, which clearly shows the common problems of all national legal systems.

Regulations to mention are in particular those of Sweden of 1973, the US of 1974 (in a special statute), Denmark, France, Norway and Austria of 1978, Luxembourg of 1979, Iceland and Israel of 1981, Australia of 1982, San Marino of 1983, Great Britain of 1984, Canada of 1985, Finland of 1987, Ireland, Japan, and the Netherlands of 1988, Iceland of 1989, Slovenia of 1990, Portugal of 1991, Belgium, Switzerland, Spain, Slovakia and the Czech Republic as well as Hungary of 1992.⁵⁷

The harmonization of national laws was considerably strengthened by the activities of international organizations. Especially important are the Convention of the Council of Europe and the OECD-Guideline of 1980 as well as the UN-Guidelines and the draft EC-Directive of

- ⁵¹ Regulation about the Data Protection in Services of the German Mail Postal Service / Postal Bank / Telecommunications of 24 June 1991, BGB1. I, pp. 1385, 1387, 1390.
- ⁵² Act Concerning the Documents of the State Security Service of the Former GDR of 20 December 1991, BGBI. 1 p. 2272.
- ⁵³ Act Against Illegal Drug Trafficking and Other Forms of Organized Crime of 15 July 1992, BGBI. 1, p. 1302. Regulations on data protection are in particular contained in sections 98a, 98b, 98c of the Criminal Procedure Code, which were newly introduced by this law.
- ⁵⁴ Act on the Tracing of Financial Benefits from Serious Crime Money Laundering Act of October 25, 1993, BGBI. I, p. 1770.
- ⁵⁵ Act for the Amendment of the Criminal Code, the Criminal Procedural Code and Other Laws (Crime Prevention Act) of October 28, 1994, BGBI. 1994 1, p.3186. Especially sections 474 et. seq. of the Criminal Procedural Code which have been amended by this law contain regulations about data protection.
- ⁵⁶ Decisions of the Federal Constitutional Court (BVerfGE), Volume 65, pp. 1 et seq.

⁴⁸ Act on a Census of Population, Professions, Buildings, Housing and Workplaces (Population Census Act) of 8 November 1985, BGBI. 1, p. 2078.

⁴⁹ Cf. the First Draft for an Amendment of the Model Draft of a Uniform Police Act of the Federation and the Regions (VEME PolG) of 12 March 1986, sections 8a - d, printed in Kniesel / Vahle, Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder, 1990, pp. 4 et seq. Cf. also e.g. Saarland Police Act of 8 November 1989, Saarland Law Gazette (Amtsblatt) p. 1750 (there sections 25 to 40) or the Act about the Functions and Competences of the Bavarian State Police of 14 September 1990, Bavarian Law Gazette (GVBL) p. 397 (there articles 30 to 49).

⁵⁰ Cf. Act on the Cooperation of the Federation and the States in Matters of the Protection of the Constitution and through the Federal Agency for the Protection of the Constitution (Act on the Federal Agency for the Protection of the Constitution) of 20 December 1990, BGB1. I, p. 2954.

⁵⁷ For detailed information on these reform laws cf. the references in Sieber (ed.), Information Technology Crime, 1994, in particular on Belgium Spreuels (p. 63), on Canada Piragoff (p. 120 [fn. 127)), on Finland Pihlajamäki (pp. 157, 159, 165), on France Francillon (pp. 179 et seq.), on Great Britain Wasik (p. 499), on Hungary Kertész / Pusztai (pp. 252 et seq.), on Israel Lederman / Shapira (p. 264 [fn. 6]), on Japan Yamaguchi (p. 317), on Luxembourg Jaeger (p. 327 [fn. 11]), on the Netherlands Kaspersen (p. 358 [fn. 49]), on Portugal de Faria Costa (p. 396 [fn. 24], for the regulations in detail pp. 396 et seq.), on Sweden Jareborg (p. 443), on Switzerland Roth (p. 471 [fn. 59], for the regulations in detail pp. 471 et seq.), on the USA Wise (pp. 518 [fn. 49], 525 et seq.).

1990 respectively 1992.⁵⁸ A comparison of the different international activities and the national legislation shows that national laws were not passed *after* the international recommendations, but to a considerable degree *at the same time*. In other words: The recommendations and the guidelines of, most importantly, the European Council, the OECD and the UN were not so much effective because of their authority, but it was the exchange of thoughts and the cooperation of the competent representatives of the countries during the preparation of the recommendations that were decisive.⁵⁹

The analysis of the still existing differences between the national legal systems shows - in particular in criminal law - an important difference between the European and the Anglo-American data protection laws: Whereas Anglo-American law uses criminal provisions only reluctantly, European data protection laws also impose an accessory criminal sanction on most violations of provisions of purely civil and administrative nature. The classic ultima-ratio-function of criminal law and the requirements of certainty for blanket criminal provisions are strong arguments against the European concept. Europe therefore needs a decriminalization which limits criminal law to clearly determinable and grave violations of data protection. Corresponding resolutions were adopted during the AIDP-Colloquium on Computer Crime in Würzburg in 1992 and during the 15th International Conference on Criminal Law in Rio de Janeiro in 1994.⁶⁰

B. Economic Criminal Law

The second reform wave of computer-specific legislation developed at the beginning of the 1980s as a reaction to computer-related economic crime. Legal amendments became necessary because new forms of computer crime posed a threat not only to the traditional objects of criminal law protection, but also to intangible goods (e.g. bank deposit money or computer programs), and they were accompanied by new forms of committing the offense (e.g. computer manipulations instead of deceiving a human). In order to avoid an extension of the wording of already existing offenses, many countries passed new laws for the fight against computer-specific economic crime and also provided for new offenses for the prevention of unauthorized access to computer systems.

In Germany, the Second Act for the Prevention of Economic Crime of 1986 provided for reform measures in the most important areas of crime mentioned above: For the prevention of manipulations, sabotage and espionage, the relevant traditional objects of criminal protection were also protected against new, "technical" forms of violation. As a reaction to "hacking", the formal sphere of secrecy in the area of DP was acknowledged as a new object of legal protection, and the action of "unauthorized acquisition" of data was penalized.

In order to cover computer manipulations, the existing loopholes of punishability in the field of theft, embezzlement, fraud, defalcation and forgery of documents were closed by the two new offenses of

⁵⁸ Cf. the suggestions for an EC-Directive on Data Protection COM (90) 314 final - SYN 287 of 5 November 1990 and COM (92) 422 final - SYN 287 of 15 October 1992. On February 20, 1995 the Council of Ministers of the European Union agreed on a "common point of view" which still has to be approved by the European Parliament, cf. Handelsblatt, no. 37 of February 21, 1995, p.8; For the international activities cf. the summary in *Sieber*, The International Emergence of Criminal Information Law, 1992, pp. 82 et seq. and United Nations, International Review of Criminal Policy, no.43 and 44, 1994.

⁵⁹ Cf. for the effect of international recommendations and conventions - important for the doctrine of reception - Sieber, 103 ZS1W (1991) p. 961.

⁶⁰ This Würzburg Resolution Draft is printed in *Steber* (ed.) Information Technology Crime, 1994, pp. 627 et seq. (for data protection cf. pp. 630 et seq.).

computer fraud (section 263a Criminal Code) and the falsification of data of probative value (section 269 Criminal Code). For the prevention of sabotage actions, the offense of damage to property (section 303 Criminal Code) was completed by the offenses of alteration of data (section 303a Criminal Code) and computer sabotage (section 303b Criminal Code). The protection against economic espionage was shifted to an earlier stage by tightening section 17 of the Unfair Competition Act. Penetrating into foreign computer systems (so-called "hacking") was fought by the creation of a new provision against the spying of data (section 202a Criminal Code).⁶¹

The development in other countries was parallel. An "international wave of reform" emerged in particular from 1985 onwards.

Corresponding laws were passed in almost all States of the US since 1975, in different provinces of Australia in 1979, in Great Britain in 1981, in 1984 on federal level in the US, in Denmark and Canada in 1985, in Sweden in 1986, in Australia, Japan, Norway, and Austra in 1987, in the former GDR, in France and Greece in 1988, in Great Britain in 1990, in Finland, Portugal and Turkey in 1991, in Switzerland and Spain in 1992 as well as in France, Italy, and in the Netherlands in 1993.⁶²

Important contributions for achieving greater uniformity of law were made by the works of the OECD of 1985, of the Council of Europe of 1990 as well as of the EC, the UN and the AIDP of 1992.⁶³ In this context, too, an analysis of the procedure of reception shows that the recommendations of the international organizations were effective not just with their adoption, but already by the common consultations of the involved lawyers.

Today, the only important noticeable difference between the various national laws is that some countries - such as Japan and Austria⁶⁴ - do not have special criminal law provisions against hacking (i.e. the mere penetration into foreign computer systems). A corresponding criminal offense would be desirable in accordance with existing international recommendations.⁶⁵

⁶¹ Cf. in summary on the Second Act for the Prevention of Economic Crime Schlüchter, Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, 1987; Tiedemann, JZ 1986, pp. 868 et seq. Especially on the provisions in the field of computer crime cf. Möhrenschlager, wistra 1982, pp 201 et seq.

⁶² Cf. the references in Sieber (ed.), Information Technology Crime, 1994, in particular on Austria Schick / Schmölzer (pp. 24 et seq.), on Canada Piragaff (p. 92, fn. 23), on Finland Pihlajamäki (p. 157), on Great Britain Wasik (pp. 489, 493 et seq.), on Japan Yamaguchi (pp. 311 et seq.), on the Netherlands Kaspersen (pp. 359 et seq.), on Portugal de Faria Costa (p. 401, pp. 402 et seq.), on Turkey Erman (p. 483), and on the USA Wise (pp. 513 et seq., fn. 22, 23). For Switzerland now also cf. Schmid, Computer- sowie Check- and Kreditkarten-Kriminalität, Zurich 1994.

⁶³ Cf. for a summary Sieber, The International Emergence of Criminal Information Law, 1992, pp. 73 et seq.and United Nations, International Review of Criminal Policy, no. 43 and 44, 1994. For the initiatives of the EC, the UN and the AIDP during the Würzburg Conferences cf. Dersey (pp. 585 et seq.), Jescheck (pp. 623 et seq.), Kleinke / Purbach (pp. 661 et seq.), Marryn (pp.595 et seq.), Nilsson (pp. 575 et seq.), Openheimer (pp.655 et seq.), Piragoff (pp. 607 et seq.) and Woltring (pp.603 et seq.) in: Sieber (ed.), Information Technology Crime, 1994.

⁶⁴ In Austria, hacking is only punished - according to the respective circumstances - under the aspects of data protection (section 49 Data Protection Act) and alteration of data (section 126a Criminal Code), cf. Schick / Schmölzer, in: Sieber (ed.), Information Technology Crime, 1994, pp. 26 et seq. In Japan, hacking is, also after the criminal law reform of 1987, only punishable with regard to certain consequences of the offence, e.g. as obstruction of business according to section 234 subsection. 2 of the Japanese Criminal Code; cf. Yamaguchi, in: Sieber (ed.) Information Technology Crime, 1994, pp. 314 et seq.

⁶⁵ Apart from that, the use of abstract strict-liability offences for the prevention of computer viruses is increasingly being called for; cf. e.g. for Japan Yamaguchi, in: Sieber (ed.), Information Technology Crime, 1994, p. 316.

C. Protection of Intellectual Property

In the course of the 1980s, various legal amendments led to an improved protection of intellectual property in the field of information technology. After computer programs had been excluded from patent protection throughout the world in the 1970s, various countries at first passed new laws which assured a civil law copyright protection for these programs. At the same time, more severe provisions of criminal copyright law entered into force in numerous legal systems. Since 1984 additional laws for the protection of topographies of semiconductor chips were passed.

The historic development of German law clearly shows the reactions of the legislator which rapidly followed one another: In Germany, important laws for the prevention of software piracy were the Copyright Amendment Act of 1985,⁶⁶ the Second Act for the Prevention of Economic Crime of 1986,⁶⁷ the Victims Protection Act of 1986,⁶⁸ the Product Piracy Act of 1990⁶⁹ as well as the Second Copyright Amendment Act of 1993,⁷⁰ which was passed as a consequence of the EC-Directive of 1991. In most Western countries, the development was similar.

a) In many countries, the copyright protection by civil law was improved by legal clarifications. Corresponding reforms were carried out on the Philippines in 1972, in the US in 1980, in Hungary in 1983, in Australia, India, and Mexico in 1984, in France, Great Britain, and Japan in 1985, in Brazil, Canada, and Spain in 1987, in Denmark and Israel in 1988, in Columbia and Sweden in 1989, in Chile, Norway, and in former Czechoslovakia in 1990, in Finland in 1991, in Denmark, Great Britain, Italy, Norway, and Switzerland in 1992, and in Austria, Cyprus, Germany, Greece, and Sweden in 1993.⁷¹ Reform plans are currently being discussed in Belgium, France, the Netherlands, and Poland.⁷²

In the field of copyright protection by civil law, an analysis of national laws and of the activities of international organizations with respect to time shows that there has been an extension of copyright protection since 1984 which was not directed by international organizations. This development was triggered by the pressure of economic interest groups - supported by multinational corporations - in all industrialized countries. A further harmonization of copyright protection by civil law was then initiated by the EC-Directive on the Legal Protection for

- ⁶⁸ With the victim's right of access to records granted by section 406e Criminal Procedure Code, which is important for proving software violations. Cf. Victims Protection Act of 18 December 1986, BGB1. 1, p. 2496.
- ⁶⁹ With information rights, rights to destruction, seizure by customs authorities and different enhancements of ranges of punishment. Cf. Act for the Improvement of the Protection of Intellectual Property and for the Prevention of Product Piracy of 7 March 1990, BGBI. I, p. 422.
- ⁷⁰ With special provisions on computer programs in sections 69a 69g Copyright Act. Cf. Second Act for the Amendment of the Copyright Act of 9 June 1993, BGBI. 1, p. 910 and Dreier, GRUR 1993, pp. 781 et seq.
- ⁷¹ Cf. the references in Sieber (ed.), Information Technology Crime, 1994, in particular on Brazil de Araujo Jr. (p. 71, 76), on Canada Piragoff (p. 110 [fn. 98]), on Chile Kunsemuller (p. 133), on Finland Pihlajamäki (p. 157), on France Francillon (p. 181.), on Israel Lederman / Shapira (p. 279), on Sweden Jareborg (p. 444), on Switzerland Roth (p. 461, 467), and on the USA Wise (p. 518).
- ⁷² Cf. the discussion of the drafts in Sieber (ed.), Information Technology Crime, 1994, in particular on Belgium Spreutels (p. 58) and on Poland Buchala (p. 378).

⁶⁶ With the introduction of "computer programs" in the catalogue of protected works of section 2 subsection 1 Copyright Act and the aggravation of the section 108 Copyright Act. Cf. Act for the Amendment of Provisions in the Field of Copyright Law of 24 June 1985, BGBI. 1, p. 1137.

⁶⁷ With the aggravation of section 17 Unfair Competition Act and the criminal provision of section 202a Criminal Code, which is now also discussed in the context of "decompiling" source codes of programs. Cf. Second Act for the Prevention of Economic Crime of 15 May 1986, BGB1. 1, p. 721.

Computer Programs in 1991.⁷³ Detailed suggestions for supplementing the Berne Convention are currently being discussed.⁷⁴

b) An international tightening of *criminal* copyright law can be observed in a number of countries since 1981.

Reforms to mention are in particular those in Italy of 1981, in Great Britain of 1982, in Sweden and in the US of 1982, in Finland of 1984, in, Denmark and France of 1985, in Canada of 1987, in Great Britain of 1988, in Hungary of 1992.⁷⁵

This tightening of criminal law was not so much based on the activities of international organizations, but on the new need for protection in the information society, which brought about - against the background of a changed Zeitgeist - an improved protection of intellectual property by criminal law.

c) The development concerning the legal protection of topographies was different. The EC-Directive on Legal Protection for Topographies of 1986 - influenced by American pressure forced the Member States of the European Community to rapidly pass corresponding laws. American "pressure" that was exerted by a strong requirement of mutuality in the American Semiconductor Chip Act was effective in other countries, too.

Corresponding laws were passed in the US in 1984, in Japan in 1985, in Sweden in 1986, in Denmark, France, Germany, Great Britain, Japan, and the Netherlands in 1987, in Austria and Spain in 1988, in Australia, Italy, and Portugal in 1989, in Belgium and Canada in 1990, in Finland and Hungary in 1991.⁷⁶

The passing of semiconductor chip laws in the Member States of the European Union after 1986 shows that the possibility of the European Community to pass binding directives leads to a new age of legal harmonization and a *ius commune* in Europe.⁷⁷

d) The same development could also be shown in the field of general product piracy. In the future, a further harmonization and extension of legal protection will also be achieved by the EC-Directive for the Legal Protection of Data Banks that was passed in 1996⁷⁸ and does not have to be discussed in detail at this point. The changes presented above have already illustrated the major lines of reform: The protection of intellectual property both by civil law and by criminal law was extended considerably in the whole world during the last decade. In this field, the law has reacted to the shift from the industrial to the information society in a remarkable manner.

⁷³ Cf. OJ 1991 No. L 122/42 of 17 May 1991. For a summary of the international initiatives cf. Sieber, The International Emergence of Criminal Information Law, 1992, pp. 73 et seq.

⁷⁴ Cf. WIPO Doc. No. BCP/CE/III/2-1 of 12 March 1993, Committee of Experts on a Possible Protocol to the Berne-Convention-Memorandum, pp. 2 et seq., the wording of the "Agreement on Trade-Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit foods" (TRIPS-Agreement) of the WTO is printed in the International Review of Industrial Property and Copyright Law (IIC) 1994, pp. 209 et seq. (cf. in so far especially art. 10).

⁷⁵ Cf. in detail the references in Sieber (ed.), Information Technology Crime, 1994, in particular on Great Britain Wasik (p. 499) and on Hungary Kertész/Pusztai (p. 254). For a summary - also on the international activities - cf. Sieber, The International Emergence of Criminal Information Law, 1992, pp. 76 et seq.

⁷⁶ Cf. in detail the references in Sieber (ed.), Information Technology Crime, 1994, in particular on Austria Schick/Schmölzer (p. 30 [fn. 56]), on Canada Piragaff (p. 110 [fn. 99]), on Finland Pihlajamäki (p. 157), on Italy Lanzi (p. 300 [fn. 3]), and on the Netherlands Kaspersen (p. 346 [fn. 12]).

⁷⁷ Cf. Coing, NJW 1990, p. 937.

⁷⁸ Cf. EC-Directive 96/9 of the European Parliament and Council on the Legal Protection of Data Banks of 11 March 1996, O.J. no. 77/20 of 27 March 1996.

D. Communication Offenses

At the end of the 1980s and in the 1990s, a new complex of issues surfaced in the field of substantial law. The dissemination of pornography, racist statements as well as information glorifying violence, in particular via the Internet, raised the question as to what extent these offenses could be confronted with the help of criminal law. For that purpose, two legal issues have to be distinguished: a) the first one concerns the criminal liability of the *author* of the respective statements, and b) the second one is about the additional liability of the *service-provider*⁷⁹ whose networks and servers are abused by third persons.

a) The general criminal liability of the author of pornographic and racist statements is regulated differently in the individual legal regimes. Whereas, e.g., in Germany, the use of symbols of National Socialist organizations is punished under section 86a German Criminal Code, the US lacks a corresponding criminal provision. With respect to the Internet, there is the additional problem that the general criminal offenses of the national legal regimes partly require a dissemination of these statements by "publications" which are defined as corporeal objects. In order to be able to apply the traditional criminal law provisions to new media, the German legislator added a subsection 3 to section 11 German Criminal Code in 1974, which states that "sound and image carriers, depictions and other representations" shall be deemed "publications" if this subsection is referred to in another criminal law provision.⁸⁰ For the near future, another extension of the term "publication" in section 11 subsection 3 German Criminal Code is planned with regard to the new information and communication services.⁸¹

In many other legal systems, the situation is similar, partly because of the interpretation of traditional criminal law provisions by the courts,⁸² partly because of new legal regulations.⁸³

b) The criminal liability of the author of such statements must be distinguished from the issue of an additional co-liability of service-providers for the statements disseminated via their computer systems and data networks. In Germany, the latter question is currently being examined in the course of various criminal investigations, in particular by the public prosecution authorities of Munich and Mannheim.⁸⁴ Legal literature mostly denies a co-liability of the service-provider because the service-provider can only be accused of not exercising a sufficient amount of control: However, a ("guarantor's") duty to control the content of the networks does not exist under criminal law.⁸⁵ In Germany, a solution of this issue is currently under consideration (on the federal level) in the draft "Information and Communication Services Act" and (by the Länder) in

⁷⁹ The service-provider offers access to the network and special services at the same time, cf. Sieber, JZ 1996, p. 434/435.

⁸⁰ References can be found in sections 74d, 80a, 86, 86a, 90, 90a, 90b, 103, 111, 131, 140, 165, 166, 184, 186, 187, 187a, 194, 200, 219b German Criminal Code (Strafgesetzbuch - StGB).

⁸¹ Cf. Sieber, JZ 1996, p. 495, as well as the draft of the "Federal Bill for the Regulation of the Basic Conditions for Information and Communication Services (Information and Communication Services Act - luKDG), published by the Federal Ministry for Education, Science, Research and Technology on 6 June 1996.

⁸² E.g. in the Netherlands and Spain, cf. the articles in Sieber (ed.), supra (fn.3), in particular for the Netherlands Kaspersen (p. 350), and for Spain Gutierrez Francés (S. 436).

⁸³ Reform laws can be found in Finland, Greece, Israel, Japan and Canada; cf. the articles in: Sieber (ed.), supra (fn. 3), in particular for Finland Pihlajamäki (p. 158), for Greece Vassilaki (p. 244), for Israel Ledermann/Shapira (P. 282), for Japan Yamaguchi (p. 312) and for Canada Piragaff (p. 90).

⁸⁴ Especially the preliminary investigation against the US company CompuServe Inc. caused international attention, because the blocking of the news-groups the Munich prosecutor's office had complained about had a world-wide impact. In the US, the company was accused of censorship measures, of violations of the freedom of speech and the freedom of the press as well as of "bowing" before German authorities.

⁸⁵ Cf. for a summary Sieber, JZ 1996, pp. 429 et seq., 494 et seq.

the "Convention on Media Services". In this context, the Federal Government attributes particular importance to a voluntary self-control by the content-providers and network-operators.⁸⁶

In other countries, also an even further-reaching liability of the service-provider is supported, partly on the basis of an interpretation of existing laws, partly on the basis of new legal regulations. A corresponding liability on the basis of traditional criminal law provisions exists, e.g., in Switzerland, if the service-provider obtains knowledge of the existence of illegal content in his network and, nevertheless, does not deny access to such content.⁸⁷ In the US, a statute-based criminal liability was introduced with the "Communications Decency Act" of 1996.⁸⁸ The incompatibility of the CDA with the fundamental right of freedom of speech (1st Amendment to the American Constitution) has just recently been determined by a US federal court.

c) An international standardization of "communication offenses" and the liability of serviceproviders has not occurred so far. However, such standardization would be essential to prevent service-providers from relocating to so-called "oasis countries" and thus creating "computer crime havens" as well as distortions of competition. Therefore, initiatives of the European Union, the Council of Europe, the OECD, the G7 countries or the United Nations are needed.

E. Criminal Procedural Law

Another current reform wave concerns procedural law. The subject of these reforms is, however, not limited to procedural problems of computer crime only. Mostly on the occasion of investigations into white collar crime, prosecuting authorities have to analyse computer-stored book-keeping data. In addition to this, perpetrators in the field of organized crime increasingly make use of computer systems and transfer data to computers abroad via telecommunication networks in order to render access more difficult for the prosecution authorities. Therefore, the use of computers in almost all areas of life frequently confronts prosecution authorities with computer-stored means of evidence, even on the occasion of investigations into "classic" forms of crime.

Legal problems mainly occur in the areas of statutory powers of prosecuting authorities and the corresponding passive duties of witnesses. In many countries, problems exist with the questions of whether and to what extent prosecuting authorities have the right to search computer systems, to seize data, to intercept and record telecommunication between computers, to have access to telecommunication data and to electronically supervise computers. A particular problem represents the access to data which are stored at another location, possibly even abroad, in a telecommunication network that branches out in all directions.⁸⁹

⁸⁶ Cf. for this the home-page of the Federal Ministry for Education, Science, Research and Technology at "http://www.kp.dlr.de/BMBF/rahmen/eckwerte_bmbf.html".

⁸⁷ Cf. for this the decision of the Swiss Federal Court in: BGE 121, 1995, IV, 109, with a consenting review by Widmer / Bähler, CR 1996, 178.

The text of the Act can be retrieved on the Internet at "http://www.eff.org/pub/Alerts/s652_hr1555_96_draft_bill.excerpt".

⁸⁹ Cf. for these powers of access in different countries the articles in Sieber (ed.), Information Technology Crime, 1994, in particular on Germany Möhrenschlager (pp. 226 et seq.), on Finland Pihlajamäki (p. 167), on Greece Vassilaki (pp. 246 et seq.), on Great Britain Wasik (p. 502), on Hungary Kertész / Pusztai (p. 259), on Israel Lederman / Shapira (pp. 292 et seq.), on Japan Yamaguchi (p. 319), on Luxembourg Jaeger (pp. 334 et seq., 338 et seq.), on Switzerland Roth (p. 471), on (pp. 367, 371), on Poland Buchala (p. 384), on South Africa van der Merwe (p. 425), on Switzerland Roth (p. 471), on

- As to the duties of witnesses to active cooperation, it is questionable whether a user of a computer is already obliged to provide a printout of encrypted data by the "traditional" duties of witnesses or whether a new statutory power in criminal procedural law is needed for this purpose.⁹⁰
- Additional problems are those of data protection in criminal procedure⁹¹ and mainly in Anglo-American law - rules of evidence concerning the admissibility of computer data in court.⁹² Further problems are the applicability of national criminal law for offenses in international data networks as well as the national borders for investigative actions.⁹³

Corresponding reform laws were therefore enacted in several countries since 1984. On the international level, a work-group of the European Council has dealt with these questions.⁹⁴ Hence, the development of this fourth reform wave of computer-related criminal law reforms has not finished yet, but has only just begun.

Reform laws in this field were enacted in Great Britain in 1984, in Denmark in 1985, in the United States in 1986, in Canada in 1988, in Germany in 1989, and in the Netherlands in 1993.⁹⁵ Most of the cited laws introduced new procedural powers for the prosecuting authorities, but there is a lack of thorough consideration and of a uniform dogmatic concept also with regard to legal policy. This lack may result in serious disturbances of the complicated balance between the necessary powers of intervention of the prosecuting authorities on the one hand and civil liberties on the other hand.

F. Legal Regulations on Protection Measures

The possibility of manipulations in data networks has led to the additional question as to what extent legal regulations on security measures are necessary. Three different questions must be distinguished: (a) duties to implement protection measures, (b) prohibitions of certain protection measures, and c) consequences of possible manipulations for the use of electronic contracts.

a) A general *duty to implement safeguard measures* for the protection of data processing systems does not exist for the private sector (unlike the situation in the public sector). In a free society and market economy, the individual citizens are free to decide whether they want to protect their individual interests or at least their computer systems by costly measures or whether they are ready to accept the risk of an "electronic burglary".

Tunisia Ben Halima (pp. 479 et seq.), and on the USA Wise (p. 527). Also cf. in detail for the legal situation in Germany Bär, Der Zugriff auf Computerdaten im Strafverfahren, 1992.

⁹¹ For the corresponding questions of data protection cf. the articles in Sieber (ed.), Information Technology Crime, 1994, in particular on Belgium Spreutels (p. 65), on Germany Möhrenschlager (pp. 226, 230), on France Francillon (pp. 189-192), on Hungary Kertész / Pusztai (p. 256), and on Luxembourg Jaeger (pp. 334 et seq.).

⁹² For the admissibility of computer printouts cf. the articles in Sieber (ed.), Information Technology Crime, 1994, in particular on Canada Piragoff (p. 126), on former Czechoslovakia Nett (p. 151), on Germany Möhrenschlager (p. 228), and on South Africa van der Merwe (p. 425).

- 93 Cf. Sieber, in: Cheswick / Bellovin, Firewalls und Sicherheit im Internet, pp. 302 et seq. (1995).
- ⁹⁴ Cf. Sieber, The International Emergence of Criminal Information Law, 1992, p. 94 and Council of Europe, Doc. No. PC-PC (92) 5, European Committee on Crime Problems (CDPC), Committee of Experts on Procedural Law Problems Connected with Computer-Related Crime (PC-PC), Summary Report of 18-20 May 1994.
- 95 Cf. the articles in Sieber (ed.), Information Technology Crime, 1994, in particular on Canada Piragoff (pp. 122 et seq.), on the Netherlands Kaspersen (pp. 366 et seq.), on the USA Wise (p. 527 [fn. 104]).

⁹⁰ Cf. for the legal situation in the different countries the articles in Sieber (ed.), Information Technology Crime, 1994, in particular on Canada Piragoff (p. 124), on Chile Kunsemuller (p. 140), on Germany Möhrenschlager (pp. 228 et seq.), on Greece Vassilaki (p. 247), on Hungary Kertész / Pusziai (p. 249), on Japan Yamaguchi (p. 319), on Luxembourg Jaeger (pp. 338 et seq.), on the Netherlands Kaspersen (pp. 367 et seq.), on Poland Buchala (p. 385), on Switzerland Roth (p. 471), on Tunisia Ben Halima (p. 479), on Turkey Erman (p. 487), and on the USA Wise (p. 527).

However, this principle is not valid if the lack of safeguard measures does not only lead to the infringement of interests of the respective computer user, but also infringes the interests of third parties. In these cases, the legislator demands adequate measures for the protection of these persons (who in most cases cannot decide themselves about the implementation of safeguard measures) and for the protection of general interests (e.g. the interest of a functioning network). Such duties exist above all for companies that process personal data of third parties, e.g., insurance companies or credit inquiry agencies. In so far, reference can be made to the general explanations above concerning the field of data protection (criminal) law.⁹⁶ In Germany, there are in particular specific provisions for the respective fields, e.g., for the protection of telecommunications secrecy (section 10a subs. 1 Telecommunications Installations Act),⁹⁷ for the protection 2a Telecommunications Installations Act) and for the secrecy of the telecommunications supervision (section 12a Telecommunications Act and the new Telecommunications Services Companies Data Protection Ordinance.

The development in other countries was parallel as far as the general provisions of data protection law are concerned.⁹⁹ Comparative analyses and an international co-ordination are still lacking for specific regulations in the respective fields. Starting in the middle of 1996, the author is going to carry out a research project on behalf of the EC Commission, which will be dealing with these questions.

b) *Prohibitions of security measures* can serve the protection of public interests on the one hand and the protection of third party interests on the other hand: General prohibitions of security measures for the protection of public interests are discussed in particular in the field of cryptography in order to allow law enforcement authorities and secret services to listen in on data communication. In Germany, however, there has not been any general prohibition to use cryptography-software so far. However, the export of encoding programs to non-EU countries is subject to a duty of authorization under the EC-Regulation on "dual use" goods, which is in force in all EU member states since July 1st, 1995.¹⁰⁰ In the US, encryption has not been regulated so far either, and is moreover discussed controversially. However, the export of encoding technologies also requires a public license.¹⁰¹ Contrary to that, encoding programs may in general not be used in China, France and Russia without public authorization.¹⁰² A group of experts of the European Community is currently dealing with a co-ordination of the relevant questions.

These prohibitory provisions protecting the public interests must be distinguished from the ban of supervisory measures in the interest of third parties. Such provisions must in particular be considered if personal activities of internal or external users of a computer system are recorded for safety reasons. The scope of relevant cases ranges from the recording of attempts to get

97 BGBI. 1994 I, pp. 2363 et seq.

100 Cf. for this Kuner, NJW-CoR 1995, 413, 414.

⁹⁶ Cf. above II.A.

⁹⁸ BGB1. 1995 I, p. 722.

⁹⁹ Cf. the summary by Sieber, in Cheswick / Bellovin (ed.), supra (fn. 93), pp. 309 et seq.

¹⁰¹ However, this license is issued only for "keys" up to 40 bits. Because this practice encounters heavy opposition due to safety considerations, licenses are to be issued for "keys" up to 80 bits in the future. In exchange the producers have the duty to deposit the "keys" at an independent body which is obliged to provide the "keys" to certain authorities on a court order; to be read on the Internet at "http://www.zdnet.com/intweek/daily/960518y.html". Cf. in this context the references in Kuner, NJW-CoR 1995, 413, 415 concerning the discussion about the introduction of a "Clipper-Chip".

¹⁰² Cf. Kuner, NJW-CoR 1995, pp. 413 et seq.

unauthorized access to a computer, via the recording of connection data at the router, to the content supervision of discussion forums and electronic mail. In Germany, the respective supervision measures are not covered by the provisions of the Criminal Code, but only by general and specific data protection laws. Specific German regulations can mainly be found in section 14a Telecommunications Installations Act, in the Deutsche Telekom Data Protection Ordinance¹⁰³ and in sections 3 et seq. Telecommunications Services Companies Data Protection Ordinance.¹⁰⁴ Comparative studies as well as an international co-ordination are still lacking in this field.

c) The manipulation possibilities described above lead to the additional question as to what extent *contracts* concluded via data networks should be recognized. In practice, the use of digital, encoded signatures tries to safeguard that a document originates from a certain person (authentication) and that it cannot be falsified.¹⁰⁵ Legal regulations concerning certain encoding procedures do not exist in Germany at the moment.¹⁰⁶ However, the Federal Government wants to establish harmonized security criteria together with the groups of industry concerned. An adaptation of the Civil Code is being examined. Issues to be addressed are in particular whether the stringent formal requirements of civil law (conclusion of written contracts) are still reasonable for modern transactions or whether paperless transactions make special legal regulations necessary. Comparative studies do not exist for the relevant questions. On the supranational level, the European Commission has proposed a directive on consumer protection in the conclusion of contracts via a distance. For specific contracts on the exchange of goods and services, it is planned to allow the consumer to withdraw from the contract within a minimum delay of seven days.¹⁰⁷

G. Summary

The development in the areas discussed above can largely be summarized by the following three statements:

- The legislator reacted rapidly in four waves of computer-related reforms to the new forms of information technology crime. These law reforms also included mainly in the area of data protection and copyright protection of computer programs measures belonging to administrative law and to civil law. However, the emphasis of legal reactions for the prevention of computer crime was put on criminal law.¹⁰⁸
- The reactions of the legislators were similar in most Western countries. International
 organizations especially the OECD, the European Council, the EC, the WIPO and the
 AIDP supported the national law reforms from the beginning and created a high level of

¹⁰³ BGB1. 1991 I, p. 1390.

¹⁰⁴ BGB1. 1991, p. 2337; cf. Sieber, in: Cheswick / Bellovin (ed.), supra. (fn. 93), pp. 313 et seq.

¹⁰⁵ The most commonly used cryptographic process at the moment is the Rivest-Shamir-Adleman (RSA)-Process; cf. for this Cheswick / Bellovin (ed.), supra (fn. 93) p. 259/260; Witte, CR 1993, 243, 244.

¹⁰⁶ Cf. for the current legal situation Sieber, in: Cheswick / Bellovin, supra (fn. 93) pp. 139 et seq.

¹⁰⁷ Cf. for the whole the Internet address in fn. 86.

¹⁰⁸ Most of the enacted criminal law aggravations were justified by the new challenges of information technology. A clear over-criminalization is so far only to be found in the field of data protection. Beyond this, a future over-criminalization is also possible due to a creation of abstract strict-liability offenses regarding computer viruses and following an enactment of new investigative powers for law enforcement agencies under criminal procedural law.

harmonization. Pressure by industry - which was effective all around the world - also contributed to this legal harmonization.

The legislator solved the emerging problems rapidly, but in an ,,ad hoc" manner and in an isolated way. Basic considerations about the function of criminal law in the information society and about the connections between the particular law reforms hardly took place.

III. Paradigm-Shifts and Perspectives

The preceding analysis of the most important offenses and of the legal problems of computer crime has shown a wide range of different problems which were all caused by computer technology, but which were solved in legal practice without a solid basic concept. The scientist cannot be satisfied with this pragmatic handling of singular questions. The sum of individual cases and questions makes him ask for the underlying powers, the change of paradigms, and the prospects which are analyzed in the last part of this article.

This last part mainly deals with three fundamental changes: the development from the industrial to the information society and the resulting information law (infra A), the developing risk society and the ensuing changes of criminal law (infra B), as well as the loss of importance of national borders and the international harmonization of law (infra C).

A. Information Society and Information Law

1. Social Changes

The most important power underlying the illustrated changes is the present development from the industrial to the information society. This development has rightly been called a "second industrial revolution" by economists and sociologists. While the characteristic of the first industrial revolution during the 19th and 20th century was the replacement of manpower by machines, the characteristic of this second phase of industrial development consists in the shifting of human intellectual activity to machines. The economic and social effects of this new development will, therefore, surpass the changes caused by the first industrial revolution by far. This development to an information society is especially characterized by the fact that beside material objects, immaterial assets like, e.g., deposit money, copyrights, business secrets and other forms of know-how increasingly gain importance. Information has not only become a new value, but a factor of power and a potential danger.

2. Consequences in the Legal System

The analysis of the existing reform laws in the second part of this article has shown that this social change of paradigms¹⁰⁹ - from material to immaterial values - has already reached criminal law. However, a general theory referring to the protection of information is still missing.¹¹⁰

¹⁰⁹ Cf. for the term " Change of Paradigms" in science Kuhn, The structure of Scientific Revolutions, 1962.

¹¹⁰ The respective regulations are often developed in analogy to the protection of material objects without sufficiently taking into account the particularities of immaterial goods.

For this reason, the theory of "information law" or "law of information technology" developed in the author's inaugural lecture at the University of Bayreuth¹¹¹ outlines a general theory concerning the legal status of information and takes these changes into account. In accordance with the findings of cybernetics and computer science, this theory evaluates information as a third basic element next to matter and energy:¹¹² Information is a new economic, cultural, and political good, but it also creates a special potential danger. The new theory of "law of information technology" realizes that the modern information technology increases the significance of information: Information becomes an active factor which causes changes in automatic data processing systems without any human involvement; systems of information technology replace human decisions.

This new aspect of ,,(criminal) information law" shows in particular that the legal assessment of material and immaterial goods must be different.

- A first aspect deals with the protection of the "proprietor" or "possessor" of material or immaterial goods. In contrast to corporeal objects which, as a rule, are exclusively assigned to certain persons, information is rather a "public good" which, in an open society, must flow freely and must therefore not be protected by rights that exclude all others. These basic principles of "freedom of information" and "unrestrained flow of information" are an essential prerequisite for a free economic and political system.¹¹³
- Another particularity of the legal assessment of immaterial goods follows from the fact that protection of information must not only take into account the economic interests of the proprietor, but at the same time also the interests of those who are concerned by the content of the piece of information. The new requirements for the protection of privacy in the field of electronic data processing resulted from this aspect of information which does not exist with regard to material objects.
- With the increasing importance of information, rights giving access to information gain significance - not only for criminal prosecution authorities but also (e.g. in data protection law) for the citizen (so-called "access to information rights").¹¹⁴ Thus, it becomes obvious that legal rules for information cannot be developed by way of analogy from provisions on corporeal objects, but that they need their own independent basis and theory.

For *criminal* information law, the consequences of this general theory are evident: A limited protection of the creator of information, the protection of the citizen concerned by information, as well as the access to information are also to be guaranteed by criminal law - in so far as other measures are not sufficient. "Intellectual property", "privacy" and "access to information rights" describe the new objects of legal protection, which have not only provided the basis for the previous reform legislation, but which can, in the information society of the 20th century, rightly claim protection by criminal law as well.

¹¹¹ Cf. Sieber, Informationsrecht und Recht der Informationstechnik, NJW 1989, pp. 2569 et seq.

¹¹² Cf. N. Wiener, quoted after Steinbuch, GRUR 1987, pp. 579 et seq. (at p. 581): "Information is information, not matter or energy. Any materialism which does not admit this can survive at the present day".

¹¹³ Cf. John Stuart Mill, On Liberty, 1859; Popper, The Open Society and Its Enemies, 2 volumes, 1945.

¹¹⁴ Cf. for the access to information rights in the different countries the articles in Sieber (ed.), Information Technology Crime, 1994, especially for Brazil de Araujo Jr. (pp. 82 et seq.), for Canada Piragoff (p. 120), for Germany Möhrenschlager (p. 212), for Hungary Kertész / Pusztai (p. 253), for Italy Lanzi (p. 301), for Luxembourg Jaeger (p. 332), for the Netherlands Kaspersen (p. 359), for Romania Antoniu (p. 416), for Spain Gutiérrez Francés (p. 439), for Tunisia Ben Halima (p. 477), and for Turkey Erman (pp. 484 et seq.). Cf. for the German legal situation Lodde, Die Informationsrechte des Bürgers gegen den Staat, 1995.

B. Risk Society and Changed Risk Control

1. Social Changes

The increasing significance of information in the post-industrial information society described above is mainly caused by the development and expansion of information *technology*. The development of the *technological* society and of *technology* law is, therefore, the second major force of change behind the singular questions analyzed above. Since the 1980s, sociologists and lawyers have been discussing the social impact of modern technology under the term of "risk society".¹¹⁵ A presentation of this academic discussion must, therefore, necessarily precede an analysis of how far the ascertained changes of *general* technology are valid also in the field of *information* technology.

Since the eighties, the discussion about the risk society in Western countries focused on the general technology dangers of chemistry, nuclear energy, genetic engineering and of other installations with possible harmful impacts on man and nature. The *actual changes* dealt with in the discussion can be traced back to three main aspects:

- New risks with greater impacts arise which cannot be limited in space, time or with regard to the group of persons affected.
- In many fields,¹¹⁶ risks have acquired a "social dimension" and cannot be traced back to individually responsible persons.
- The complexity and the speed of development of social and technological changes are increasing.¹¹⁷

2. Consequences in the Legal System

The resulting legal changes - until now especially discussed in environmental law - can be reduced to three lines of development as well:

- With respect to greater risks, an improved crime prevention by social politics, but also a more
 powerful state and intensified legal control are called for. Repressive controls are replaced
 also in criminal law by preventive regulations with more intensive interventions.¹¹⁸
- The social dimension of risks leads to risk communities, solutions by insurance law, new objects of legal protection and strict liability. It is especially controversial in how far criminal law can solve the problems mentioned. On the one hand, wider rules of imputation and protective concepts are called for, on the other hand, a reduction of criminal law is demanded

¹¹⁵ I.e. the "epoch in which the dark sides of progress more and more rule social conflicts". Cf. Beck (ed.), Politik in der Risikogesellschaft, 1991, p.10, as well as the basic work of Beck, Risikogesellschaft, Auf dem Weg in eine andere Moderne, 1986. For the meaning of this term for criminal law cf. Prittwitz, Strafrecht und Risiko, 1993.

¹¹⁶ For example the hole in the ozone layer, water pollution or floods.

¹¹⁷ Cf. Stratenwerth, 105 ZStW (1993), p. 681.

¹¹⁸ Cf. Albrecht, KritV 1988, p. 182 (at p. 209); Callies, NJW 1989, pp. 1338 et seq.; Hassemer, NStZ 1989, p. 553 (at p. 558); Hilgendorf, NStZ 1993, p. 10 (at pp. 13 et seq.); Kuhlen, GA 1994, pp. 347 et seq.; Wolf, 15 Leviathan (1987), p. 357 et seq.

as it is regarded inappropriate for the regulation of social dimension risks and for a risk balance independent of fault because of its classic needs for imputation.¹¹⁹

 Because of the greater complexity and dynamism, the law makes more and more use of indefinite legal terms, of blanket clauses and dynamic references. Legislation by private organizations (especially so-called self-regulation) increases.¹²⁰ Apart from this, the correlation between different fields of law becomes closer; new intermediate fields emerge.¹²¹

3. Information Technology as Part of the Risk Society

The analysis in the first part of this paper has demonstrated that most changes of the risk society also occur in the field of information technology: Small alterations of data can move large amounts of deposit money. Computer sabotage - for example in banks or with flight control systems - affects the most vital parts of the modern economy. Complexity and speed of development are growing. Accordingly a lot of the general findings and controversies concerning the "law of the risk society" apply to the field of information technology as well:

- The future information society requires mainly non-criminal measures for the prevention of computer crime. Technical security standards that include access control systems, instructions for the system users concerned and appropriate general conditions of civil and administrative law are much more important than criminal law provisions.¹²²
- However, at the same time an adaptation of criminal law to the new risks is necessary: The general reproach of an over-criminalization by the protection of collective interests as well as the use of "per se bans" and strict-liability offenses of "risk criminal law"¹²³ is not justified in this analyzed field of information technology. The presented analysis of "information law" has shown that the introduction of new objects of legal protection by the reform laws especially intellectual property and the citizen's right to privacy is justified by new needs for protection in the information society. Problems of imputation of the risk society as well as the resulting "per se bans" can hardly be noticed in the field of criminal information law. Only in the field of criminal data protection law is there an over-criminalization, which is however not due to the creation of new collective objects of legal protection or "per se bans", but to disregarding the classic ultima-ratio principle of criminal law.
- Legal regulations must not concentrate on coincidental technological changes as was done in various formulations of the 2nd German Act for the Prevention of Economic Crime. What is

¹¹⁹ Cf. for the first opinion Stratenwerth, 105 ZStW (1993), p. 679 (at pp. 691 et seq., 659); Tiedemann / Kindhäuser, NStZ 1988, p. 337 (at pp. 339 et seq.); for the opposite opinion cf. Calliess, NJW 1989, pp. 1338 et seq. (at p. 1343); Hassemer, NStZ 1989, p. 553 (at p. 558).

¹²⁰ Cf. for the regulatory techniques in the field of environmental law Hoppe / Beckmann, Umweltrecht, 1989, pp. 41 et seq., 159. For the constitutional problems of these regulatory techniques cf. Denninger, Verfassungsrechtliche Anforderungen an die Normsetzung im Umwelt- und Technikrecht, 1990, pp. 31 et seq., 79 et seq., 117 et seq., 148 et seq. For the problems concerning the participation of expert committees in legislation of. Hofmann, Privatwirtschaft und Staatskontrolle bei der Energieversorgung durch Atomkraft, 1989, pp. 42 et seq.

¹²¹ A popular example for such an intermediate field is - besides information law - especially environmental law.

¹²² Cf. for the necessity of a stronger political (non-legal) control of technological and economic sectors from the discussion about the risk society especially *Albrecht*, KritV 1988, pp. 182, 205, 209. In particular on computer crime cf. *Sieber*, The International Handbook on Computer Crime, 1986, pp. 117 et seq.; cf. especially for organized crime *Sieber / Bögel*, Logistik der Organisierten Kriminalität, 1993 pp. 287 et seq.

¹²³ Cf. especially Hassemer, NStZ 1989, pp. 557 et seq.; ZRP 1992, pp. 378 et seq.

necessary is structural thinking and a description of the functions thus resulting to law which can also deal with a changed technology.¹²⁴

Summing up the discussion about the consequences of the risk society, one can say that the development of crime and law in the field of information technology disproves for this particular sector the global, general criticism of a too far-reaching "risk criminal law". The new criminal provisions and likewise the new procedural powers of intervention for criminal investigations in the field of information technology are predominantly justified by the social changes presented. Legal policy must nevertheless accept the reproach that non-criminal measures have been neglected and that a partly insufficient legal technique has been used.

C. Global Society and International Legal Harmonization

1. Social Changes

The third general line of development behind the problems described here is the loss of importance of national borders and the corresponding international harmonization of law. The coming together of the citizens of the world - in general related to a greater mobility - can be seen in the field of computer crime particularly with the use of international telecommunication networks: The mobility of data in these networks makes it possible to commit a crime with the help of a computer of which the results take place abroad. Data can be transferred via international networks in a split second without any control possible.

2. Legal Effects

Different national laws for the prevention of computer crime would therefore necessarily lead to "data havens" or "computer crime havens",¹²⁵ which would then entail national restrictions to the free flow of information. Such national barriers would not only be inefficient because of the existing possibility of using international telecommunication networks for an encoded transfer of data abroad. National restrictions and supervision would moreover endanger the citizens' right to privacy and the business secrets of enterprises and would hinder the economic development of an international information market. If we want to characterize the changes analyzed with some catchwords, we must add the catchword "global society" to the terms "information society" and "risk society".

For this reason the international harmonization of information law by the EC, the Council of Europe, the OECD, the UN, the WIPO and the AIDP has to be welcomed and to be carried on. Furthermore, in a time of radical changes with new dangers of informatics and technology, a strengthening of contacts among the single nations is necessary.

¹²⁴ Cf. Sieber, Informationstechnologie und Strafrechtsreform, 1985, pp. 33 et seq.

¹²⁵ An example in the field of software piracy is the distribution of illegal copies with the help of foreign mailboxes; cf. for Canada *Piragoff*, in: Sieber (ed.), Information Technology Crime, 1994, p. 87.

IV. Summary

The criminological part of this paper has shown that the spreading of computer technology into most areas of life, especially the increasingly close relationship between data processing and data telecommunication technology, has made computer crime more diverse, more dangerous, and more international. The legal part of the article could trace back the multitude and the complexity of the resulting legislative reactions to six groups of problems and "waves" of reform: the protection of privacy, the fight against computer-related economic criminal law, the protection of intellectual property, the fight against pornography and other communication offenses, the reform of procedural law as well as new regulations concerning safeguard measures and the recognition of an electronic signature.

These developments of crime and the law are based on the underlying social changes and shifts of paradigms which will continue to exert crucial influence on our law in future:

- The emergence of the information society with its new objects of protection under criminal law,
- The changes of the risk society in which non-criminal measures deserve greater attention but in which measures of criminal law and criminal procedural law will also play an important role, as well as
- The growing together of the citizens in a "global society" in which new challenges can only be coped with by means of international cooperation.

These changes entail a loss of power of the classic national state both in favor of regional and supranational governmental organizations as well as in favor of multinational companies. Therefore, the effective protection of the citizen in the newly emerging information and communication society is only possible if these basic changes are considered and shaped positively. We need an intensified cooperation of national states and supranational organizations, new prevention and prosecution measures of information technology, as well as adequate control strategies of data protection law.

Senate Permanent Subcommittue

U. S. Department of Justice on Investigations

EXHIBIT # _____33

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

NOV 1 3 1995

The Honorable Sam Nunn Ranking Minority Member Committee on Governmental Affairs Permanent Subcommittee on Investigations United States Senate Washington, D.C. 20510

Attn: Dan Gelber, Chief Counsel (Minority) Permanent Subcommittee on Investigations

Dear Senator Nunn:

Thank you for your letter concerning the prosecution of computer related crimes. We apologize for any inconvenience our delay in responding has caused. You asked for statistics on computer intrusion investigations and prosecutions from 1993 to the present and the number of Justice Department employees who have been subject to disciplinary action for computer misuse.

We have examined our records (1) for those specific cases in which a computer related statute is the lead charge [18 U.S.C. §§ 1030, 2701], and (2) under the program category for "computer crimes," which indicates computer-related prosecutions under more generic criminal statutes where the office that prosecuted the case classified it as being primarily computer related.

You requested statistics by calendar year; however, our database is maintained on a fiscal-year basis and would require special programming with monthly counts to produce information by calendar years. If a report by fiscal year is satisfactory, I can tell you that at the beginning of FY 1993 there were 121 investigative matters involving 129 individuals, and 28 cases pending against 31 defendants. "Matters" refers to criminal investigations presented to the United States Attorneys for review or other action. A "matter" becomes a "case" when an indictment is returned or information filed that commences the actual prosecution. New matters received or cases filed in FY 1993 and subsequent years are as follows:



The Honorable John Glenn Page 2

	New matters/cases by Fiscal Year			
	<u>1993</u>	1994	1995	1996 [6 months]
Matter Count	138	134	162	71
(Subjects)	164	167	229	89
Case Count	53	47	45	27
(Defendants)	57	57	64	39

The FY 1996 numbers are for the first six months of the fiscal year, from October 1995 through March 31, 1996.

In answer to your second question about DOJ employees who have had disciplinary action taken against them, we found that 26 instances of disciplinary action categorized as "computer misuse" have occurred. Disciplinary action taken extends from reprimands to various periods of suspension.

We hope that this is of assistance to you. Please do not hesitate to contact this office if you have questions or concerns regarding this or any other matter.

Sincerely,

U. 1a

Andrew Fois 44 Assistant Attorney General

Senate Permanent Subcommittee on Investigations

EXHIBIT # 34

NEWS RELEASE

WarRoom Research

WarRoom™ Operations • Competitive Intelligence • Security Safeguerds

FOR IMMEDIATE RELEASE

Contact: Mark Gembicki Executive Vice President WarRoom Research, LLC. 410.437.1106 or 410.437.1110

1996 Information Systems Security Survey

Findings Reveal Security Problems in Fortune 1,000 Corporations

Baltimore, Maryland (November 21, 1996) — A new information security survey of Fortune 1,000 firms has produced striking evidence of serious problems in many commercial organizations. Nearly half of the 205 firms that responded admitted that their computer networks had been successfully attacked and penetrated by "outsiders" in the past year -- with losses and associated costs considerably higher than previously estimated.

The results of the '96 Information Systems Security Survey, which was sponsored by WarRoom Research, LLC, will be presented during a Morning Newsmaker press conference at the National Press Club in Washington, DC, 9 am Thursday, November 21, 1996. The survey drew an unprecedented high rate of response from the estimated 500 corporate professionals surveyed, noted WarRoom Research executive vice president Mark Gembicki.

"It was sent to the right people," Mr. Gembicki explained. "It was distributed by executives and staff from six prominent organizations, among them several leading vendors of information security technologies which typically passed it on to senior managers who are clients and associates." Representatives from the six organizations who distributed the survey are scheduled to appear at the press conference to comment on and help explain the results.

The objectives of the survey were two-fold. The first was to better quantify the potential security threats and vulnerabilities to these businesses, as well as to the National Information Infrastructure -- the nation's vital computer systems such as banking, transportation, and telecommunications. We also hoped this research would foster a greater awareness of the need for joint public/private-sector initiatives to better secure corporate and government networks, noted WarRoom Research president Steven Shaker.

The survey also had another intriguing credential. The survey questionnaire was accompanied by a letter from Senator Sam Nunn's Chief Counsel with the U.S. Senate's Permanent Subcommittee on Investigations, expressing their interest in the results and promising to respect the survey's guarantee of anonymity to all respondents.

596

Mr. Gembicki expressed his gratitude to the respondents and to the groups that distributed the survey: IBM, Interpact, National Computer Security Association, Security Dynamics, Symantec, and the WheelGroup. Comments from the distributing companies include:

Interpact/www.infowar.com - "The WarRoom Survey serves as yet another wake-up call to Corporate America and the Government: computer crime, cyber-terrorism, and espionage are all real facets of Information Warfare," said Winn Schwartau, president. "It's time to take them seriously."

Symantec/www.symantec.com -- "Symantec provides solutions addressing two of the top three security vulnerabilities identified by this study, including anti-virus and encryption software," said Bill Stover, senior director of federal sales. "Symantec was pleased to participate in distributing the survey, and is committed to addressing security issues among individuals as well as corporate and government users."

WheelGroup/www.wbeelgroup.com -- "A large percentage of respondents indicated they had policies on computer use which is an encouraging statistic on the surface," said Chris Goggans, senior network security engineer. "However, 129 of the 205 companies actually caught insiders misusing their computer systems and this may be an indication that corporate security policies are not adequate and more technical solutions are needed."

Executives from 98 of the 205 firms which responded to the survey acknowledged that their staff had detected intruders who gained unauthorized access to computer systems in the past year -- but fully 27 percent of the respondents doubted their organization had the capability to detect illicit access attempts, or even penetration of their computers.

The corporations surveyed were willing to estimate the losses and associated costs for each successful intrusion by outsiders into their computer network. Costs per incident were estimated at over \$50,000 by 84 percent (136) of the respondents. Moreover, 41 percent indicated losses of more than \$500,000 per intrusion with 36 of these companies estimating losses at over a million dollars.

The next phase of this project will begin in early 1997 and include a much broader study of information systems security issues. One area of focus will be an analysis of emerging threats and vulnerabilities, as well as interviews with executives on known competitor and adversary attacks. "Typical security indicators don't reveal how far someone will go to target a company and what methods they will use," said Mr. Shaker. "We are going to take a hard look at information systems security when it comes to illegal espionage and legal competitive intelligence."

#

WarRoom Research, LLC, of Baltimore, Maryland, was founded in 1995 to research and develop alternative technologies and techniques to assist organizations in gaining a competitive edge in today's global business environment. It offers a line of WarRoom[™] products and consulting services which blend the distinct, yet interrelated areas of collaborative decision making, competitive intelligence, information security, and operations security. Training services include the new seminar series entitled Raising the Competitive IQ[™], which provides instruction on how to develop and maintain a successful level of "competitiveness" as well as the Quarterback Technique[™] for collecting competitive intelligence at conferences and in cyberspace.

1996 Information Systems Security Survey Conducted by WarRoom Research, LLC

»	
Notes:	

Sent (est.) - start 7/18/96	500
Received - end 10/18/96	238
Rcvd. %	47.2%
Used - qualified and direct responses	205
Used %	86.9%

'Specified' means response was detailed.

'Developed response' means it was not on the survey form. 'Developed table' means responses were tabulated.

I. General Information	Response	Genaral	Specific
1. Position in the organization?			
security/loss prevention mgmt.	102	49.8%	
executive mgmt.	74	36.1%	
other mgmt. (specified)	29	14.1%	
	205	100.0%	
2. Security areas responsible for?			
anti-terrorism/personnel protection	3		0.4%
crime/loss prevention	66		8.3%
computer/information security	127		16.0%
disaster/emergency mgmt.	57		7.2%
facility mgmt.	19		2.4%
human resources	0		0.0%
Investigations/auditing	41		5.2%
legal counsel	6		0.8%
operations security	88		11.1%
physical security	72		9.1%
proprietary information	112		14.1%
safety	15		1.9%
sales/service	38		4.5%
security awareness/education	74		9.3%
security personnel	48		6.0%
strategic planning	13		1.6%
other (specified)	18		2.3%
	795		100.0%

WarRoom Research, LLC

Page 1

3. Adequately respond based on understanding and insight?			
yes	205	100.0%	
no	Q	0.0%	
	205	100.0%	
* If 'yes', how much time spent on security matters?			
None (developed response)	2		1.0%
<10%	7		3.4%
10-20%	24		11.7%
11-30%	38		18.5%
31-50%	51		24.9%
51-70%	46		22.4%
71-90%	37		18.0%
71-8076	205		100.0%
4. How many people supervised? a. Directly			
0	5	2.4%	
1-5	37	18.0%	
6-10	62	30.2%	
11-15	54	26.3%	
16-20	29	14.1%	
>20	18	8.8%	
	205	100.0%	
b. Indirectly			
0	21	10.2%	
1-5	65	31.7%	
6-10	39	19.0%	
11-15	37	18.0%	
16-20	26	12.7%	
>20	17	8.3%	
- 64	205	100.0%	

WarRoom Research, LLC

Page 2

599

5. Type o	of industry?		
Primar	y business		
	agriculture	0	0.0%
	architectural/engineering firm	3	1.5%
» ⁵	communication service	17	8.3%
	distribution/warehousing	2	1.0%
	educational inst.	8	3.9%
	entertainment or sports	2	1.0%
	environmental	7	
	food service	ó	3.4% 0.0%
	financial inst.	12	5.9%
	health care	8	
	hotel/motel/resort	3	3.9%
	industrial/manufacturing	21	1.5%
	Insurance	13	8.3%
	news media	2	1.0%
	oil, gas, or mining extraction	4	
	pharmaceutical	17	2.0%
	public relations		8.3%
	real estate	1	0.5%
	retail	6	2.9%
	R&D	15	7.3%
	security consulting firm	11	5.4%
	security service, guards and alarms	16	7.8%
	transportation/travel	3	1.5%
	utilities	13	6.3%
	other (specified)	9	4.4%
	orie. (opening)	12	5.9%
		205	100.0%

Secondary business * Not calculated, not as relevant.

II. Policy	Response	General	Specific
6. Written policy on computer use and misuse?			
yes	171	83.4%	
no	34	16.6%	
	205	100.0%	
7. Mandatory warning banner putting users on notice to	be monitored online?		
yes	137	66.8%	
no	68	33.2%	
	205	100.0%	
a. If 'yes', ever enforced banner?			
yes	51		37.2%
no	86		62.8%
	137		100.0%

WarRoom Research, LLC

Page 3

148	72.2%	
57	27.8%	
205	100.0%	
Hone?		
		65.5%
		34.5%
148		100.0%
205	100.0%	
Response	General	Specific
facility if suspects	d or witnesse	d attacke?
		a allevere :
205	100.078	
In the investigation	1?	
125		64.4%
42		21.6%
27		13.9%
194		100.0%
stems?		
	72 7%	
205	100.0%	
ccess to network re	sources, etc.	
205	100.0%	
eveloped table)		
41		41.8%
24		24.5%
24 16		16.3%
		16.3% 10.2%
16		16.3% 10.2% 5.1%
16 10		16.3% 10.2%
	57 205 80ns? 97 51 148 179 26 205 Response 1 facility if suspecte 194 11 205 1 facility if suspecte 194 11 205 205 205 205 205 205 205 205 205 205	57 27.8% 205 100.0% ions? 97 51 148 179 87.3% 26 12.7% 205 100.0% Response General 1 facility if suspected or witnesse 194 94.6% 11 5.4% 205 100.0% In the investigation? 125 42 27 194 vistems? 149 194 72.7% 55 27.3% 205 100.0% ccesss to network resources, etc. ses in past 12 months? 119 58.0% 25 12.2% 61 29.8% 205 100.0%

WarRoom Research, LLC

Page 4

601

13. If ex	perienced intrusions by outsiders, type of activity	performed?		
	manipulated data integrity	41		6.8%
	installed a sniffer	40		6.6%
	stole password files	34		5.6%
`,	probing/scanning of system	88		14.6%
	Trojan logons	35		5.8%
	IP spoofing	29		4.6%
	introduced virus	64		10.6%
	denied use of services	38		6.3%
	downloaded data	49		8.1%
	compromised trade secrets	59		9.8%
	stole/diverted money	2		
	compromised e-meil/documents	76		0.3% 12.6%
	publicized intrusion	78		0.5%
	harassed personnel	27		
	other (specified)			4.5%
	other (specified)	18		3.0%
		603		100.0%
14. Hov	w many insiders caught misusing computer system			
	Unknown	20	9.8%	
	0	56	27.3%	
	1-5	24	11.7%	
	6-10	48	22.4%	
	11-15	32	15.6%	
	16-20	13	6.3%	
	21-25	9	4.4%	
	>25	5	2.4%	
		205	100.0%	
a. 1	f 'yes', what disciplinery action was taken?			
	oral admonishment	70		54.3%
	written admonishment	27		20:9%
	suspended	7		5.4%
	resigned	8		8.2%
	fired	11		8.5%
	referred to law enforcement	2		1.6%
	out of court settlement			
	no ection	0		0.0%
	other (specified)	4		3.1%
	outer (specified)	Q		0.0%
		129		100.0%

WarRoom Research, LLC

Page 5

Summary of Results				
IV. Damage & Reporting Res	ponse	General	Specific	
15. Cost for each successful intrusion into computer systems?				
a. By insider				
Unknown (developed response)	26	12.7% 0.0%		
\$0	0	0.0%		
\$1 - 1,000	3	1.5%		
\$1,001 - 5,000	11	5.4%		
\$5,001 - 10,000	23	11.2%		
\$10,001 - 50,000 \$50,001 - 200,000	46	22.4%		
\$200,001 - 500,000	41	20.0%		
\$500,001 - 1,000,000	23	11.2%		
Over \$1,000,000	32	15.6%		
	205	100.0%		
b. By outsider	43	21.0%		
Unknown (developed response)	43	0.0%		
\$0	ő	0.0%		
\$1 - 1,000	ő	0.0%		
\$1,001 - 5,000	9	4.4%		
\$5,001 - 10,000	17	6.3%		
\$10,001 - 50,000 \$50,001 - 200,000	30	14.8%		
\$200,001 - 200,000	39	19.0%		
\$500,001 - 1,000,000	31	15.1%		
Over \$1,000,000	36	<u>17.6%</u>		
	205	100.0%		
16. How many intrusions investigated internelly? (developed table)	21		13.5%	
0 1-5	38		24.5%	
6-10	26		16.8%	
11-15	23		14.8%	
16-20	19		12.3%	
21-25	15		9.7%	
>25	13		8.4%	
-	155		100.0%	
a. If 'yes', who conducted inquiry?				
corporate security	41		30.6%	
general counsel	12		9.0%	
computer security	22		18.4%	
systems administration	31		23.1% 13.4%	
executive mgmt	18		5.2%	
mid-level mgmt	7		2.2%	
other (specified)	134 134		100.0%	

WarRoom Research, LLC

,

Page 6

¢

603

17. How many intrusions reported to security firms that investig	ated? (developed table)
1-5	23	54.8%
6-10	9	21.4%
11-15	4	9.5%
, 16-20	4	9.5%
>20	2	4.8%
	42	100.0%
a. Of these, how many referred to law enforcement? (deve	eloped table)	
1-5	3	75.0%
6-10	1	25.0%
	4	100.0%
b. If not referred to law enforcement, what was reason?		
didn't get into system	4	4.4%
didn't want to get person in trouble	2	2.2%
didn't know it was a crime	1	1.1%
didn't want law enforcement in system	13	14.3%
take over system, loose productivity	13	14.3%
access to sensitive information	11	12.1%
don't think they would be interested	0	0.0%
don't think they would solve it	2	2.2%
crime become public	19	20.9%
loss of client confidence	18	19.8%
loss of competitive status	8	8.8%
opted for civil remedy	0	0.0%
other (specified)	Q	0.0%
	91	100.0%
18. What circumstances would be willing to report computer in	trusions to law enforce	ment?
anytime detected	33	6.8%
could report anonymously	146	30.2%
only if everyone else reported	105	21.7%
only if mandatory by law	181	37.4%
other (specified)	19	3.9%
	484	100.0%

V. Financial Institutions Only

19. Performing EFTs * No feedback from ALL financial institutions.

WarRoom Research, LLC

Page 7

•

604



Senate Permanent Subcommittee on Investigations

EXHIBIT # _____ 36

June 4, 1996

Via Facsimile

Dan Gelber, Esquirc Chief Counsel, Minority Permanent Subcommittee on Investigations Committee on Governmental Affairs United States Senate 193 Russell Senate Office Building Washington, DC 20510

Dear Mr. Gelber:

This letter is in response to your request that Mark Rasch and Hank Kluepfel of SAIC appear before the Subcommittee on June 5, 1995 to testify regarding computer crime in the commercial sector and about fraud related to public switch networks.

Although we would like to assist the Committee in its hearings and with respect to its work, we must decline on behalf of Mr. Rasch and Mr. Kluepfel because of significant ellent confidentiality concerns. We are very sorry for any inconvenience this decision has caused the Committee and we have reached this decision reluctantly, after much consideration.

We will, of course, continue to provide background information about these areas to the Committee. If you have any questions, please feel free to contact me at 703 556-7236.

Yours truly,

Mr. French

Susan M. Frank Corporate Counsel

1710 Goodridge Drive, P.O. Box 1303, McLean, Virginia 22102 • (703) 821+4300 Oniz 3410 Ottow. Advessed Golden, Isano, Fan Orma, Hanenka Isa Virge, Ine Alex Ine Angelee, Kirkan, 134 Pirge, Olarde San Onge, Scatte, Tunece



TED STEVENS ALASKA, CHAIRMA

WILLIAM V ROTH. JA. DELAWARE WILLIAM S COHEN, MAINE FRED THOMPSON, TENNESSEE THAD COCHRAN, MISSISSIPP JOHN MCCAIN, ARIZONA BOB SMITH, NEW HAMPSHIRE HANK BROWN, COLORADO

JOHN GLENN DHO SAM NUM, GEORGIA CARL LEVIN MICHIGAN GAVID PRYOR, ARKANSAS JOSEPH I LIBERMAN CONNECTICUT DANEL K. AKAKA, HAWAH BYRON L. DORGAN, NORTH DANDTA

ALBERT L MCDERMOTT, STAFF DIRECTOR LEONARD WEISS, MINORITY STAFF DIRECTOR

ferred 5/30 mailed

United States Senate

COMMITTEE ON GOVERNMENTAL AFFAIRS WASHINGTON, DC 20510-6250

May 30, 1996

Mark D. Rasch, Esquire Director Information Security Law & Policy Center for Information Protection Science Applications International Corporation (SAIC) 8301 Greensboro Drive, E-4-1 McLean, Virginia 22102

Dear Mark:

Thank you for agreeing to participate in the Permanent Subcommittee on Investigations' hearing next week on *Security in Cyberspace*. I'm sure your testimony will assist the Subcommittee in its efforts to explore the vulnerability of our national information infrastructure.

As we discussed today, I will advise Senator Nunn of your concern that your testimony not reveal proprietary information about your firm's business, including the identity of past or present clients. You may refer to that assurance in your statement if you so choose. There should not be any difficulty in acquiescing to this request.

Sincerely,

Dan Gelber Chief Counsel (Minority) Permanent Subcommittee on Investigations

DG:mdr



Ο

