AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 108–516

VIRTUAL THREAT, REAL TERROR: CYBERTERRORISM IN THE 21ST CENTURY

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

FEBRUARY 24, 2004

Serial No. J–108–58

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

94–639 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
LINDSEY O. GRAHAM, South Carolina
LARRY E. CRAIG, Idaho
SAXBY CHAMBLISS, Georgia
JOHN CORNYN, Texas

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
CHARLES E. SCHUMER, New York
RICHARD J. DURBIN, Illinois
JOHN EDWARDS, North Carolina

BRUCE ARTIM, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Democratic Chief Counsel and Staff Director*

SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY

JON KYL, Arizona, *Chairman*

ORRIN G. HATCH, Utah
ARLEN SPECTER, Pennsylvania
MIKE DEWINE, Ohio
JEFF SESSIONS, Alabama
SAXBY CHAMBLISS, Georgia

DIANNE FEINSTEIN, California
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
JOHN EDWARDS, North Carolina

STEPHEN HIGGINS, *Majority Chief Counsel*
DAVID HANTMAN, *Democratic Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	3
prepared statement	32
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	1
prepared statement	36
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, prepared statement	42

WITNESSES

Lourdeau, Keith, Deputy Assistant Director, Federal Bureau of Investigation, Washington, D.C.	6
Malcolm, John G., Deputy Assistant Attorney General, Department of Justice, Washington, D.C.	5
Schmidt, Howard A., Vice President and Chief Information Security Officer, eBay, Inc., San Jose, California	23
Verton, Dan, Author, Burke, Virginia	18
Yoran, Amit, Director, National Cyber Security Division, Department of Homeland Security, Washington, D.C.	8

SUBMISSIONS FOR THE RECORD

Forbes Magazine, Peter Huber and Mark Mills, September 15, 2003, article	34
Lourdeau, Keith, Deputy Assistant Director, Federal Bureau of Investigation, Washington, D.C., prepared statement	44
Malcolm, John G., Deputy Assistant Attorney General, Department of Justice, Washington, D.C., prepared statement	53
Schmidt, Howard A., Vice President and Chief Information Security Officer, eBay, Inc., San Jose, California, prepared statement	67
Verton, Dan, Author, Burke, Virginia, prepared statement	77
Yoran, Amit, Director, National Cyber Security Division, Department of Homeland Security, Washington, D.C., prepared statement	87

VIRTUAL THREAT, REAL TERROR: CYBERTERRORISM IN THE 21ST CENTURY

TUESDAY, FEBRUARY 24, 2004

UNITED STATES SENATE,
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND HOMELAND SECURITY, COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:11 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Jon Kyl, Chairman of the Subcommittee, presiding.

Present: Senators Kyl and Feinstein.

OPENING STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Chairman KYL. Good morning. This hearing of the Judiciary Committee Subcommittee on Terrorism, Technology and Homeland Security will come to order.

First, as I catch my breath, my apologies particularly to the witnesses here before us, but also to Senator Feinstein and to those of you in the audience. We are well over-scheduled. Senator Feinstein, I know, has a meeting that began at ten o'clock, too, so her presence here is very, very much appreciated for however long you can be here. Let me just give a brief opening statement, then call on Senator Feinstein, and then we are anxious to hear from our panel.

On January 27, this Subcommittee examined the security of our seaports and their vulnerability to terrorist attacks. Today, we are going to examine the security of our cyber infrastructure and its vulnerability to cyberterrorist attacks.

As the world has grown more connected through the Internet and cyberspace, the dangers associated with attacks on that technology have also increased. The quantity and quality of cyber attacks are on the rise. The number of computer security intrusions increased from about 84,000 in 2002 to 137,000 in 2003.

Computer viruses are spreading at much faster rates and causing more damage than ever before. While it took 26 hours for a virus in 2001 to infect 300,000 machines worldwide, a virus in February 2003 infected 300,000 machines within only 14 minutes. As Secretary Ridge stated in December, "anywhere there is a computer...whether in a corporate building, a home office or a dorm room...if that computer isn't secure, it represents a weak link because it only takes one vulnerable system to start a chain reaction that can lead to devastating results."

Since 1997, this Subcommittee has held seven hearings on cyber attacks and critical infrastructure protection. During the most recent of these hearings, witnesses expressed concerns about terrorists conducting cyber attacks against the United States. Terrorists already use cyber tools to raise funds and to organize physical attacks. They could obviously use those same tools for conducting cyber warfare.

In 2000, FBI Director Louis Freeh testified before this Subcommittee that cyberterrorism was, and I am quoting now, "a very real, though still largely potential threat." Today's hearing will focus on the status of that threat now and what we are doing to reduce the threat.

Terrorists are targeting our cyber infrastructure and we have got to educate the public about this threat. According to news reports, data from al–Qaeda computers found in Afghanistan show that the group had scouted systems that control critical U.S. infrastructure. An attack on these systems could have devastating results, especially if done in conjunction with a physical attack.

A study by the National Infrastructure Protection Center concluded that the effects of September 11 would have been far greater if launched in conjunction with a cyber attack disabling New York City's water or electrical systems. An attack on these systems would have inhibited emergency services from dealing with the crisis and turned many of the spectators into victims.

The Subcommittee today will hear from five witnesses, three experts from the Federal Government and two from the private sector. The first is Assistant Attorney General John Malcolm at the Department of Justice. He is the Deputy Assistant Attorney General in the Criminal Division of the Department of Justice. He oversees the Computer Crime and Intellectual Property Section, the Child Exploitation and Obscenity Section, the Domestic Security Section, and the Office of Special Investigations. An honors graduate at Columbia College and Harvard Law School, Mr. Malcolm served as a law clerk to judges on both the U.S. District Court for the Northern District of Georgia and the Eleventh Circuit Court of Appeals.

Second is Deputy Assistant Director Keith Lourdeau, Cyber Division of the FBI. Keith Lourdeau is the Deputy Assistant Director of the FBI's Cyber Division. He previously served as Assistant Special Agent in Charge of the St. Louis Division, where he was responsible for the daily operation of that division.

Mr. Lourdeau entered the FBI in 1986 and has served in the Chicago, Little Rock and St. Louis field offices. While serving at FBI Headquarters, Mr. Lourdeau was detailed to the CIA to assist in establishing a new initiative between the CIA and the FBI in targeting international organized crime groups.

Director Amit Yoran, National Cyber Security Division, Department of Homeland Security. He is the Director of the National Cyber Security Division for DHS. Previously, he served as the Vice President for Managed Security Services at Symantec Corporation, where he was primarily responsible for managing security infrastructures in 40 different countries.

Before working in the private sector, Mr. Yoran was the Director of the Vulnerability Assessment Program within the Computer

Emergency Response Team at the Department of Defense and the Network Security Manager at the Department of Defense, where he was responsible for maintaining operations of the Pentagon's network.

On the second panel, we have two individuals. Dan Verton is the author of Black Ice: The Invisible Threat of Cyberterrorism, which is a book analyzing al–Qaeda's ability to conduct cyber attacks and U.S. vulnerability to cyber terrorists. He is also a senior writer on the staff of Computerworld, covering national cyber security and critical infrastructure protection.

Mr. Verton is a former intelligence officer in the United States Marine Corps, where he served as senior briefing officer for the Second Marine Expeditionary Force and analyst in charge of the Balkans Task Force from 1994 to 1996.

Finally, Howard Schmidt is the Vice President and Chief Information Security Officer for eBay. Prior to that, Mr. Schmidt served as the Chair of the President's Critical Infrastructure Protection Board in 2003, and as the Special Adviser for Cyberspace Security for the White House from 2001 to 2003. Mr. Schmidt has also worked as the chief security officer for Microsoft and as the head of the Computer Exploitation Team at the FBI's National Drug Intelligence Center. From 1983 to 1994, I am proud to say he was an officer for the Chandler Police Department in Arizona.

In conclusion, the United States has not suffered a major cyberterrorist attack, but we have got to continue to improve our security of our critical infrastructure systems because the more dependent we become upon technology, obviously the greater challenge in protecting it.

We have a distinguished panel of witnesses before us today and I am very interested in examining with them the threats and vulnerabilities that we face and what Congress can do to help prevent cyberterror and to prosecute cyber criminals in the United States and abroad.

As always, I want to thank Senator Feinstein for her hard work in helping to put together this hearing. We have had an excellent relationship in dealing with this particular subject over the years that we have been together on this Subcommittee and I look forward to working with her.

[The prepared statement of Senator Kyl appears as a submission for the record.]

Chairman KYL. Senator Feinstein.

STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thanks very much, Mr. Chairman, and I appreciate your leadership and your agreement to have this hearing.

Let me just begin right at the top and say my concern is that we really don't take cyberterrorism as seriously as we should, that it isn't at the top of this huge totem pole in Homeland Security. I believe Mr. Yoran reports to an assistant secretary, and the strategy up to this point, as I understand it, is to leave most of this to the private sector. I am not really sure, long-term, that this is going to work.

I think you only have to look at a recent computer virus, MyDoom, that recently spread in January like wildfire across the Internet to really understand the threat. MyDoom was responsible for sending 100 million infected e-mails in its first 36 hours, and accounted for one-third of all e-mails sent worldwide on one evening. The virus shut down the website of the SCO Group, and also attacked the Microsoft website. Damages worldwide ran into hundreds of millions of dollars.

Denial-of-service attacks offer only a small glimpse into what is a huge potential cyberterror threat. A terrorist could theoretically use a computer to open the flood gates of a dam—we have talked about this before—disrupt the operations of an aircraft control tower, shut down the New York Stock Exchange or other important businesses or government agencies, or disrupt emergency communications of law enforcement and safety officials. And we know how many invasions there are a year of Defense computers here in the United States. It is a real problem, and we have been fortunate so far.

One oft-cited example is an April 2000 incident in Australia where a disgruntled consultant sabotaged the electronic controls to a sewage system, letting loose millions of gallons of sewage on a town. But the threat is uniquely insidious. In contrast to attacks on our ports or biological or chemical weapons, cyberterror does not have to be launched within the United States geographic confines.

I would also note that 85 to 90 percent of our Nation's cyber infrastructure remains under the control of the private sector. And as I said, the administration so far has embraced a voluntary, market-based approach to cyber security. In December 2002, Governor Gilmore criticized this voluntary approach. He said, "So far, pure public/private partnerships and market forces are not acting...to protect the cyber community." So I am concerned that we essentially are unprepared for a major cyber attack.

Here are some questions I hope the panel can address: How real is the threat? Has the Department of Homeland Security placed a high enough priority on defense against cyberterrorism? Are we better prepared today to defend against a cyber attack than we were on 9/11? Is the current voluntary private sector and government collaboration working? Is there more we can or should do to defend ourselves?

Now, I understand that an NIE is going to be released sometime later this week on cyberterrorism. So we might want to also take a look at that and see where we go from here.

Thanks very much.

[The prepared statement of Senator Feinstein appears as a submission for the record.]

Chairman KYL. Thank you very much, Senator Feinstein.

It is also very helpful having Senator Feinstein also on the Intelligence Committee, on which I served for 8 years. And it is going to be interested to coordinate with the Intelligence Committee, as well, any specific activities that we follow through on here.

Senator FEINSTEIN. As a matter of fact, I am going to have to leave in about 20 minutes. We have George Tenet over in Intelligence this morning.

Chairman KYL. I was aware of that, so let's get right to the panel. I think we will do the clock just so you can get an idea of when you have spoken for 5 minutes. Obviously, any other statements you would like to make for the record, in addition to your written statements, we will include.

Let's start with Mr. Malcolm and then go on down to Mr. Lourdeau and then Mr. Yoran.

STATEMENT OF JOHN G. MALCOLM, DEPUTY ASSISTANT ATTORNEY GENERAL, DEPARTMENT OF JUSTICE, WASHINGTON, D.C.

Mr. MALCOLM. Thank you, Chairman Kyl, Senator Feinstein. On behalf of the Department of Justice, I would like to thank you for inviting me to appear before you this morning to discuss the important issue of cyberterrorism.

Under the President's National Strategy to Secure Cyberspace, the Department of Justice and the FBI are charged with leading the national effort to investigate and prosecute cyber crime. Our role as law enforcement distinguishes what we do from what the Department of Homeland Security does.

Specifically, while DHS deals with vulnerability assessment, prevention and damage mitigation, we act to prevent and deter cyber crime by investigating cyber crime incidents and identifying and prosecuting those who violate Federal laws.

Cyberterrorism involves the use of computer systems to carry out terrorist acts, which are in turn defined by reference to specific criminal statutes. True cyberterrorism is characterized by large-scale destruction, or the threat of such destruction, coupled with an intent to harm or coerce a civilian population or government.

Because attacks on critical infrastructure have the potential for large-scale disruptions and mass casualties, even if not accompanied by terroristic intent, the issues of cyberterrorism and critical infrastructure protection are often intertwined. We have been fortunate enough not to experience a devastating attack of cyberterrorism or a crippling attack on a critical infrastructure. Nevertheless, the hard lessons of 9/11 teach us that preparation is critical.

The Department has developed specialized expertise in the area of cyber crime, led by the Computer Crime and Intellectual Property Section, or CCIPS, which I oversee. That section's 37 attorneys focus exclusively on issues relating to computer and intellectual property crime. They are supported in the field by 212 computer and telecommunications coordinators, or CTCs, who are specially trained Assistant United States Attorneys who function effectively as a resource for their respective districts and as a point of contact for multidistrict cases.

The Department has also focused on developing partnerships with other Federal agencies, with State and local law enforcement and with industry organizations. We work closely with DHS's National Cyber Security Division and the Cyber Interagency Incident Management Group, with the National White Collar Crime Center's Cyber Crime Advisory Board and the National Association of Attorneys General, and with InfraGard, an important initiative

that expands direct contacts between government and private sector infrastructure owners and operators.

Because cyber attacks frequently transcend geographic boundaries, the Department's cyber crime initiatives have not been confined to the United States. CCIPS chairs the G8 Subgroup on High–Tech Crime and has successfully spearheaded the development of the 24/7 Network. In addition, CCIPS is active on several committees of the Organization of American States that relate to cyber security, and it has worked with other regional governmental groups including the Asia Pacific Economic Cooperation Forum, or APEC.

We intend to continue our work toward improving the quality of cyber crime legislation and response mechanisms in other regions of the world. We believe that improved laws will not only serve as a deterrent, but will also increase the overall prosecution of cyber criminals, including cyberterrorists, who would seek to operate in otherwise lawless nations.

The Department relies on a number of tools, both substantive and procedural, to investigate and prosecute cyber attacks. One of the most important of these is the USA PATRIOT Act. You are no doubt aware that many of the USA PATRIOT Act's provisions are currently set to expire. Because these provisions, including the emergency service provider exception, the hacker trespass exception and the nationwide search provision, would be essential to any investigation or prosecution of cyberterrorism, I would urge you not to allow these provisions to sunset.

While I would like nothing better than to be able to assure you that an attack of cyberterrorism will never occur, unfortunately I can't do that. I can, however, assure you that the Department is taking and will continue to take the necessary steps to prepare to respond appropriately in the event of a cyber attack.

I thank you again for allowing me the time to address this Subcommittee on this important issue and I look forward to your questions.

[The prepared statement of Mr. Malcolm appears as a submission for the record.]

Chairman KYL. Thank you very much, Mr. Malcolm. You are right on the button time-wise.

Mr. Lourdeau.

STATEMENT OF KEITH LOURDEAU, DEPUTY ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, D.C.

Mr. LOURDEAU. Good morning, Chairman Kyl, Senator Feinstein. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in combatting cyberterrorism.

As our Nation's economy becomes more dependent on computers and the Internet becomes an increasingly more integral part of our society, new digital vulnerabilities make U.S. networks systems potential targets to an increasing number of individuals, including terrorists.

The Director of the FBI has established protecting the U.S. from terrorist attacks as its number one priority and protecting the U.S. against cyber-based attacks and high-technology crimes as its num-

ber three priority. The FBI's Cyber Division's number one priority is counterterrorism-related computer intrusions.

Our network systems make inviting targets for terrorists due to the potential for large-scale impact to the Nation. The vulnerabilities to our network systems arise from easy accessibility to those systems via the Internet, harmful tools that are available to anyone with a point-and-click ability, the globalization of our Nation's infrastructures, and the interdependencies of networked systems.

Terrorist groups are increasingly adopting the power of modern communication technology for planning, recruiting, propaganda purposes, enhancing communications, command and control, fundraising and fund transfers, and information-gathering.

To date, cyber attacks by terrorists or persons affiliated with them have largely been limited to relatively unsophisticated efforts, such as the e-mail bombing of ideological foes or the publication of threatening content. However, increasing technical competency in these groups is resulting in an emerging capability for network-based attacks. The more familiar they become with computers and their potential as a viable weapon against us, the more likely they will try to acquire the skills necessary to carry out a cyberterrorist event.

The FBI assesses the cyberterrorism threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful and possibly devastating purposes is on the rise. Terrorist groups are showing a clear interest in developing basic hacking tools, and the FBI predicts that terrorist groups will either develop or hire hackers particularly for the purpose of complementing large physical attacks with cyber attacks.

Attacks against regional targets could have a significant effect on computer networks, while coordinated attacks on multiple regions could achieve a national effect with severe repercussions. There are numerous control systems whose destruction would have a far-reaching effect. Large-scale distribution systems, such as those involving natural gas, oil, electric power and water, tend to use automated supervisory and data acquisition systems for administration. These SCADA systems tend to have both cyber and physical vulnerabilities.

A major method used in preventing cyberterrorism is the sharing of intelligence information. The FBI routinely passes intelligence received in active investigations or developed through research to the intelligence community. Throughout the FBI field offices, special agents serve on cyber task forces with other agencies. The FBI is also a sponsor/participant in the InterAgency Coordination Cell. This environment of information-sharing and cooperation is expanding to include foreign governments such as the 5 Eyes.

The FBI has established cyber task forces, public/private alliances, cyber action teams, cyber training, and a cyber intelligence center, all to provide a strategic framework and program management tool for all FBI computer intrusion investigations.

While the following two incidents were not cyberterrorism, they are an indication of the ability of individuals to gain access to our network systems and the possible damage that can result.

For example, an individual used simple explosive devices to destroy the master terminal of a hydroelectric dam in Oregon. Although there was no effect on the dam's structure, the simple attack completely disabled the dam's power-generating turbines and forced a switch to manual control.

A coordinated attack on the region's infrastructure systems, such as the SCADA systems that control Washington, D.C.'s electric power, natural gas and water supply, would have a profound effect on the Nation's sense of security. This incident demonstrated how minimal sophistication and material can destroy a SCADA system.

In another example, on May 3, 2003, an e-mail was sent to the National Science Foundation's Network Operations Center which read, "I've hacked into the server of your South Pole Research Station. Pay me off, or I will sell the station's data to another country and tell the world how vulnerable you are."

The e-mail contained data only found in the NSF's computer systems, proving that this was no hoax. NSF personnel immediately shut down the penetrated servers which control the life support systems for the 50 scientists wintering over at the South Pole. The FBI determined that the hackers were accessing their e-mails from a cyber cafe in Romania.

Through joint FBI and Romanian investigative efforts, the Romanian authorities seized documents, a credit card used in the extortion, and the e-mail account that was used to make the demands of the NSF. On June 3, 2003, two Romanian citizens accused of hacking into the NSF South Pole Research Station were arrested.

The unique complexity of protecting our Nation's network systems is a daunting task. The protection of our network systems is a shared responsibility between the private sector, Federal, State and local law enforcement, the Department of Homeland Security and the intelligence community, both domestic and foreign.

Again, I offer my gratitude and appreciation to you, Chairman Kyl, and Senator Feinstein for dedicating your time and effort in addressing this vitally important issue. I would be happy to respond to any questions you may have. Thank you.

[The prepared statement of Mr. Lourdeau appears as a submission for the record.]

Chairman KYL. Well, thank you very much, Mr. Lourdeau. That one story you told, I am sure, is illustrative of many others, but it is a great story. We need to get more of that information out so that we can follow our educational role here and really convince people that this is real, this isn't just hypothetical.

Mr. Yoran.

STATEMENT OF AMIT YORAN, DIRECTOR, NATIONAL CYBER SECURITY DIVISION, DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, D.C.

Mr. YORAN. Thank you, Chairman Kyl, Senator Feinstein. I appreciate the opportunity to appear before you today to discuss the important issue of cyberterrorism. I also welcome the chance to provide your Subcommittee with an update on the efforts of the Department of Homeland Security's National Cyber Security Division to defend our Nation against the menace of cyber threats.

The National Cyber Security Division, established by the Department in June of 2003, represents a crucial component of the Information Analysis and Infrastructure Protection Directorate. Under the leadership of Under Secretary Frank Libutti and Assistant Secretary Robert Liscouski, the IAIP Directorate leads the Nation's efforts to protect the Nation's critical infrastructures from attack or disruption.

Placement of the National Cyber Security Division in the IAIP Directorate allows for the careful integration of physical and cyber security approaches into a common, holistic management framework. Through the integration of physical and cyber protection capabilities, the components of IAIP work together to protect America's critical infrastructures.

Under the leadership of Assistant Secretary Liscouski, we are considering the full range of risks to the Nation, including loss of life, disruptions to infrastructure services, economic impact and national security implications. Recognizing that future terrorists attacks may not be limited to cyber or physical acts, but rather a combination of the two to amplify impact, the Office of Infrastructure Protection is organized to examine threats and vulnerabilities across multiple dimensions, including integrating and mapping vulnerabilities to threats, assessing sector-specific and cross-sector vulnerabilities, and understanding national, regional and local impacts.

Moreover, the close linkage of the Office of Information Analysis, led by Assistant Secretary Patrick Hughes, the primary threat information intelligence-gathering and analysis capability of the Department of Homeland Security, promotes the ability to map threat information with cyber vulnerabilities. This mapping allows for the effective prioritization of potential risks and implementation of remediation efforts as quickly as possible to limit the impact of computer incidents.

For the remainder of my remarks, I will provide an overview of the cyber threat environment facing the Nation and activities the National Cyber Security Division is undertaking with its partners to reduce our National vulnerability to these threats.

As members of this Subcommittee have heard on numerous occasions, cyber threats continue to be a significant national and global concern. When vulnerabilities are identified, viruses are launched, or when other types of cyber attacks are reported, it is often difficult to immediately identify and understand the underlying motives for such attacks.

Is it an isolated cyber attack, for example, a part of a terrorist plot, a criminal enterprise, or a teenager surfing the Net in search of a thrill? The difficulty is that vulnerabilities and techniques that are exploited in the interest of cyber crime or even cyber hacktivism are the same vulnerabilities and techniques that are at issue when discussing cyberterrorism.

Therefore, the National Cyber Security Division employs a threat-independent strategy of protecting the Internet and critical infrastructures from all types of attacks. While staying acutely aware of how terrorists might exploit cyber techniques, we face challenges in distinguishing between malicious acts of terrorism versus other types of attacks as an event is occurring in real time.

Rather than only focusing on specific attack profiles, we are developing programs and initiatives that apply to the gamut of attack approaches. In other words, our mission extends to protecting cyber systems across the entire threat spectrum, regardless of an actor's intent. If we attempt to stovepipe our protection efforts to focus on different types of attackers who may use the cyber infrastructure, we risk the possibility of limiting our understanding of the entire threat environment.

While maintaining a threat-independent approach, the National Cyber Security Division recognizes that DHS and the Federal Government must remain vigilant in the identification of all types of cyber attackers. Components of the IAIP Directorate and our Federal partners in law enforcement, defense and intelligence devote considerable time and energy to identifying groups and individuals with the capability to launch cyber attacks and to determining the individuals responsible for an attack and its aftermath.

At the Department of Homeland Security, the question we ask ourselves everyday is how are we making America safer, because in the end that is our key metric for success. In preparing to testify, I reflected on how far we as a country have progressed in cyber security in the past decade. The accomplishments are truly remarkable.

In that time, we have created a Cabinet-level agency to bring together government, industry and academia to manage national cyber incidents. Government agencies, private corporations and our research community have developed, fielded and improved cyber security technologies such as firewalls, anti-virus technology and intrusion prevention systems to better protect our networks.

Again, I wish to thank the Chairman, Ranking Member and members of the Subcommittee for the opportunity to speak with you today and I look forward to answering your questions.

[The prepared statement of Mr. Yoran appears as a submission for the record.]

Chairman KYL. Thank you very much, Mr. Yoran.

In view of the fact that Senator Feinstein is going to have to leave, would you like to lead with the questions?

Senator FEINSTEIN. Oh, how nice. Thank you very much. I would be happy to.

I strongly believe that cyber security should be one of the lead priorities of the Department of Homeland Security. Before the creation of the Department, your predecessors, Richard Clarke and Howard Schmidt, had senior positions on the White House staff. They served as special advisers to the White House on cyberspace security. Now, as I said, cyber security is relegated to a mid-level position in the Department. As Director, you don't report directly to Secretary Ridge, but to an assistant secretary.

My question is this: Given your lack of seniority in the Department, how will you be able to direct assistant secretaries in other directorates to bolster up cyber security? Do you have the organizational clout, for example, to get the Border and Transportation Directorate to bolster its cyber security policies? Tough questions.

Mr. YORAN. Senator Feinstein, I would maintain that cyber security maintains a very high profile within the administration and within the Department of Homeland Security. We must continue to

maintain cyber as an integral component of our overall risk management approach to our critical infrastructures and to our public interest. It should not be stovepiped as an individual protection approach.

I would also maintain that there are advisers within the White House who maintain very close awareness of cyber activity and cyber preparedness, but that within the Department of Homeland Security, through Homeland Security Presidential Directive 7, the Department of Homeland Security should maintain an organization to be the Nation's focal point for cyber security preparedness.

Senator FEINSTEIN. At this point, have any directives been given by Homeland Security to other departments to tighten their cyber security?

Mr. YORAN. The National Cyber Security Division works very closely in collaboration with the Office of Management and Budget, with the National Institute of Standards and Technology and with a number of other organizations across the Federal Government who have responsibility and authority to create standards and help define protection strategies for our Government.

Senator FEINSTEIN. Well, I take it the answer is no to my question.

Today, 85 to 90 percent, as I understand it, of the cyber security infrastructure is in private hands, and private sector control makes defending this aspect of our homeland somewhat unique. What can the Federal Government do to ensure the security of so many resources that are now outside of Government control, anyone that would like to have a crack at it?

Mr. LOURDEAU. Well, one of the things that we need to do is we still need the public/private alliances between Government and private industry. There are contingency plans and other issues that the Government could assist private industry with so that there is a consistency across the board for security, both cyber and physical.

As we know, there is a correlation between physical attacks and cyber attacks, and if the infrastructure's physical capabilities are not protected, then the cyber capability is not going to be protected. So I think it is very important that we continue that relationship between private industry and Government, and assisting in providing contingency plans and have that consistency across the board.

Senator FEINSTEIN. Is that happening today? Are these plans available for review? Could this Subcommittee take a look at those plans?

Mr. LOURDEAU. Yes, we have those. When the FBI had the National Infrastructure Protection Center, we were assisting in providing contingency plans, and I believe that Homeland Security has taken that over.

Mr. YORAN. That is correct. In Homeland Security Presidential Directive 7, there is new focus on critical infrastructure protection planned. In addition, we have a tremendous amount of collaboration ongoing with the private sector through a number of different forums and we are working aggressively on contingency planning in various bad-base scenario capabilities, such as the Critical Infrastructure Warning and Information Network, so that we can com-

municate with the private sector and amongst the key Federal departments and agencies who would respond to cyber incidents.

Senator FEINSTEIN. Mr. Chairman, I think it would be very useful if our joint staffs were able to take a look at those plans, because there is no way of us really exercising any oversight if 85, 90 percent of this is private sector.

Now, if those alliances exist and are in writing, it seems to me we ought to be able to review them, and I would make that request that our joint staffs have an opportunity to take a look at what does exist with respect to achieving cyber security in the private sector now.

Chairman KYL. Any difficulty with providing us that information and meeting with us and our staff?

Mr. LOURDEAU. No, and I will speak for both of us. We will make sure that is available to you.

Chairman KYL. All right.

Senator FEINSTEIN. May I place a statement by the ranking member, Senator Leahy, in the record?

Chairman KYL. Yes. Without objection, it will be received.

Senator FEINSTEIN. Thank you very much, and I am going to excuse myself. Thank you for your courtesy.

Chairman KYL. Well, thank you. I know you had to leave that other hearing. We appreciate you being here.

Senator FEINSTEIN. Thank you.

Chairman KYL. Let me now ask some questions. Specifically as a follow-up to Senator Feinstein's question here, we have held, as I said, a number of hearings on this. Back before there was a Department of Homeland Security, we had testimony about the NIPC, in fact, a couple of different times.

In 2001, at one of our hearings, the GAO had prepared a report on the National Infrastructure Protection Center, at that time located in the FBI. It was critical of the NIPC, stating that NIPC had failed to develop a broad strategic analysis of cyber-based threats. What I am interesting in knowing is how DHS, now having taken that over, has proceeded to address concerns like that, or have you?

I will tell you, let me ask you a second follow-up question because it relates specifically to your testimony, Mr. Yoran. In the year 2000, the Director of the CERT Coordinating Center, which is a reporting center for computer security programs that is located at Carnegie Mellon—Richard Pethia, who is the director of that center, testified that the Government was awash in a sea of vulnerability studies, and what we really needed was to develop an accurate threat assessment for cyber attacks. He reasoned that the private sector could not afford to eliminate every vulnerability in their operations and had to prioritize.

In your testimony, you state that the National Cyber Security Division employs a threat-independent strategy or protecting the Internet and critical infrastructures, and I understand the rationale behind that. Nonetheless, have you focused on developing a threat assessment of cyber attacks, in addition to dealing with your independent strategy?

Mr. YORAN. Mr. Chairman, our protection strategy is threat-independent. In the Directorate of Information Analysis and Infrastruc-

ture Protection, we have the ability to fuse and review threat information coming from across the sources with which information analysis deals, including law enforcement and intelligence.

Chairman KYL. Well, let me ask it another way. Mr. Malcolm testified that the FBI doesn't do a threat assessment, that that is now DHS' job. That may be fine if it is being done and if it is very transparent, but I still haven't heard you say that DHS has done a threat assessment for cyber attack.

Again, I appreciate the rationale for the need to protect against and deal with an attack, whatever its source. But in order to appreciate the potential, and therefore devise ways of dealing with a specific kind of attack, it seems to me that DHS must be carrying out a cyber threat analysis and must have some kind of threat analysis in existence.

This is something that I had talked with Mr. Mueller about before DHS existed as part of the overall response to 9/11, in which it was determined that the FBI no longer could simply respond to crimes and investigate them and provide evidence to prosecutors to prosecute the crimes, which is pretty much, Mr. Malcolm, what you said the role was with the creation of DHS.

That is fine, if somebody else is now doing the job that we had asked the FBI to do right after 9/11, not leaving it just to the CIA. But in this country, we needed a threat assessment of cyber attack; it had to be done by somebody. If the FBI isn't doing it, then we need to know that DHS is doing it and I am still not clear on what DHS does in this regard and what you have in this regard.

Mr. YORAN. Mr. Chairman, the Department of Homeland Security, in accordance with Homeland Security Presidential Directive 7, is developing a critical infrastructure protection plan which would be an integrated threat and protection strategy. It does not stovepipe cyber threats as an independent or stovepiped approach or threat to our infrastructures, but looks at cyber as one component of infrastructure protection.

I would also add that through conducting exercises such as Live Wire, we are looking at threats against our infrastructures and ways which we can improve our preparedness and our response capabilities to cyber as an integrated attack vector to our Nation.

Chairman KYL. Well, I appreciate that. Is somebody else doing a threat analysis of cyber attack from terrorists or other state sponsors?

Mr. MALCOLM. Mr. Chairman, perhaps I will throw Mr. Yoran a lifeline, which is that DOJ has participated in things like Live Wire and, through CCIPS, we work very closely with DHS. I didn't hear Mr. Yoran to say that DHS is not doing that threat assessment. I heard him to say that it is subsumed as part of general critical infrastructure threat assessment.

I can tell you, for instance, that in work dealing with telecommunications transactions, sub-cyber transactions within the Committee for Foreign Investment in the United States, I work on behalf of DOJ on that interagency committee. I have worked with Mr. Yoran, I have worked with Mr. Liscouski.

We have discussed on numerous occasions vulnerabilities, including cyber vulnerabilities, and we do that vulnerability assessment both in terms of the current infrastructure and also in terms of

players—nation states, potential private company threats within that worldwide infrastructure.

Mr. YORAN. Mr. Chairman, I would just add you mentioned earlier the National Intelligence Estimate currently being released this week for a classified understanding of cyber threats, and also a focus or a requirement—not to openly disagree with Mr. Pethia's opinion, but the focus is and needs to remain on infrastructure services.

And the goal here, the intent, is not cyber preparedness for cyber security's sake. It is in the delivery of infrastructure services to serve the public, and so we need to look at cyber as part of an integrated approach to infrastructure protection.

Chairman KYL. Well, I appreciate that, but I know—well, let me just ask this question. The NIE is being prepared by a group of agencies of our Government, and there will be primarily the classified version of that which includes obviously intelligence collection and our military use of cyber.

But as a separate threat to our infrastructure, whether it be primarily Government or purely private sector, is there anywhere that you know of in our Government a specific threat assessment of terrorists or state sponsors of terror with respect to the Internet or our cyber security? I shouldn't just say the Internet because there are systems that aren't necessarily directly Internet-connected.

Mr. LOURDEAU. If I may answer, Chairman, the Cyber Division at the FBI has created—and I believe we have shared it with your staffers—the FBI's cyber threat assessment which is target-based to the threats, the targets that we believe are threats to the United States. That is, again, a classified threat assessment and we will be more than happy to share that with you.

Chairman KYL. Well, is this a target-based assessment of threats from any source or is it an assessment of the risk from terrorism to the system?

Mr. LOURDEAU. Again, it is directed toward identifying the targets that are threats to the United States, and so it goes toward terrorism and state nations, and then the whole range of the concern over the Internet as far as child pornography, Internet fraud, intellectual property rights. It reaches all different aspects of cyber.

Chairman KYL. Well, I don't mean to belabor this, but obviously I need to get some more follow-up from each of you on this point and I would like to have some further clarification.

It seems to me that in properly analyzing the threat and how to protect our systems, both government and non-government, when you have kind of a matrix, for one thing you examine the vulnerabilities, the threat-independent assessment of the private and governmental sectors. But you also would be obviously aided by an analysis of the kinds of attacks which could occur, ranging from the relatively benign nuisance kind of attacks, to non-benign hacking, to criminal enterprises, to terrorist attacks, and then specifically state-sponsored intrusion for all of the reasons that states attempt to intrude.

Now, at that level you are really into classified material, I understand. But it seems to me that the assessment should be on both sides: who might attack us, and why and how, and how is our system vulnerable. I understand that when an attack occurs, you can't

know immediately where it is coming from, and one of the first things is to try to figure that out so you know where you have to go. And it doesn't much matter in the early stages whether it is from a state or a terrorist or a couple of hackers who, in effect, replicate terrorists. But it is important as time goes on to know how to deal with it and what are the systems to warn or shut down, and so on.

So I am still trying to understand whether there is a document, other than the NIE that is coming out—and perhaps it will be all-inclusive; I don't know—which analyzes the types of threats, including an assessment of risk from terrorist organizations. I mean, can I find a document that does that, and if so, what is it? Do any of you know where that might be?

Mr. LOURDEAU. Again, our threat assessment does not really address the vulnerabilities that would be attacked. We are looking at the entities or the places that might attack the U.S. That is what the FBI is focusing our energies on, is trying to address those threats. So, again, if I understand correctly, it is not as complete an assessment as what you are looking for.

Chairman KYL. But now what you just said then contradicts at least what I thought I heard before. DHS is looking at the vulnerabilities of the government and non-government systems in a threat-independent way.

What you just said, Mr. Lourdeau, is that the FBI is actually looking less at the vulnerability of the systems than to the origins of the threat to try to understand those threat origins. Is that correct?

Mr. LOURDEAU. That is correct.

Chairman KYL. So is there a threat assessment that is prepared by the FBI from that point of view?

Mr. LOURDEAU. Yes, sir.

Chairman KYL. Okay, and I presume there are both classified and unclassified versions of that?

Mr. LOURDEAU. We just have a classified version.

Chairman KYL. All right.

Mr. LOURDEAU. And that has been shared with your staffers.

Chairman KYL. Okay. My staff is shaking his head no, so we will need to get this—

Mr. LOURDEAU. I am sorry. We will make sure that it is available to you.

Chairman KYL. Okay. So then just to summarize this point, let me just ask you all, do you think—Mr. Yoran, let me specifically ask you, do you think that our Government somewhere needs to have a threat assessment of potential terrorist attacks on government and non-government infrastructure?

Mr. YORAN. Sir, if I could defer a response until after we see what comes out in the National Intelligence Estimate, I think at this stage, with the report pending this week, it would be premature to say that we need an additional threat assessment on what the capabilities are of various cyberterrorist organizations.

Chairman KYL. I am not saying additional. I mean, maybe that does the trick, but we need a threat assessment, right?

Mr. YORAN. Yes.

Chairman KYL. In other words, the DHS threat-independent work that you are doing, you would agree, is not enough?

Mr. YORAN. Sir, that is focused on vulnerability identification and protection remediation strategies. It is not focused on threat assessment.

Chairman KYL. Right, but you assume that the NIE will, in fact, also focus on a threat assessment?

Mr. YORAN. Yes, sir.

Chairman KYL. Right, assume that, and so we will take a look at that and visit with you all on that later.

Mr. YORAN. Sir, we have been working through the directorate and the information analysis folks in the production of that NIE. So we are an integral part of the production of that document and understanding what is happening there.

Chairman KYL. Well, again, I don't mean to belabor it, but I happen to know that, for example, intrusions into key Government computer systems by what we believe to be states represents a totally different kind of threat than the occasional—not occasional—it is almost ongoing, constant hacking by pretty capable people. And you deal with those vulnerabilities in different ways, right?

Mr. LOURDEAU. Yes, sir.

Mr. YORAN. Sir, you deal with the threats in different ways.

Chairman KYL. Yes, that is exactly right, but whether the system is vulnerable to a particular technique that may be used by both a state sponsor, a terrorist or a hacker isn't the only point in being able to defend. It is also helpful to assess the threat coming from each of those various sources. At least it seems to me it is. I will be curious to get some follow-up response from each of you, including we will take a look at the NIE and then visit with you.

Mr. Malcolm, you specifically mentioned the USA PATRIOT Act and I appreciate your doing that. We may well need to follow up on your testimony there to get an elaboration of why it is so important to permit those sections that you said are very valuable to you to remain and not be sunsetted.

If I could just even at this point ask you for any additional information that you could elaborate for us on that point, I would appreciate it, because one thing that we want to do in this Subcommittee is be sure that when that debate on sunsetting begins that we have developed all of the information we need to to demonstrate why we need to retain key provisions of the PATRIOT Act and why, in fact, it is working and doing a job right now. And that was your point.

Mr. MALCOLM. Well, I welcome that opportunity and I will be certain to do so in even greater detail than what I am about to tell you in follow-up questions. But certainly in terms of the ability to get computer records through nationwide search warrants, the enlarged scope of information that is obtainable by subpoena—those are tools that prosecutors across the country are using everyday to catch terrorists and serious criminals.

In terms of things like, for instance, the emergency exception for obtaining stored communications, I know of at least one case that involved a bomb threat to a high school in which the owner of the network had not been aware of the fact that there was now a life-and-limb emergency disclosure exception. Upon being made aware

of that, he turned over the content of those communications and law enforcement authorities were immediately able to trace the perpetrator of that threat to a student in the school.

I know that that disclosure exception has also been used recently in the threat against a U.S. embassy overseas. There are many examples that I am confident I will be able to provide you.

Chairman KYL. Thank you for that. I think it is really important that we get this information out because, as you know, the PATRIOT Act is under attack by some who I think fail to appreciate the way in which it has helped our law enforcement. So the more we can get that information out, the better we are going to be.

Mr. MALCOLM. Thank you, Senator.

Chairman KYL. This past week, DHS launched the Protected Critical Infrastructure Information program to enable the private sector to voluntarily submit infrastructure information to the Government. In the past, we have had testimony before our Subcommittee that businesses have been reluctant to provide certain information to the Government or even share it with other businesses, fearing, for example, that it would harm their business of the public understood what was potentially or actually happening to them.

They also feared that information might be obtained by the public under the Freedom of Information Act, and also possibly that sharing of this information or strategies of dealing with it might even violate antitrust laws. That was another concern that they expressed to us. Senator Bennett and I had a bill in 2001 that would have eliminated those problems, and the Homeland Security Act of 2002 did address the FOIA issue which established an exception for certain data submitted to DHS.

Particularly for Mr. Yoran or Mr. Malcolm, do you know of any impediments today that prevent the private sector from fully reporting cyber intrusions and critical information data to the PCII program or other Federal agencies? Is there anything further that we need to do that you know of?

Mr. MALCOLM. Actually, Senator, I testified about that issue. Really, that question would probably be better addressed to Mr. Schmidt on the second panel, since he is in the private sector and they are the people who possess the information.

Chairman KYL. Okay.

Mr. MALCOLM. We have certainly, with the help of people such as yourself, tried to address those concerns so that we can get the information that we need to do our job, since, as has been pointed out several times now, 85 to 90 percent of these networks are controlled by the private sector. To some extent, we don't know what we don't know, but we have certainly bent over backwards and appreciate your assistance to make it easier to report that information.

Chairman KYL. I appreciate that. Of course, we will ask the question. But, before, it was the law enforcement agencies that were saying we are not getting cooperation from the private sector because they have these fears. So that was really the impetus for our legislation.

This is kind of a general follow-up, but in your testimony, for example, you discussed the Department's successes in prosecuting

cyber criminals. Are there any other modifications to the law that you can think of that you want to bring to our attention that might help you in doing your job?

Mr. MALCOLM. I am confident, Mr. Chairman, that if I put my mind to it, I could think of one or two. Suffice it to say these are very sophisticated criminals who are very good at perpetrating these acts and very good at covering their tracks. We are constantly thinking of new ways to get information as rapidly as possible because this type of evidence is truly evanescent and is gone within seconds. We are happy to work with your staff to come up with some proposals.

Chairman KYL. Okay. Well, for all three of you, anytime—not just after this hearing, but anytime you become aware of improvements that we could make in the law, I mean one of our jobs in this Subcommittee is to constantly—that is why we have had so many hearings on this subject, to pin you. Is there anything else we need to be doing here to follow through on your request to retain these provisions in the PATRIOT Act and provide a forum for discussion and education on that matter?

So if at any time there is something that comes across your desk that you think we could profitably deal with, we invite you to bring that to our attention. That is our job in this Subcommittee.

Mr. MALCOLM. Thank you.

Chairman KYL. Is there anything else that any of you, based upon what I have said—I didn't mean to ever cut any of you off, but is there anything that any of you would like to bring to our attention here before we bring up our second panel?

Well, we will look forward to reviewing the NIE and then getting back to you and determining whether there is any follow-up that we need to make from that. Unless you have any further, then what we will do is call the second panel up. I want to thank you for your testimony here. We will be staying in touch with you, and again call on us if you think that our Subcommittee can help.

Mr. MALCOLM. Thank you, Mr. Chairman.

Chairman KYL. Thank you.

I have already introduced our other two witnesses, Mr. Dan Verton and Mr. Howard Schmidt. Simply because that is the way you line up, unless by prior agreement you would like to switch it, Mr. Verton, we could start with you and follow with Mr. Schmidt.

Is that all right with the two of you?

Mr. VERTON. Yes.

Chairman KYL. All right. Again, we will use the lighting system here to just let you know when you have concluded 5 minutes, but obviously we are anxious to hear anything you have to say. So thank you.

STATEMENT OF DAN VERTON, AUTHOR, BURKE, VIRGINIA

Mr. VERTON. Well, thank you, Mr. Chairman. I want to thank you for the honor of appearing before you today to discuss what I think is an urgent national security matter.

I am heartened to hear that the National Intelligence Estimate will be released this week. I might add that my latest research shows that that is about 5 years late at this point. One of your colleagues in the House requested one that long ago and it is finally

coming out. I don't know if 5 years is really the time frame fast enough to keep up with cyber threats, so I think that is a very important development this week.

Chairman KYL. If I could just interrupt, I concur in your comments. When we scheduled this hearing prior to our break, we did not know that this was the time that the NIE was going to be released or perhaps we would have done it afterward. However, given the fact that a lot of that will be classified and not subject to discussion in an open forum like this, I think it is well to go forward with this hearing, but perhaps we will have to do some follow-up. But thank you for that.

Mr. VERTON. What I would like to do today, Mr. Chairman, is actually try to give you an open-source threat assessment, if you will. What I would like to cover today is the Nation's current level of vulnerability to cyberterrorism, al–Qaeda's specific capability to conduct cyberterrorism, and the potential implications for a combined physical and cyberterrorist attack against U.S. critical infrastructure.

Before meaningful discussion can be conducted about the Nation's vulnerability to cyberterrorism, I think it is important to know that there is no longer any separation between the physical, real world and the cyber world. Computers control real things in the real world, and most of these things, as you have already heard, are critical infrastructures that have both financial and economic implications, as well as public safety implications.

This understanding must lead us to a new, more flexible definition of cyberterrorism. We can no longer view cyberterrorism with blinders on, simply from the perspective of somebody sitting behind a computer and launching malicious code or hacking and disrupting other computers and other computer networks.

If there is one thing we learned from 9/11, it is that traditional physical terrorist attacks can have devastating cyber ramifications for the U.S. critical infrastructure, and it can also disrupt to a significant extent the United States economy. A little bit later on in my statement, I am going to get to where the economic aspects of cyberterrorism fit into this puzzle.

It is an unprecedented level of interdependency that right now accounts for most of the vulnerability of the U.S. critical infrastructure. The economy right now has multiple Achilles heels. Every sector is dependent upon another sector for their day-to-day operation. As we learned on August 14, which I will address a little bit later in more detail, no one sector can survive without electric power, without telecommunications, and so on and so forth.

Perhaps one of the most important areas where an unprecedented level of vulnerability remains today is in the widespread adoption of wireless technologies. Although there are tested ways to secure wireless technologies that are being adopted today, they are not always adopted correctly, they are not always managed correctly, and sometimes they are not deployed at all.

In my research, I have found evidence of unprotected wireless networks in use at hospitals; curbside baggage checking at some of the Nation's largest airlines; remote heating systems for portions of the railroad network; in support of emergency controls and alarms for uranium mining operations; at water and waste water

treatment facilities; security cameras at both airlines, airports, and at defense installations; and at oil wells and water flood operations around the country.

Let me just say a word about SCADA systems, since you have heard some talk about SCADA systems this morning already from the first panel. Despite what you may be told, SCADA systems are not the secretive, proprietary systems that their names implies—supervisory control and data acquisition systems—nor are they separate from the public Internet.

In some cases, they are indeed protected, but in most cases—and I have seen this through my own research with my own eyes—wiring diagrams that connect the real-time control systems that run the day-to-day operations of the electric power grid in the United States are connected to the corporate networks of some of the utilities around the country.

Now, this indirect connection provides the connection to the public Internet and is what makes these control systems vulnerable to things like the Blasto Worm, and so on and so forth. So there is, to my knowledge, a major research and development program underway right now to provide security for those systems. But make no mistake about it, they are indeed vulnerable to attacks over the general Internet.

My fear then, Mr. Chairman, is that the next time we experience a major power failure, such as August 14 of last year, it will not be a self-inflicted wound—for example, a self-inflicted failure—but it will be a terrorist-induced failure that is quickly followed up either by suicide bombings, by out-of-control gunmen on the streets of Manhattan where thousands of people are coalescing, or by chemical or biological attacks on the folks who are stranded in the subway systems. And that goes directly to the use of cyberterrorist tactics as a force multiplier, not in an end to itself, but as a force multiplier effect for traditional-style terrorist attacks.

As far as the ability of groups such as al Qaeda to carry out successful cyberterrorist attacks, I think it is important for us to start now thinking differently about the future, and particularly thinking differently about the future of international terrorism.

The high-tech future of terrorism is inevitable, and like the events leading up to September 11—events that we ignored for 8 years prior to that event—we are now beginning to see the indications and warnings that terrorist groups understand the advantages of using cyberterrorist tactics against the United States. Also, these tactics, as you will see here in a few minutes in my statement, support the strategic goals of groups like al Qaeda, strategic goals that we have not yet paid much attention to.

Terrorism is in a constant state of evolution, and terrorist tactics and modes of operation evolve over time. Sometimes, they evolve so slowly that we fail to recognize them. Al Qaeda's view of cyberterrorism is a case in point, and because I think I am running out of time here, let me get quickly to some concrete examples of al Qaeda's movement toward the adoption of cyber tactics from an offensive standpoint.

L'Houssaine Kherchtou was a 36-year-old Moroccan who was recruited by al Qaeda and he attended electronics training in a guest house owned by Osama bin Laden in Peshawar, Pakistan, in the

early to mid-1990's. Mr. Kherchtou showed up with absolutely no credentials whatsoever in electronics training, and there were two instructors that were present at the facility and they were working on advanced encryption algorithms, advanced methods of breaking encryption for the nations that were trying to track them down, and various other ways to use high technology to create fraudulent travel documents.

Because he had no understanding and no formal training in electronics, they basically started him at the ground floor. They handed him a book and told him to take apart an old computer and start to learn what the components of the computer were.

Several weeks later when a more senior instructor arrived at the guest house, he asked Mr. Kherchtou the same question. What are your credentials? And, of course, he said he had no credentials. That senior instructor then said to him he was not allowed to attend that training. He first needed to go to the local university and earn a degree in engineering and then he would be allowed to come back and conduct that training.

Now, the importance of this example is that the picture most Americans have of al Qaeda and other terrorist groups is as a mindless hoard of thugs living a hand-to-mouth existence in caves in Afghanistan. But the example I just gave you is a technologically sophisticated, thinking enemy that values formal training and I think we need to change our—this goes directly to the National Intelligence Estimate and the questions that you were asking about who are we worried about.

The second example that I will give you is an interview I conducted in November of 2002 with a gentleman named Sheikh Omar Bakri Muhammad. Just to give you an idea of the type of individual we are talking about, Bakri Muhammad is the leader of a London-based organization called al Muhajirun. He considers himself to be the official spokesman for the political wing of al Qaeda, as if there is such a thing as the political wing of al Qaeda. This is an individual who has recruited suicide bombers by his own admission, and his organization has been linked through FBI memos to various individuals at Phoenix area flight schools to his London-based organization.

He spoke to me for about 30 minutes, during which most of the time was taken up speaking about the justification for using weapons of mass destruction in support of the global jihad being waged by al Qaeda. But then he got specifically to the issue of using technology against the United States, and you can attribute the following quotes to Bakri.

"In a matter of time, you will see attacks on the stock market." "I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies." And he said, "The third letter from Osama bin Laden...was clearly addressing using the technology in order to destroy the economy of the capitalist states. This is a matter that is very clear."

This is the first time that a high-profile radical Islamic cleric has spoken in such a detailed manner about the potential for using sophisticated cyber attack tools against the United States in support

of a strategic goal, which is to damage the economy of the United States.

There is nothing in the driving factors from my research behind al Qaeda's operations, which are intent, resources and opportunity, to suggest that al Qaeda would rule out using this method of attack.

First, the strategic intent of this group is clear. Al Qaeda wants to cripple the economy of the United States in order to force us to withdraw our military from around the world, and also to withdraw our support for Israel and the Middle East. The targeting of corporate America in this respect is clear.

Second, the growing number of technologically sophisticated sympathizers around the world, especially among young Muslim children around the world who are successfully being radicalized by groups like al Qaeda today—these are the children who are now studying computer science and mathematics, who tomorrow may feel it is more advantageous for them to strike out at the United States through computers or targeting the cyber infrastructure rather than strapping dynamite around their waists and walking into crowded cafes. Tomorrow's threat may not look like today's threat. In fact, tomorrow's threat probably will not look like today's threat, and the frightening thing is that tomorrow may literally be tomorrow.

Finally, America continues to present al Qaeda, as you have heard this morning, and other terrorist groups with ample economic targets in cyberspace. There is really great work being done, but we are almost now heading into the third anniversary of 9/11 and we are nowhere near where we should be, in my opinion.

Finally, the potential danger stemming from combined physical and cyberterrorist attacks was proven in November of 2000 during the first major infrastructure interdependency exercise that took place in the Pacific Northwest.

Known by its code name Black Ice, the exercise was sponsored by the U.S. Department of Energy and the Utah Olympic Public Safety Command. When it was over, Black Ice demonstrated in frightening detail how the effects of a major cyberterrorist attack can significantly amplify the effects of either a natural disaster or a traditional physical-style terrorist attack.

Without going into details of the exercise, I will make this one point about the exercise. Unlike many other similar exercises that have taken place since, this was an exercise scenario that was developed with the help of the actual owners and operators of the critical infrastructures in that region.

So the owners of the electric power grid, the owners of the telecommunications networks, the owners of the natural gas, government, emergency services, got together and they asked them to provide them with their worst-case scenarios, their worst fears based on their inside knowledge of their own vulnerabilities. It was a very realistic scenario.

The end result, according to my interviews with the officials who put together the exercise, was that electric power from a combined physical and cyberterrorist attack would be lost for at least a month throughout a five-State region of the United States and three Canadian provinces. Some estimates put it at several

months, and a lot of that had to do with the physical aspects of the attack because we do not stockpile strategic reserves of electric-generating systems. Most of them are manufactured overseas and it would probably take that long, if those systems were physically destroyed, to get them here into the country.

Black Ice showed the growing number of critical interdependencies that exist throughout the various infrastructure systems and how devastating these types of attacks can be. Perhaps most important, the final report on the lessons learned from Black Ice, as well as a follow-on exercise code named Blue Cascades, concluded the final statement: government and private sector participants, quote, "demonstrated at best a surface-level understanding of interdependencies and little knowledge of the critical assets of other infrastructures." Moreover, most companies and government officials failed to recognize their own "overwhelming dependency upon IT-related resources to continue business operations and execute recovery plans."

So with that, Mr. Chairman, I will hand it over to my colleague, Mr. Schmidt, and I will be happy to answer your questions.

[The prepared statement of Mr. Verton appears as a submission for the record.]

Chairman KYL. Thank you, Mr. Verton.

Mr. Schmidt.

STATEMENT OF HOWARD A. SCHMIDT, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, EBAY, INC., SAN JOSE, CALIFORNIA

Mr. SCHMIDT. Thank you, Mr. Chairman. It is good to see you again and thank you for your leadership, and Senator Feinstein, for this issue that is very critical to all of us.

As you are very much aware, when we put out the National Strategy to Defend Cyberspace almost a year ago now, a little over a year ago, it was probably the first and maybe only time that we have ever engaged in public dialogue in the creation of a national strategy. We held a series of town hall meetings. We held meetings with CEOs, with journalists, with anyone we could get a hold of to talk about what it would take to secure and defend cyberspace. As you made the comment in your opening comments, Secretary Ridge has also stated an insecure computer anywhere is a weakness within the network.

Today, my remarks will primarily focus on some of the threats we see, the nature of the threats themselves, some insights as to what we have been doing relative to the private-public partnerships, and a few ideas that I think the Subcommittee would hopefully find valuable, some things we can do moving forward.

The good thing about being the clean-up hitter is all the scary stories have already been told, so I get to focus a little bit on some of the things that we can do to help remediate some of these.

First and foremost, I would like to put things in perspective. It is estimated today that there are over 840 million users on the Internet, and it is expected to grow to over 904 million at the end of 2004. So even though we have this great capacity—and eBay is a perfect example of that; millions of people worldwide make their living in using this great resource we have and providing a global

economic democracy. But by the same token, our dependencies have increased significantly as we have put more systems out there to work with.

The interesting piece of this is during the Cold War we had the ability, those of us in defense, to look at many different many aspects of threat assessments and intelligence data, satellite data, to sort of determine where the enemy was looking at and where we need to protect.

But in this era of the online world, particularly in cyberspace, we don't have that capability. It doesn't make any difference to many of us whether the attack comes from the Mideast or the Midwest, Eastern Europe or northern Arizona. If it is disruptive to our critical infrastructure, our critical cyber infrastructure, we care about it.

Now, we see this manifesting itself in a number of fashions; first and foremost, denial of service attacks; hacking; phreaking, which used to be very prevalent in the 1980's and which is coming back again, that is the hacking of PBX systems; authentication attacks; identity theft; phishing, the latest scams that we have been seeing which could lead very easily to identity theft; malicious code; viruses, et cetera; and, of course, as many of us have mentioned, the SCADA and digital control systems.

But we have seen an evolution. It used to be at one time if you wanted to take on a nation or you wanted to take even a small country on, you needed some sort of weaponry. Now, we have seen with the—and I will use the illustration of the denial of service attacks in 2000. A number of universities and businesses were taken over to launch attacks, ranging in the space of about 800 megabits per second, 800 million characters per second being thrown at systems.

What we are seeing now with the great advent of technology and cable modems and DSL is we are seeing instances where there are 20 to 30,000 systems that now are owned by unknown groups that can launch those same denial of service attacks at more than 2-gigabit-per-second rates.

Also, the area of zero-day vulnerabilities. The time frame between the discovery of a vulnerability and the release of an exploit is increasingly smaller. We have seen initially 6 months to a year; now, we are seeing a matter of hours and days that takes place.

The last threat I am concerned about, of course, is what we refer to as the blended threats. We saw this in the form of Code Red and NIMDA and, of course, NIMDA occurred just one week after September 11. And neither one of those today have we been able to identify the source, whether it was indeed a criminal organization, a clever hobbyist, or indeed a terrorist activity.

Now, quickly to the private-public partnerships, one of the major improvements we have seen in working with the manufacturers of software and hardware over the past couple of years is their commitment to make products more secure out of the box, and to make sure that they reduce the number of vulnerabilities. But this will take some time.

We don't have the capability or the financial wherewithal in today's economy to rip out IT infrastructure that was not designed to meet the current threats that we are dealing with. So it is going

to be an evolutionary process. It is going to take some resources and it is going to take some planning to be able to do this.

Additionally, the creation of the U.S. CERT at Carnegie Mellon University with DHS has also provided a gateway for the private sector to get more up-to-date information around threats that don't have to be a part of a big organization. Anybody can do it, regardless of the size of their organization.

Another thing that has been helpful for the private-public partnerships is the FBI, as John Malcolm mentioned, and the G8 Subcommittee on Cyber Crime have now engaged private sector representatives as delegates of these discussions. Also, the State Department has engaged the private sector. So we do have a lot more private sector involvement in these areas.

In my final few seconds here, I want to touch briefly on some quick recommendations that I see of vital importance to us. First and foremost, in the area of cyber crime investigations, as you pointed out earlier, we don't know until we put the habeas gravis on someone what their motive is or where they are coming from. But it is important to make sure as we develop this information, as we conduct investigations, including investigations where we never identify someone, that we have the ability to correlate and aggregate that data.

Currently, a lot of the agencies, particularly Federal agencies—the Secret Service's Electronic Crimes Task Force, the FBI's cyber crime squads—are doing really good work. But what we are not seeing is that joining of the forces to be able to at some point connect the dots that says an investigation that one agency is working on is related to one that someone else is working on. My fear, Mr. Chairman, is someday we will have a Committee hearing on why we didn't connect those dots relative to law enforcement activity.

The second piece is identity management. We have seen, as was mentioned earlier by Senator Feinstein, attacks on defense systems. A lot of those have been successful in the past just because someone has been able to hijack someone's identity by failure of the system, a blank password, for example.

Identity management is crucial to us to be able to do a better job in securing the systems. Two-factor authentications, such as Defense is now going to with the smart card concept—the two-factor is something you have, such as a physical device and the PIN number, very similar to the ATM cards we use today. These things are critical to provide better authentication into our systems as we move forward.

The last one, as was touched on by the previous panel, is vulnerability remediation and patch management. General Dave Brian at the Joint Task Force for Computer Network Operations at DoD has cited for a number of years that 98.7 percent of the successful intrusions into defense systems were related to not having a patch on the system. If we could reduce the vulnerability by that amount, it would be a tremendous service to our ability to secure the critical infrastructure.

In my reserve capacity as a special agent with Army CID, I get to work with the folks over at the Law Enforcement Counterintelligence Cell. And to your earlier question about the threat analysis, these folks are doing that on a regular basis, and DoD has been

doing it for a long time, identifying potential threats both in nation states and including organized hacker groups.

So with that, I would like to thank you once again for the opportunity and turn it back to you, and I would be happy to answer any questions you may have.

[The prepared statement of Mr. Schmidt appears as a submission for the record.]

Chairman KYL. Well, thank you both very much. First, let me just follow up on a question that I asked the previous panel that has to do with the needs of the private sector.

Mr. Schmidt, I will start with you on this. We did the FOIA legislation, so that you don't have to worry if you are bank and you report to the center that you are being hacked. You don't have to worry about people later being able to find out all about that, but there are still some concerns like the antitrust concerns.

Is there anything that you know of, based upon your work with the private sector, that we need to do from either a Federal legislative standpoint or better administering the cooperative efforts between the private sector and the Government?

Mr. SCHMIDT. Yes, and I thank you. I had dinner with Senator Bennett last night and thanked him once again for the FOIA legislation. That has really opened up some doors. I think the concern we still have, though, is the States and the sunshine laws that we face in the States.

During my time at the White House, I worked with the folks at the New York Department of Homeland Security, and the public utilities commission was sending out subpoena after subpoena asking for information from telecommunications carriers and energy providers to provide them with information which is fully discoverable.

So some sort of a Federal preemption would be helpful in order to be able to work across this area with the relative security of knowing that we can provide this information to help better secure up the infrastructure without displaying our vulnerabilities to anybody that cares to exploit them.

Chairman KYL. Okay, at least perhaps starting with some effort at a voluntarily cooperative effort with State law enforcement and other officials, and maybe start with that before we try to actually preempt the field. But maybe we would have to preempt it is what you are saying?

Mr. SCHMIDT. Well, I think that is one of the options. And to your point of the relationship with State law enforcement as well as Federal authorities, we have had a number of cyber crime summits around the country, generally led by the Information Technology Association of America and the FBI. These brought in senior leadership, as well as senior law enforcement folks, to engage in that dialogue on a voluntary basis, and we see that taking place.

But as you know yourself, that is often agent-to-agent or investigator-to-investigator type of activity. But when you go to the general counsel and say, well, listen, we think we have something we need to talk to someone about, there is a great deal of concern about that. I think the way to mitigate that is to actually get this down the system enough to make sure that we can say, yes, we are protected by the some of the legislation that is currently in place.

Chairman KYL. Mr. Verton, your book uses the term "invisible threat." We know that terrorists' primary goal is to spread fear, to spread terror. If you are a terrorist now and you are very familiar with the Internet—you raise money with it, you communicate with your buddies through use of the computer—what kind of a plan would you dream of putting into place to maximize the spreading of terror throughout our society?

Mr. VERTON. Well, Mr. Chairman, in my book I provide some fictional scenarios, and the interesting thing about those scenarios is that they are all based on actual events that have really taken place in the real world and I have just gone ahead and taken the liberty to put them all into one scenario.

The scenarios are endless, but the things that pop to mind when you talk about fear and uncertainty—and, you know, a lot of the experts out there, a lot of the people in the IT community feel that the term "cyber terrorism" or terrorist use of information technologies is and of itself fear, uncertainty and doubt, something that will never happen because they are not interested in it.

Well, the fact of the matter is, as your question implies, fear and uncertainty and doubt are key components of cyberterror, what they would like to create by using this tactic. So I can imagine a scenario where some of the wireless technologies that I outlined in my testimony at hospitals, for example—you can sit in the parking lot and potentially do things like change blood types in patient records, so that all of a sudden you have people dying of the wrong blood transfusions or getting sick so people will become fearful that that will happen to them if they get put into the hospital.

You have got scenarios where you can have people fearful of putting their money in the market if attacks on the stock market are successful. That is not necessarily maybe terrorism, per se, but it is certainly fear that would have an economic impact on the economy.

Chairman KYL. Well, I appreciate that and that leads to my second question for both of you. You heard the first panel. We discussed the need for a threat analysis, as well as a vulnerability analysis. We have had a lot of the latter, and except for the Defense Department which you pointed out, Mr. Schmidt, I haven't seen a whole lot of the former.

So take the case, for example, of al Qaeda looking at the U.S. stock market. Is it possible that understanding that potential threat as a terrorist threat would cause us to plan differently, to put in place different kinds of protections and to react differently, as opposed to simply looking at it from the back end as a threat-independent situation when it occurs and focusing just on the vulnerability of the system?

In other words, can we protect the infrastructure without understanding and taking into consideration the origin of the activity; i.e. the nature of the threat? Does it help us both to prevent and to deal with the aftermath of an attack if we have been able to understand its etiology rather than just its effect?

Mr. SCHMIDT. You know, that is something we have wrestled with for quite a long time, is trying to determine does the nature of the threat or the source of the threat make any difference on how we are going to protect against it.

Chairman KYL. That is better way to put my long question.

Mr. SCHMIDT. I think most of us in the business agree that irrespective of the nature of the threat, we are going to have to take the same forward steps to protect against anything because we never know. As I mentioned earlier, during NIMDA and Code Red, we to this day don't know the source of that. It could have very easily been a terrorist, it could have easily been a hacker group. But the steps that we have take to protect against that are the same thing as if it were a terrorist attack as well.

It is interesting. The Banking Committee held a hearing in the aftermath of the blackout last year and one of the questions was were we better prepared from a cyber perspective because of much of what we had done as far as vulnerability remediation in that event. And the answer was yes, because the same response mechanism to bring the systems back up and the same ability to identify the systems that are critical to us were in play for either scenario.

Chairman KYL. Let me give you a devil's advocate question, then. Mr. Verton talked about the combination of a physical attack and a cyber attack with a synergistic effect far greater than the effect of either one of them. That is the kind of threat that one would want to be able to anticipate and to deal with that would not come from a hacker or somebody trying to commit a crime, probably.

So wouldn't it make sense to try to anticipate the effect of the combination of those two occurring at the same time, and doesn't that point you more to a threat assessment of terrorism potential as opposed to just hacking?

Mr. SCHMIDT. The simple answer is yes, that is very much the case. The idea of looking at the interdependencies between the physical and the cyber world is something that we originally had that the National Infrastructure Assessment Center is supposed to be working on, looking at the interdependencies, looking at the critical systems and what happens if we do lose the physical aspect of, say, a telecom hotel in New York City. What effect is that going to have on our ability to communicate? Those things are critical, and the protection of those resources is critical as well.

Mr. VERTON. Mr. Chairman, I will just add to that that there is something to be said for knowing your enemy when we start to talk about a threat assessment of any group, al Qaeda or any other terrorist organization.

In terms of knowing your enemy, I would hope—and I have no way to know this—that there are constant red-teaming exercises that are being conducted against the U.S. critical infrastructure, a la Eligible Receiver. I don't know that those are taking place. However, once you have established a capability profile, per se, of a group like al Qaeda, I would hope that the NIE, for example, would have some classified data on who al Qaeda cells have been coordinating with or communicating with in the black hat community, for example, who may, in fact, be working with them, if they are at all.

That would allow us to be able to think like the people who are trying to do us harm and to conduct Eligible Receiver-like red-teaming against the infrastructure to test our own ability to withstand those attacks.

Chairman KYL. And it seems to me also that if we were lucky enough to find some documents of al Qaeda or some other terrorist group that discussed ways of attacking our infrastructure, that becomes part of a threat assessment that adds some texture to the just general understanding we have about the vulnerability of our systems. It gives us a specific reason to be perhaps prioritizing.

Another question here is we have a lot to do and we can't do it all at once. You talked about the need to actually rebuild portions of our infrastructure because they are not secure, and in terms of identifying the priorities one way of doing that would be to focus on what potential threats we thought were most imminent.

Mr. SCHMIDT. That is correct, sir. That is one way to do it. One of the things that I think we have developed in that public-private partnership ever since the President's Commission for Critical Infrastructure Protection in 1996 took place is clear identification to the private sector owner-operators of where their components fit into the bigger structure of the overall infrastructure.

It is kind of an interesting thing because I was with Defense at that time, and as I went out and met with CEOs and met with other folks, they were very focused on their business model and it wasn't very clear to them the dependency that we had in Defense, the dependency we have in Justice, the dependency we had in the economy of their infrastructure. It was just a business to them.

I think we have seen that change slowly but surely as we started to approach Y2K, and then dramatically after the September 11 attacks. We have seen people looking at this. Where do I fit in this big picture and how can I remediate it quickly?

Even though I disagree with the fundamental premise of Rich Pethia saying that there are just too many things to do out there and we will never get them done, we can get things done, but it has to be done on a priority basis and with the economic resources we have, which is a challenge, as you know.

Chairman KYL. Let me ask you a final question. It has been a year since the President put forward the National Strategy to Secure Cyber Space, and you were one of the authors of that. What is your assessment of the progress that we have made in implementing that strategy?

Mr. SCHMIDT. I think we are pretty well on track, and I know there are some folks who are somewhat cynical on that, saying, well, we expect DHS to do more, we expect the NCSD to do more. My answer has been all along that, as everyone has pointed out, 80 to 85 percent of this critical infrastructure is owned by the private sector. So the call to arms was made, the rallying call was there, and the private sector has been organizing amongst themselves.

I flew in on the red-eye this morning from RSA. Senator Bennett was out there, and we have organized now 70 chief security officers of major corporations, from Hershey Foods to Royal Bank of Canada, with us sharing information about how we can better conduct our audits, how we can keep our supply chain going. That is one example of the private sector not waiting for the Government to do something. The expectation was that they have got enough work to do trying to organize DHS and we will continue to call this forward.

In December of last year, we had a cyber security summit and we have held five task forces. As a matter of fact, on March 1 we will have the task force reports that come back, everything from awareness and education to corporate governance. So there has been a lot of movement. It has not been as public as maybe we could have been to advertise it, but the movement continues and I think we are making good progress.

Chairman KYL. Just one suggestion. Make sure they all have a copy of Black Ice. That will get them motivated.

Mr. SCHMIDT. I am still waiting for mine.

Chairman KYL. Mr. Verton?

Mr. VERTON. Mr. Chairman, I will just add to that that the proof is in the pudding. While I applaud the national strategy, all of my work suggests that the current non-regulatory model—and you can make the argument that there is plenty of regulation out there already, but the current non-regulatory model has not worked yet, has not proven itself up to the challenge. I will say otherwise when the situation gets appreciably better in terms of security.

My argument all along was that it is unprecedented in American history that the private sector owns so much of the national security equation today in terms of owning and operating 85-plus percent of the national infrastructure. The problem is they have no mandate to be the defenders of America against these types of attacks.

Traditionally, historically it has fallen to the Federal Government. The model now is hands-off; allow the private sector to do it because the private sector is concerned about losing the ability to innovate, losing the ability to be flexible in their business processes.

Well, the problem has been that there is no pressure from the consumers on the private sector developers of these technologies to change the formula. The buyers are buying what the sellers are selling, and right now I have heard time and time again that the sellers are not necessarily selling very good products from a security standpoint. So until that equation changes, I don't think the national strategy will have much of an effect.

Chairman KYL. In fact, also we encourage a lot of competition and deregulation which results in less and less robust redundancy and infrastructure. Back in the days of the regulated monopolies, for example, of the phone system or the utility systems, there was an awful lot of costly redundancy built into the system. But the companies could afford to do it because they were monopolies.

Now, you have got a lot of competition out there and everybody wants to go right to the margin, so that nobody has the incentive to really invest in that robustness of the system which from a national security perspective we do have to see built in. This is one of the challenges we are going to have to deal with, and getting it right, the degree of mandate versus an expectation that the private sector will do what is in its own best interest. But its own best interest won't necessarily always coincide with national security interests.

Mr. SCHMIDT. Senator, I would like to just make one quick comment relative to Dan. It is sort of disagreement. I bet you there are a whole lot of CEOs that I have talked with and Dick Clarke has

talked with and other folks have talked that believe they do have a mandate. They believe they have a clear mandate to make this infrastructure more secure.

As a matter of fact, about the time we are having this hearing, Bill Gates is going to be making an announcement at RSA. Bill Chambers and everyone is committed, and I believe they understand they have a clear mandate to make it more secure.

Chairman KYL. Well, I appreciate that. That mandate has to be understood all across the spectrum, and there are certainly some leaders and you have certainly mentioned them here. But, obviously, through hearings like this and books and through the good work that you are doing, Mr. Schmidt, and others, we can get the information out there that we have all got a stake in this. To the extent that we all participate in the system, we can help to protect this Nation.

Mr. VERTON. Mr. Chairman, I think the issue is to get that mandate message to the owner of the small utility. Those are the individuals I am really referring to.

Chairman KYL. Yes, and as somebody mentioned before, it is the weakest-link problem that we have here.

Well, I appreciate both of you testifying here today and would appreciate the ability to continue to be in touch with you and have you comment on what we are doing here, on the NIE when it comes out, to the extent you are able to review it, and to provide us with any other information that you think will help us do our job.

I want to make it clear that the hearing record here is going to remain open for questions until 5:00 p.m. on Tuesday, March 2, and for you all to put anything else into the record that you think would be appropriate.

With that, if there is nothing further to come before the Subcommittee, I will declare this hearing adjourned.

[Whereupon, at 11:44 a.m., the Subcommittee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

News from . . .

Senator Dianne Feinstein

of California

FOR IMMEDIATE RELEASE:
Tuesday, February 24, 2004

Contact: Howard Gantman
or Scott Gerber 202/224-9629
http://feinstein.senate.gov

Statement of Senator Dianne Feinstein On The Threat of Cyberterrorism

***Washington, DC** – The U.S. Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security today convened a hearing to assess the current cyberterror threat and examine how well federal agencies and companies are prepared for it.*

Following is the statement of subcommittee ranking member U.S. Senator Dianne Feinstein (D-Calif.):

"You only have to look at the MyDoom virus that recently spread like wildfire across the Internet to understand the threat of cyberterrorism.

MyDoom was responsible for sending 100 million infected emails in its first 36 hours, and accounted for one-third of all emails sent worldwide on one evening.

The virus shut down the website of SCO Group and also attacked the Microsoft website. Damages worldwide ran into hundreds of millions of dollars.

Denial-of-service attacks offer only a small glimpse of the cyberterror threat. A terrorist could theoretically use a computer to:

- open up the flood gates of a dam;
- disrupt the operations of an aircraft control tower;
- shut down the New York Stock Exchange or other important businesses or government agencies; or
- disrupt emergency communications of law enforcement and safety officials.

We've been fortunate so far. There are only a couple of historical examples of cyberterrorism.

- more -

One oft-cited example is an April 2000 incident in Australia where a disgruntled consultant sabotaged the electronic controls to a sewage system, letting loose million of gallons of sewage on a town.

But the threat of cyberterrorism is uniquely insidious. In contrast to attacks on our ports or biological or chemical weapons, cyberterror does not have to be launched within the U.S. geographical confines.

I would also note that 85 to 90 percent of our nation's cyber-infrastructure remains under the control of the private sector.

The Administration has so far embraced a voluntary market-based approach to cybersecurity.

In December 2002, Governor Gilmore criticized this voluntary approach:

'So far, pure public/private partnerships and market forces are not acting ... to protect the cybercommunity.'

I am concerned that we remain under-prepared for a cyberattack, and, like Governor Gilmore, that market forces and public/private partnerships are inadequate.

Here are some questions I hope the panel can address:

- How real is the cyberterror threat?
- Has the Department of Homeland Security placed a high enough priority on defense against cyberterrorism?
- Are we better prepared today to defend against a cyberattack today than on 9/11?
- Is the current voluntary private sector and government collaboration working?
- Is there more we can or should do to defend ourselves?"

###

Forbes.com

On The Cover/Top Stories

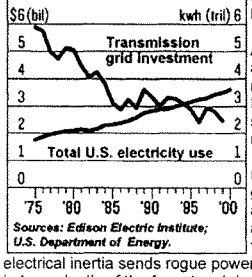
Brawn & Brains

Peter Huber Mark Mills, 09.15.03

The country's trillion-dollar power system would be immensely more valuable if we could find a way to spend a few billion on intelligence for the network.

Transmitting Electric Power

Demand for electricity has risen steadily while investment in transmission capacity has fallen.



Sources: Edison Electric Institute; U.S. Department of Energy.

It now appears that the Aug. 14 blackout began--or at least gathered its destructive momentum--in an hour-long series of line failures and plant shutdowns in northern Ohio, near Cleveland. The final collapse took nine seconds to unfold--a long time, in the power business. This is excellent news--we know how to fix such problems, and relatively cheaply at that. The grid does need more expensive work, too. But first things first. To stop blackouts like this last one, add bits.

As instant pundits were too quick to point out last week, investment in grid assets has declined steadily in recent decades, while electricity demand has risen. Tangled regulatory reasons are to blame, and new investment in grid hardware is now urgently needed. But the grid was not, in fact, particularly stressed on Aug. 14. New power plants and transmission lines probably would not have averted this particular blackout.

Put aside the big plants that generate the power. The expensive parts of the grid itself are the wires--some 680,000 miles of transmission backbone and another 2.5 million miles of wires for local distribution. Because they're so long, and carry so much current, they store huge amounts of energy in the magnetic fields that surround them. When loads or supplies change quickly, this electrical inertia sends rogue power sloshing up and down the system, like waves in a bathtub that move water independently of the faucet and drain. Grid engineers call this "reactive" power--the wires appear to contain malignant generators of their own.

Engineers maintain and restore order, if they can, at "interties" and "substations." These switching points can flatten out or at least isolate the waves, by routing power in and out of different lines and through huge transformers and capacitors. High-power switches thus add order to the grid much as microscopic gates add logic to a Pentium.

The grid's "supervisory control and data acquisition" (Scada) networks move the bits that control the power. Sensors and dedicated communications links feed information about the state of the grid to regional transmission authorities and utility control centers, and the latter control the switches. With real-time access to Scada networks in Ohio, utilities across the Northeast could, in principle, have seen the problem coming, and activated protective switches before the giant wave swept east to overpower them.

But utility Scada networks have evolved piecemeal over the decades, and regulators have recently pushed the physical interconnection of power lines far out ahead of the interconnection of the data networks, and the deployment of software systems to provide automated monitoring and control. As currently engineered, the grid moves megawatts of power much farther and faster than it moves megabits of vital information.

This creates a relatively cheap opportunity for fairly quick improvement. Scada hardware and engineering services--provided by **GE** (nyse: GE - news - people), **Siemens** (: SI - news - people), Schneider Electric, **Rockwell Automation** (nyse: ROK - news - people) and dozens of smaller vendors--generate some $3 billion per year in global revenues--pocket change compared with what's spent on the physical networks that Scada networks control. "Advances in Scada, telecom and computing provide us now with significant opportunities for technology solutions to manage the grid more reliably," says Van Wardlaw, vice president of Electric Systems Operations at the Tennessee Valley Authority. "They offer us some unique solutions that were not even available

to use five or ten years ago."

Control networks have their vulnerabilities, too, of course. Utility Scada systems have reportedly been probed by al Qaeda terrorists, and cyberattacks against these systems have certainly been multiplying rapidly. Scada systems "have generally been designed and installed with little attention to security" and are "highly vulnerable to cyberattack," concludes a recent report by Sandia National Labs, the federal entity in charge of promoting Scada security. "[S]ecurity implementations are, in many cases, nonexistent or based on false premises." But keeping the grid's control networks disconnected and comparatively stupid only increases the vulnerability of the physical assets, which are far harder to protect.

Scada networks need more and better instrumentation, too, and much more advanced software for automated control. At present, the grid has far too few sensors to monitor current, voltage and line temperature in real time, along with the status of capacitors, transformer oil, insulators, switch contacts and hundreds of other variables needed to provide effective advance warning of meltdowns. On-site power networks in many factories are monitored far more closely, and make much more sophisticated use of predictive failure algorithms.

Then, finally, the grid needs more and better strategically placed gates. Roughly speaking, each utility, at present, is expected to protect all its neighbors from faults on its own grid. But with real-time access to regional information, utilities could and would take steps to protect their own grids from problems unfolding elsewhere.

Almost all the grid's logic is currently provided by electromechanical switches. Ultrahigh-power silicon switches manufactured by companies like **International Rectifier** (nyse: IRF - news - people), **Fairchild Semiconductor** (nyse: FCS - news - people) and Powerex (a GE-Mitsubishi joint venture) can now control power flows much faster, more precisely and more reliably. Cyberex (a **Danaher** (nyse: DHR - news - people) business) and GE-Zenith Controls, for example, now build truck-size cabinets containing arrays of solid-state switches that can handle from several kilowatts to as much as 35 megawatts. These systems already play key roles in securing power supplies at military bases, airport control hubs and data and telecom centers. At ultrahigh-power levels--up to 100 megawatts--enormous custom-built arrays of solid-state switches are now being used to interconnect and isolate high-power transmission lines at about 50 grid-level interconnection points worldwide.

Meanwhile, the private sector has deployed 80 gigawatts of generating capacity--about 10% of the capacity that lights the grid--to back up (or substitute for) grid power. Another 3% to 5% of the public grid's capacity is backed up by arrays of batteries (and ancillary electronics) that cushion delicate equipment from electrical blips and supply power during blackouts ranging from minutes to hours. The bigger backup systems are controlled by local-area Scada networks of their own, as are all the electrically powered pumps and valves that control pipelines and industrial plants. New links between the private and public power-control networks would make it easier for private equipment to help relieve the pressure when the public grid gets dangerously overloaded.

With advanced control software, interconnected data networks and high-speed, high-power switches at key locations, the grid can become as smart as it is powerful. Power suppliers know where to put the software and the switches. Will they be given the economic incentive to do so?

Peter Huber, a Manhattan Institute senior fellow, is the author of *Hard Green: Saving the Environment From the Environmentalists* and the *Digital Power Report*. Find past columns at www.forbes.com/huber.

STATEMENT OF SENATOR JON KYL
CHAIRMAN
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY
SENATE JUDICIARY COMMITTEE

"VIRTUAL THREAT, REAL TERROR —
CYBERTERRORISM IN THE 21ST CENTURY"

24 FEBRUARY 2004

Overview

On January 27, the Subcommittee on Terrorism, Technology, and Homeland Security examined the security of our seaports, and their vulnerability to terrorist attacks. Today, we will examine the security of cyber infrastructure, and its vulnerability to cyberterrorist attacks.

As the world has grown more connected through the Internet and cyberspace, the dangers associated with attacks on that technology have also increased. The quantity and quality of cyber attacks are on the rise. The number of computer security intrusions increased from 84,000 in 2002 to 137,000 in 2003.[1] Computer viruses are spreading at much faster rates and causing more damage than ever before. While it took 26 hours for a virus in 2001 to infect 300,000 machines worldwide, a virus in February 2003 infected 300,000 machines within only 14 minutes.[2] As Secretary Ridge stated in December, "anywhere there is a computer . . . whether in a corporate building, a home office, or a dorm room . . . if that computer isn't secure, it represents a weak

---

[1]CERT Coordination Center, *CERT/CC Statistics 1988-2003*, available at http://www.cert.org/stats/cert_stats.html.

[2]Fiona Harvey, *Online Crime Set to Rise: Cyberspace: The Fight Against Hackers Is a Big Burden*, FIN. TIMES (London), Dec. 3, 2003, at 3.

link. Because it only takes one vulnerable system to start a chain reaction that can lead to devastating results."[3]

Since 1997, the Subcommittee has held seven hearings on cyber attacks and critical infrastructure protection. During the most recent of these hearings,[4] witnesses expressed concerns about terrorists conducting cyber attacks against the United States. Terrorists already use cyber tools to raise funds and organize physical attacks; they could use those same tools for conducting cyberwarfare. In 2000, FBI Director Louis Freeh testified before the Subcommittee that cyberterrorism was "a very real, though still largely potential threat."[5] Today's hearing will focus on the status of that threat now, and what we are doing to reduce that threat.

Terrorists are targeting our cyber infrastructure, and we must educate the public about the threat of cyberterrorism. According news reports, data from al Qaeda computers found in Afghanistan show that the group had scouted systems that control critical U.S. infrastructure

---

[3]Secretary Tom Ridge, Remarks at the National Cyber Security Summit (Dec. 3, 2003).

[4]*See Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107th Cong., 1st Sess. (July 25, 2001) (S. Hrg. 107-366, Serial No. J-107-22); *Cyber Attack: Improving Prevention and Prosecution: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (Apr. 21, 2000) (S. Hrg. 106-838, Serial No. J-106-79).

[5]*Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106th Cong., 2nd Sess. (Mar. 28, 2000) (S. Hrg. 106-839, Serial No. J-106-72), at 28 (written statement of Hon. Louis Freeh).

systems.[6] An attack on these systems could have devastating results, especially if done in conjunction with a physical attack. A study by the National Infrastructure Protection Center concluded that the effects of September 11 would have been "far greater" if launched in conjunction with a cyber attack disabling New York City's water or electrical systems.[7] An attack on these systems would have inhibited emergency services from dealing with the crisis, and turned many of the spectators into victims.

Witnesses

The Subcommittee will hear from six witnesses, three experts from the federal government and three experts from the private sector.

Deputy Assistant Director Keith Lourdeau, Cyber Division, FBI

Keith Lourdeau is the Deputy Assistant Director of the FBI's Cyber Division. He had previously served as Assistant Special Agent in Charge of the St. Louis Division, where he was responsible for the daily operation of the Division. Mr. Lourdeau entered the FBI in 1986 and has served in the Chicago, Little Rock, and St. Louis field offices. While serving at FBI Headquarters, Mr. Lourdeau was detailed to the CIA to assist in establishing a new initiative

---

[6]David McLemore, *On the Cyberterror Front Lines; San Antonio Carving a Niche by Helping Protect Vital Systems*, DALLAS MORNING NEWS, Sept. 21, 2003, at 31A.

[7]National Infrastructure Protection Center (NIPC), *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption*, at 7 (July 2002). NIPC's functions have since been assumed by the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate (IAIP), which is under the direction of the DHS witness, Director Amit Yoran. NIPC was formerly part of the Department of Justice.

between the CIA and the FBI in targeting international organized crime groups.

Director Amit Yoran, National Cyber Security Division, DHS

Amit Yoran is the Director of the National Cyber Security Division for the Department of Homeland Security. Previously, he served as the Vice President for Managed Security Services at Symantec Corporation where he was primarily responsible for managing security infrastructures in 40 different countries. Before working in the private sector, Mr. Yoran was the Director of the Vulnerability Assessment Program within the Computer Emergency Response Team (CERT) at the Department of Defense and the Network Security Manager and the Department of Defense where he was responsible for maintaining operations of the Pentagon's network.

Assistant Attorney General John Malcolm, DOJ

John Malcolm is the Deputy Assistant Attorney General in the Criminal Division of the Department of Justice. He oversees the Computer Crime and Intellectual Property Section, the Child Exploitation and Obscenity Section, the Domestic Security Section, and the Office of Special Investigations. An honors graduate of Columbia College and Harvard Law School, Mr. Malcolm served as a law clerk to judges on both the United States District Court for the Northern District of Georgia and the 11th Circuit Court of Appeals.

Dan Verton, Author

Dan Verton is the author of *Black Ice: The Invisible Threat of Cyberterrorism*, a book

analyzing al Qaeda's ability to conduct cyber attacks and U.S. vulnerability to cyberterrorists. He is also a senior writer on the staff of Computerworld, covering national cyber security and critical infrastructure protection. Mr. Verton is a former intelligence officer in the U.S. Marine Corps, where he served as senior briefing officer for the Second Marine Expeditionary Force and analyst in charge of the Balkans Task Force from 1994 to 1996.

Howard Schmidt, eBay

Howard Schmidt is the Vice President and Chief Information Security Officer for eBay. Prior to that, Mr. Schmidt served as the Chair of the President's Critical Infrastructure Protection Board in 2003, and as the Special Adviser for Cyberspace Security for the White House from 2001 to 2003. Mr. Schmidt has also worked as the chief security officer for Microsoft and as the head of the Computer Exploitation Team at the FBI's National Drug Intelligence Center. And from 1983 to 1994, he was an officer for the Chandler Police Department in Arizona.

Conclusion

Although the United States has not suffered a major cyberterrorist attack, we must continue to improve the security of our critical infrastructure systems. The more dependent we become on technology, the more we must protect it.

We have a distinguished panel of witnesses before us today. I am interested in examining with them the threats and vulnerabilities that we face, and what Congress can do to help prevent

cyberterror and prosecute cybercriminals in the United States and abroad.

I would like to thank Senator Feinstein for her hard work in putting together this hearing. We have always had an excellent working relationship, and I look forward to examining this issue with her.

###

Statement of Senator Patrick Leahy,
Ranking Member, Senate Judiciary Committee
Hearing On
"Virtual Threat, Real Terror: Cyberterrorism in the 21st Century"
February 24, 2004

Today's hearing will examine issues related to the potential misuse of computer technologies to commit terrorist acts.

As Senator Kennedy noted recently in connection with the Republican staff spying and stealing of internal Democratic computer files from the Judiciary Committee computer server, to gain access to sensitive materials it is no longer necessary to act under cover of night, or even to be physically present, as in the Watergate days. We must acknowledge and respond to the threat that devastating terrorist attacks can be launched by breaking into our most sensitive systems from across the globe. Such a cyber attack could cause immense disruption to our energy grid, water distribution systems, financial markets, and medical services. Our ability to thwart these attacks is critical to our protection of the nation's critical infrastructure.

As co-chair of the Congressional Internet Caucus, I have long supported efforts to secure Internet use. Last year, Senator Burns and I worked hard to ensure that tough criminal penalties were added to the CAN-SPAM Act, which among other things, penalized the use of spam to disable networks. In addition, last year I supported the Government Network Security Act, which helps to protect our government computers from the dangers of certain kinds of peer-to-peer software. A few years ago, I joined with Senator DeWine to pass the Computer Crime Enforcement Act, which authorized a grant program to help States prevent and prosecute computer crime. In the 104th Congress, I joined with Senators Kyl and Grassley to enact the National Information Infrastructure Protection Act to increase protection under federal law for both government and private computers and to address the problem of computer-age blackmail in which a criminal threatens to harm or shut down a computer system unless extortionate demands are met. In the 103rd Congress, I authored the Computer Abuse Amendments Act of 1994, which was included as part of the Violent Crime Control and Law Enforcement Act signed by President Clinton. Back in 1986, I sponsored the Electronic Communications Privacy Act, which outlawed tampering with electronic mail systems and remote data processing systems. In 1984, I worked to pass the Computer Fraud and Abuse Act to criminalize conduct carried out by means of unauthorized access to a computer. These are matters on which I have worked and about which I have cared deeply for more than two decades.

While to this point we have been fortunate that terrorists have not been able to infiltrate and dismantle our networks, we can assume, unfortunately, that they would if they had the opportunity. Recent reports about domestic uses of worms and other computer viruses also remind us that our vulnerability is not limited to foreign threats.

The Internet connects government computers with the private sector. It connects computers on the other side of the globe with ones responsible for monitoring our most

sensitive functions, like commercial air traffic control. And it connects us all to one another in a way that makes commerce and government more efficient than ever before. While this has brought us benefits, it has also meant that our vulnerabilities are dispersed more broadly, as well.

It is essential that we work with the private sector to thoroughly assess our weaknesses and take steps to deal with them. It is also critical that we work with our world-class university system, which has developed innovative ways to protect our critical infrastructure. For example, the National Center for Counterterrorism and Cybercrime at Norwich University in my home state of Vermont has come up with cutting-edge approaches to fend off computer attacks and determine the vulnerability level of key systems.

We must ensure that appropriate levels of security and safeguards are in place to prevent abuse and to protect public health and safety. Unfortunately, the Administration has taken a step backward in its promulgation of an interim rule on so-called critical infrastructure information. This rule provides an overly broad exemption from the Freedom of Information Act to virtually any information that private companies voluntarily submit to the Department of Homeland Security. Along with Senator Bennett and Senator Levin, I had worked out a more balanced proposal when the legislation was considered in the Senate. That language is now embodied in the Restore FOIA Act, S.609.

I welcome today's hearing. I look forward to learning more about the Government's assessments of its abilities to prevent cyber terrorism and those of other experts.

And on a personal note, we have seen recent reports that John Malcolm will soon be leaving his post at the Department of Justice to fight piracy for the Motion Picture Association of America. I wish him well in that endeavor.

# # # # #

Testimony of FBI Deputy Assistant Director Keith Lourdeau, Cyber Division
Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security
Hearing on Cyber Terrorism
February 24, 2004

Good Morning Chairman Kyl, and other distinguished Members of the Subcommittee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in combating Cyber Terrorism.

As our nation's economy becomes more dependent on computers, and the Internet becomes an increasingly more integral part of our society, new digital vulnerabilities make U.S. networked systems potential targets to an increasing number of individuals including terrorists. The Director of the FBI has established new priorities protecting the U.S. from terrorist attack as its #1 priority and protecting the U.S. against cyber-based attacks and high-technology crimes as its #3 priority. The FBI's Cyber Division's #1 priority is designated Counterterrorism related computer intrusions.

Within the past several years, the U.S. has been the target of increasingly lethal terrorist attacks which highlight the potential vulnerability of our networked systems. These attacks were carried out by terrorists wanting to harm U.S. interests in order to forward their individual cause. Our networked systems make inviting targets for terrorists due to the potential for large scale impact to the nation. The vulnerabilities to our networked systems arise from a number of sources, such as: easy accessibility to those systems via the Internet; harmful tools that are widely available to anyone with a point-and-click ability; the globalization of our nation's infrastructures increases their exposure to potential harm; and the

interdependencies of networked systems make attack consequences harder to predict and perhaps more severe.

It is also crucial to understand the interrelationship between physical and cyber security in the current technological environment. Coordinated attacks on multiple regions could achieve a national effect. The most elaborate boundary control program of firewalls, intrusion detection, and virus filtering will be of little help if an intruder is able to gain physical access to servers, networks, or sensitive information.

Terrorist groups are increasingly adopting the power of modern communications technology for planning, recruiting, propaganda purposes, enhancing communications, command and control, fund raising and funds transfer, information gathering, and the like. However, mere terrorist use of information technology is not regarded as cyberterrorism. The true threat of "Cyberterrorism" will be realized when all the factors that constitute a terrorist attack, coupled with the use of the Internet, are met.

Cyberterrorism is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services, where the intended purpose is to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda.

To date, cyber attacks by terrorists, or persons affiliated with them, have largely been limited to relatively unsophisticated efforts such as the email bombing of ideological foes or the publication of threatening content. However, increasing technical competency in these groups is resulting in an emerging capability for network-based attacks. Terrorist groups have proven themselves capable of carrying out acts of violence against our nation on a grand scale. The more familiar they become with computers and their potential as a viable weapon against us, the more likely they will try to acquire the skills necessary to carry out a cyberterrorist event.

The FBI assesses the cyberterrorism threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise. Terrorist groups have shown a clear interest in developing basic hacking tools and the FBI predicts that terrorist groups will either develop or hire hackers, particularly for the purpose of complimenting large physical attacks with cyber attacks.

If a terrorist lacked the technical sophistication to conduct a computer attack, and chose to recruit a hacker, potential damage would be increased if that hacker was an insider. Insider attacks originate from a variety of motivations (e.g., financial gain; personal grievances; revenge; recruitment; or coercion). It is not necessarily the motivation that makes insiders dangerous, but the fact that they may have unfiltered access to sensitive computer systems that can place public safety at risk. Moreover, there is an increasing concern over the prevalent trend to outsource, even to foreign conglomerates, for services which were previously handled domestically.

Attacks against regional targets could have a significant effect on computer networks, while coordinated attacks on multiple regions could achieve a national effect with severe repercussions. There are numerous control systems whose destruction would have a far-reaching effect. Large-scale distribution systems, such as those involving natural gas, oil, electric power, and water, tend to use automated supervisory and data acquisition (SCADA) systems for administration. SCADA systems tend to have both cyber and physical vulnerabilities. Poor computer security, lack of encryption, and poor enforcement of user privileges lead to risks to SCADA systems. Poor physical controls can make the disruption of the SCADA system a realistic possibility.

A major method used in preventing cyberterrorism is the sharing of intelligence information. The FBI routinely passes intelligence received in active investigations or developed through research to the intelligence community. Throughout the FBI field offices, Special Agents serve on cyber task forces with other agencies. The FBI is a sponsor/participant in the InterAgency Coordination Cell (IACC) at FBIHQ. This environment of information sharing and cooperation is expanding to include foreign governments such as the "5 Eyes."

Cyber programs are unique in nature. However, taking proactive investigative measures with tools such as Honey Pots/Nets and Undercover Operations enhances our ability to prevent a cyberterrorist attack. The FBI has undertaken the following initiatives to combat cyberterrorism: Cyber Task Forces, Public/Private alliances, International Cyber Investigative Support, Mobile Cyber Assistance Teams, Cyber Action Teams, Cyber Investigators Training, a Cyber Intelligence Center,

and Cyber Tactical Analytical Case Support. These programs provide a strategic framework and program management tool for all FBI computer intrusion investigations.

The Computer Intrusion program provides administrative and operational support and guidance to the field offices investigating computer intrusions, assists other FBI programs that have a computer dimension, and coordinates computer intrusion investigations by various criminal investigative and intelligence components of the Federal Government.

The Special Technologies and Applications program supports FBI Counterterrorism computer intrusion-related investigations with all necessary equipment and technical investigative tools.

The Cyber International Investigative program creates the ability to conduct international cyber investigative efforts through coordination with FBI Headquarters Office of International Operations, Legal Attache offices, and foreign law enforcement agencies.

The Cyber Specialized Training Program coordinates with the Engineering Research Facility, Laboratory Division, Training Division, National White Collar Crime Center, private industry, academia and others to deliver training to FBI cyber squads, Task Forces, International Law Enforcement Officers, and others.

In the event of a cyberterrorist attack, the FBI will conduct an intense post-incident investigation to determine the source including the motive and purpose of the attack. In the digital age, data collection in that investigation can be extremely difficult. The computer industry is also conducting research and development involving basic security, such as developing cryptographic hardware which will serve to filter attempts to introduce malicious code or to stop unauthorized activity. Continued research in these areas will only serve to assist the FBI in its work against cyberterrorism.

While the following two incidents were not cyberterrorism, they are an indication of the ability of individuals to gain access to our networked systems and the possible damage that can result.

In 1996, an individual used simple explosive devices to destroy the master terminal of a hydroelectric dam in Oregon. Although there was no effect on the dam's structure, this simple attack completely disabled the dam's power-generating turbines and forced a switch to manual control. A coordinated attack on a region's infrastructure systems (e.g., the SCADA systems that control Washington D.C.'s electric power, natural gas, and water supply) would have a profound effect on the nation's sense of security. This incident demonstrated how minimal sophistication and material can destroy a SCADA system.

In 1997, a juvenile accessed the Generation Digital Loop Carrier System operated by NYNEX. Several commands were sent that disrupted the telephone service to the Federal Aviation Administration Tower at the Worcester Airport, to the Worcester Airport Fire Department and to

other related entities such as airport security, the weather service, and various private airfreight companies. As a result of this disruption, the main radio transmitter and the circuit which enabled aircraft to send an electronic signal to activate the runway lights on approach were disabled. This same individual then accessed the loop carrier system for customers in and around Rutland, Massachusetts and sent commands that disabled the telephone service, including the 911 service, throughout the Rutland area.

On May 3, 2003, an e-mail was sent to the National Science Foundation's (NSF) Network Operations Center which read, "I've hacked into the server of your South Pole Research Station. Pay me off, or I will sell the station's data to another country and tell the world how vulnerable you are." The e-mail contained data only found on the NSF's computer systems, proving that this was no hoax. NSF personnel immediately shut down the penetrated servers. During May, the temperature at the South Pole can get down to 70 degrees below zero Fahrenheit; aircraft cannot land there until November due to the harsh weather conditions. The compromised computer systems controlled the life support systems for the 50 scientists "wintering over" at the South Pole Station.

The FBI determined that the hackers were accessing their e-mails from a cyber café in Romania. One of the hop points utilized by the intruder was a computer system in Pittsburgh owned and operated by a trucking company. A hop point is a computer system, usually compromised by the intruder, that is utilized to conceal the true location and identity of the intruder. Joint FBI investigative efforts with the Romanian authorities, in this matter, resulted in the seizure of documents, a credit card

used in the extortion scheme, and a computer that contained the very e-mail account that was used to make the demands of the National Science Foundation. On June 3, 2003, two Romanian citizens accused of hacking into the NSF South Pole Research Station were arrested in a joint FBI/Romanian police operation. The two are currently scheduled to stand trial in Romania. A trial date has not been set.

The unique complexity of protecting our nation's networked systems is a daunting task. The key to prevention is effective attack warning and the education of the owners and operators of those systems. The protection of our networked systems is a shared responsibility and partnership between the private sector, state and local law enforcement agencies, U.S. Federal Law Enforcement agencies, the Department of Homeland Security, and the Intelligence Community, both domestic and foreign. The FBI encourages international cooperation to help manage this increasingly global problem.

Defending against a cyber attack also requires the integration of operational, physical, communication and personnel security measures. This involves a full range of matters such as: installing effective passwords, firewall protection, avoidance of unprotected and unnecessarily opened entry points, installation of default configuration and passwords; minimization of placing servers in unprotected areas; and vigilance against disgruntled employees. System administrators must be both vigilant and serious about cyber security.

Synopsis: **According to how we have defined cyberterrorism, no cyberterrorist attack has**

occurred to date. However, in the future cyberterrorism may become a viable option to traditional physical acts of violence due to: its perceived anonymity, the proliferated number of networked targets, its low risk of detection, its low risk of personal injury, low investment requirements, and increased ease and access from various locations. The protection of our networked systems requires the integration of many components and is a shared responsibility between all sectors of our society. The FBI can not do this alone.

Department of Justice

STATEMENT

OF

JOHN G. MALCOLM
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY AND
HOMELAND SECURITY

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

CONCERNING

CYBERTERRORISM ISSUES

PRESENTED ON

FEBRUARY 24, 2004

Testimony of Deputy Assistant Attorney General John G. Malcolm on Cyberterrorism
Before the Senate Judiciary Committee
Subcommittee on Terrorism, Technology and Homeland Security
February 24, 2004

Good morning, Chairman Kyl, Senator Feinstein, and Members of the Subcommittee. On behalf of the Department of Justice, I would like to thank you for inviting me to appear before you this morning to discuss the important issue of cyberterrorism.

The Department of Justice's role in responding to cyberterrorism is shaped in large measure by the "President's National Strategy to Secure Cyberspace," which calls upon our entire society -- the federal government, state and local governments, the private sector, and the American people -- to engage in coordinated and focused efforts to secure cyberspace. Under the National Strategy, the Department of Justice and the FBI are charged with leading the national effort to investigate and prosecute cybercrime. Our role as law enforcement defines what it is that we do, namely, act to prevent and deter cybercrime; investigate cybercrime incidents; and identify and prosecute people who violate federal laws.

While we prevent and respond to cybercrime incidents, we do not do so in the same manner as the Department of Homeland Security ("DHS"). While DHS is responsible for identifying and protecting against "vulnerabilities" in the information infrastructure, we focus on responding to "threats" presented by intentional, unlawful acts that threaten the confidentiality, integrity, and availability of information networks.

I. Cyberterrorism – What is It?

Cyberterrorism involves the use of computer systems to carry out terrorist acts, which are, in turn, defined by reference to specific criminal statutes. True cyberterrorism is characterized by large-scale destruction (or the threat of such destruction) coupled with an intent to harm or coerce a civilian population or government.

There are many misconceptions about cyberterrorism. Not all cyberattacks are acts of cyberterrorism. In fact, the vast majority of network intrusions are committed by those who lack terroristic intent. Common examples of people who perpetrate cyberattacks, but who are not cyberterrorists would be so-called "script kiddies" who hack into computers for fun, sophisticated hackers who enjoy the challenge of exploiting security vulnerabilities, and disgruntled employees who seek revenge against their employers.

Even politically-motivated "hacktivists" who deface web sites in order to convey a political message will rarely qualify as cyberterrorists. For instance, the Department recently prosecuted an individual who hijacked the news agency Al Jazeera's web site, replacing it with his own political message. While these defacements can damage computer systems and networks, they do not usually cause the type of large-scale destruction that is implicit in cyberterrorism.

Attacks on critical infrastructure, on the other hand, have the potential for large scale disruptions and mass casualties, and may, depending on the motivation of the attacker, be linked to cyberterrorism. Examples of critical infrastructures include: telecommunications networks; transportation systems and services; water supply systems; energy systems; financial systems; and emergency services, including medical, police, fire, and rescue services. The issues of cyberterrorism and critical infrastructure protection ("CIP") are often intertwined for understandable reasons.

II. Cyberterrorism – What Has the Department of Justice Done to Prepare?

The Department is concerned about any unlawful computer intrusion, but most especially those that have the potential to affect critical infrastructure or which raise the specter of cyberterrorism. The motivation behind any particular cyberattack may not always be apparent at the outset of an investigation. For instance, in 1997, a juvenile hacked into the Bell Atlantic computer system, causing a system crash that knocked out power to the Worcester, Massachusetts airport. Ultimately, it was determined that the individual lacked terroristic intent, but the hack was nonetheless criminal and potentially life-threatening.

In light of the uncertainty regarding motive, prudence dictates that we respond to all cyberattacks in the same manner. After all, if the attack in question can be perpetrated by an ordinary criminal, it can certainly be perpetrated by a cyberterrorist. While we have been fortunate enough not yet to experience a devastating act of cyberterrorism or a crippling attack on

a critical infrastructure, the hard lessons of 9/11 teach us that preparation is critical.

Domestic Efforts

A. CCIPS

The Department has developed specialized expertise in the area of cybercrime. The Computer Crime and Intellectual Property Section ("CCIPS"), which I oversee, has a team of 37 attorneys who focus exclusively on issues relating to computer and intellectual property crime, and who respond daily to requests for information and advice from the 94 U.S. Attorneys' Offices across the nation. In addition, the Section coordinates multi-district cases and engages in important education and outreach efforts, providing hundreds of hours of training each year to prosecutors, agents, judges, technical experts, and government and industry groups. CCIPS has also published significant reference manuals for prosecutors, including one on *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.*

B. CTC Network

Another important component of the prosecutorial framework is the network of Assistant United States Attorneys who have been designated Computer and Telecommunications Coordinators ("CTCs"). Each district has at least one CTC (there are a total of 212 CTCs) who receives special training from CCIPS so that he or she can function effectively as a resource for

their district and as a point of contact for multi-district cases. Recent training sessions have emphasized the prosecutor's role in critical infrastructure protection and the importance of fostering communications with our military counterparts, including the Joint Task Force Global Network Operations (JTFGNO).

C. CHIP Units

There are also a total of thirteen Computer Hacking and Intellectual Property ("CHIP") Units comprised of specially-trained personnel, including prosecutors. The location of these specialized units was based on a number of factors, including their proximity to high-tech industry areas, their potential for growth in that area, and the presence of adequate FBI resources to investigate these crimes. In addition to prosecuting cases, the CHIP units focus on the prevention of cybercrime by working with local industry to anticipate future trends, identify vulnerabilities, and stop cybercrime before it occurs.

D. Partnerships

The Department has focused not only on developing internal expertise, but also on developing partnerships with other federal agencies, with state and local law enforcement, and with industry organizations. We work particularly closely with DHS's National Cyber Security Division ("NCSD") so that it can fulfill its mission of analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure

information systems. In turn, NCSD supports the Justice Department's mission of investigating and prosecuting threats and attacks against cyberspace. The Department also works with DHS as part of the Cyber Interagency Incident Management Group ("Cyber IIMG"), which develops response plans so that federal agencies will be prepared to respond in the event of a cyberterrorist attack or other cyber crisis.

At the state and local level, the Department participates on the National White Collar Crime Center's Cybercrime Advisory Board, which provides recommendations on issues of cybercrime collaboration among law enforcement, academia, and the private sector. The National White Collar Crime Center is a non-profit organization funded by Congress that provides support services to state and local law enforcement agencies and other organizations with an active interest in the prevention, investigation, and prosecution of economic and high-tech crime.

The Department has also worked with the National Association of Attorneys General ("NAAG") to compile the Computer Crime Point-of-Contact List, a 50-state list of state and local prosecutors and investigators who are responsible for computer-related crimes within their respective jurisdictions. This list allows agents and prosecutors from one jurisdiction to call upon their colleagues in another jurisdiction for rapid response in cybercrime matters.

We have also developed productive relationships with business and industry organizations. The Department has supported the FBI and the National Infrastructure Protection

Center ("NIPC") in developing the "InfraGard" initiative, which expands direct contacts between government and private sector infrastructure owners and operators and encourages the sharing of information about computer intrusions, vulnerabilities, and infrastructure threats. Since the NIPC became part of DHS, the Department has continued to engage in regular outreach through InfraGard to ensure that communication channels are open between government and the private sector.

International Efforts

Because cyberattacks frequently transcend geographic boundaries, the Department's cybercrime initiatives have not been confined to the United States. It is vitally important to have foreign counterparts who are technologically capable, who are accessible and responsive, and who have the necessary legal authority to cooperate with us and assist in our investigations and prosecutions in the event of a trans-border cyber incident.

A. G8 Subgroup on High-Tech Crime: 24/7 Network

We are working hard to build strong relationships with foreign counterparts so that the framework will be in place to quickly respond to cybercrimes, including large-scale cyber incidents. For example, CCIPS chairs (and has chaired since its inception in 1997) the G8 Subgroup on High-tech Crime. One of the most significant achievements of this Subgroup is the creation of the "24/7 Network," which allows law enforcement in the participating countries to

reach out – 24 hours a day, 7 days a week – to counterparts in other countries for rapid assistance in investigating computer crime and preserving electronic evidence. Often, cyber-criminals can be identified only if evidence of their conduct is preserved within minutes, a time-frame that is way too short for us to rely on traditional international assistance options.

Currently, 35 countries participate in the 24/7 Network. This network has been used successfully in many instances to investigate threats and other crimes in a number of countries, including the United States. Because terrorists operate throughout the world, it is critical that we continue our efforts to expand the Network in order to ensure that our law enforcement capabilities are coextensive. When it comes to combating cybercrime across international boundaries, the chain is truly only as strong as its weakest link.

B. OAS

The Department is active on several committees of the Organization of American States ("OAS") that relate to cybersecurity. OAS is the regional governmental organization for nations in North, Central and South America and the Caribbean. A senior attorney from CCIPS chairs the OAS Group of Government Experts on Cybercrime, and a CCIPS delegation recently traveled to Mexico to conduct training on drafting cybercrime laws for legislators, senior policy makers, and law enforcement officials.

C. APEC

We have worked with other regional governmental groups, including the Asia Pacific Economic Cooperation Forum ("APEC"), on issues relating to cybercrime. Specifically, CCIPS has been involved with APEC's Telecommunication and Information Working Group, which has sought to strengthen the capacity of institutions through the Cybercrime Legislation and Enforcement Capacity Building Project and the Computer Emergency Response Team Awareness Raising and Capacity Building Project. During the past year, CCIPS attorneys traveled to Thailand to conduct training on drafting cybercrime legislation.

We intend to continue our work towards improving the quality of cybercrime legislation and response mechanisms in other regions of the world. Much of our international work requires the cooperation of other federal agencies, such as the State Department's Office of International Narcotics and Law Enforcement Affairs, which has provided funding for developing international cybercrime enforcement capacity. We believe that improved laws will not only serve as a deterrent, but will also increase the overall prosecution of cybercriminals, including cyberterrorists, who would seek to operate in otherwise lawless nations.

III. <u>What Legal Tools Are Available to Respond to Cyberterrorism?</u>

A. Substantive Laws

There are a number of criminal statutes that might apply to a given cyberattack depending on the circumstances. For instance, the Computer Fraud and Abuse Act (18 U.S.C. § 1030) prohibits, among other things, unlawfully accessing classified information; obtaining information without authorization from a government computer or federal agency; and causing damage to a protected computer that results in physical injury, a threat to public health or safety, or damage to a computer system used for purposes of national defense or national security. The Department has prosecuted numerous cases under § 1030, including:

- a January 2004 conviction of a hacker who damaged computer systems belonging to eBay and Qualcomm using a Trojan program that allowed him to obtain user names and passwords;
- another January 2004 conviction of a hacker who illegally accessed the New York Times's internal computer network, including a database containing information and social security numbers for 3,000 individuals; and
- the arrest in August and September 2003 of two individuals charged with distributing variants of the Blaster computer worm.

Specific terrorism statutes might also apply in the event of a cyberattack. For instance, 18 U.S.C. § 2332b criminalizes acts of terrorism that transcend national boundaries. Other statutes might apply to domestic cyberterrorism. In one case in which an individual claimed to have electronic evidence of a missile threat targeting the opening ceremonies of the 2002 Olympic Games in Salt Lake City, which turned out to be a hoax, the individual was charged under 18

U.S.C. § 844 for making false threats regarding explosives.

Penalties for acts of cyberterrorism are great. Under the Homeland Security Act of 2002, cyberattacks that result in serious bodily injury are punishable by up to 20 years in prison. If the attack results in death, punishment may be up to life imprisonment. The U.S. Sentencing Guidelines were also modified recently to provide for an upward departure in cases where the disruption to critical infrastructure resulted in a debilitating impact on national security, economic security, public health or safety.

B. Procedural Laws

In addition to substantive laws, the Department relies to a large extent on procedural laws, which are particularly important in cybercrime cases because cyber-criminals are quite adept at covering their tracks and electronic evidence can be lost in a fraction of a second. I would like to take a moment to briefly describe the vital role that the USA PATRIOT Act plays in our CIP and cyberterrorism efforts.

Crucial provisions in the Act allow computer service providers to voluntarily disclose subscriber communications in the event of an emergency without fear of incurring civil liability. In one instance, high school officials cancelled classes and sent bomb-sniffing dogs through the school in response to an anonymous death threat posted to an Internet message board. The owner and operator of the message board initially resisted disclosing the evidence on his computer that

could be used to identify the threat-maker because he had been told that he would be liable if he volunteered anything to the government. Once the message board owner/operator understood that the USA PATRIOT Act had created an emergency provision allowing the voluntary release of information, he disclosed evidence that led to the timely arrest of a student at the high school. The student ultimately confessed to making the threat. The message board owner/operator stated that he had been worried for the safety of the students and teachers at the high school and was relieved that he was able to help because of the change in the law.

Another invaluable provision in the USA PATRIOT Act permits courts to issue nationwide search warrants for electronic communications. This provision has relieved the heavy administrative burden for prosecutors and judges in the districts that are home to the large Internet service providers. More importantly, the efficiency has preserved time-sensitive evidence in cases in which the evidence might otherwise have been lost, such as one involving the tracking of a fugitive and another involving the theft of trade secrets. Such procedural means of obtaining expedited access to electronic communications will undoubtedly be crucial in the event of a cyberterrorist incident.

I could talk at length about the importance of the USA PATRIOT Act, but in the interest of time, I will keep my remarks brief. You are no doubt aware that many of the USA PATRIOT Act's provisions are currently set to expire. Because the Department has relied on these provisions in numerous instances to conduct successful prosecutions, and because these provisions would be essential to any prosecution for cyberterrorism, I urge you to not allow these

provisions to sunset.

V. Conclusion

As you can see, we are working on multiple fronts – both domestic and international – to address cyberterrorism and attacks on critical infrastructure. Our many efforts are intended to strengthen the communication systems necessary to ensure that cybercrime is successfully prosecuted. Thus, we have focused on building relationships with state and local law enforcement, with business and industry, with other federal agencies, and with our foreign counterparts so that we can move quickly to respond to cyberattacks of any sort.

While I would like nothing better than to be able to assure you that an act of cyberterrorism will never occur, unfortunately, I cannot do that. I can, however, assure you that the Department is taking – and will continue to take – the necessary steps to prepare to respond appropriately in the event of a cyberterrorist attack.

I thank you again for allowing me the time to address the Subcommittee on this very important issue. I would be happy to answer any questions that you may have.

TESTIMONY BEFORE THE JUDICIARY COMMITTEE ON CYBER TERRORISM U.S. SENATE

By Howard A. Schmidt
Vice President and Chief Information Security Officer
eBay Inc.

Introduction

Senator Kyl, Senator Feinstein, distinguished members of the Committee; my name is Howard A. Schmidt. I am the Vice President and Chief Information Security Officer for eBay, where I lead a team responsible for ensuring the trustworthiness and security of the services that bring so many global citizens together in a vast global marketplace each day. I would like to thank you for the opportunity to come before this Committee as well as your continued leadership on this very important issue. Prior to my current position at eBay, I had the privilege of being appointed by President Bush, along with Richard Clarke, to lead the President's Critical Infrastructure Protection Board, which represented one part of the overall governmental response to the threat of cyber security attacks in the wake of September 11. I retired from 31 years of public service after completing and publishing the "National Strategy to Defend Cyberspace," working with a team of dedicated public servants, this distinguished body and the American public.

I have had the privilege of working with committed individuals in the private sector, law enforcement, and government to forge the collaboration and cooperation that is so essential to safeguard cyber space for everyone, from inexperienced home users to large well-run corporate enterprises. I assisted in the formation of some of the first collaborative efforts in the law enforcement community to address cyber crime with local law enforcement, the FBI, Secret Service and the dedicated military criminal investigators. I also helped lead the creation of the Information Technology Information Sharing and Analysis Center (IT-ISAC) and had the honor of serving as its first President.

I continue to proudly serve in the U.S. Army Reserves, assigned to the 701st MP Group, (CID) as a Special Agent with the computer crime unit at CID headquarters. I also serve on the Board of Directors for ISC2, the body that oversees certification of security professionals through the CISSP certification. And, I serve on the Information Security Privacy Advisory Board, appointed by the Secretary of Commerce to advise NIST, CSD and OMB.

My remarks today will focus primarily on the cyber security threats that we find within business and government; some insights into public-private cyber security partnerships and their effectiveness; and finally, some recommendations of things that we

can do to further improve security for consumers, enterprises of all sizes, educational institutions and government systems.

Today, it is estimated that the Internet connects over 840 million users, with an estimated growth to 904 million by the end of 2004. From major data operations conducting large-scale financial transactions, to wireless devices keeping families connected, the Internet touches virtually all aspects of our economy and quality of life. eBay is a prime example of how deeply ingrained the Internet is in American life. Every day on eBay, millions of Americans, along with millions of people in countries around the world, come together to buy and sell all types of goods and services. Business relationships and, often, deep friendships are formed on the basis of commerce and shared interests. The eBay marketplace reflects the enormous power of the Internet to unite humanity at a crucial moment in history.

More pointedly, the Internet has become a fundamental component of business processes by enhancing productivity through faster connectivity between remote locations or across functional operations. The Internet is deeply embedded in managing power, producing chemicals, designing and manufacturing automobiles, managing money and delivering government services ranging from passport services to environmental permits. Tragically, the flip side of these productivity-enhancing applications is an increase in attacks against the online community.

Today, the Internet is utilized by hundreds of millions of users all across the globe sending information ranging from homework assignments and simple greetings to the most sensitive financial and operational data of government and industry, all at the speed of light. The Internet landscape includes a private sector security industry that has grown to an estimated $17 billion per year in goods and services. And, as we are all painfully aware, attack speeds today are now measured in seconds, not days.

Threats:

During the Cold War many of the threats we identified surrounded nation states, foreign doctrine and intelligence. Threat data was often based on movements of troops and supplies, development of weapons systems that required procurement of goods and materials that provided telltale information of intent and capabilities. The threats against Critical Information Infrastructure are much different. We do not have early warning systems, or see electronic movement that indicates that some system or systems have been targeted; we do not have a single hardened point that we can secure and say we are protected. Often when we do see something it is too late.

I am often asked about the use of the term "cyber-terrorism" and I refrain from using such a term. To many of us in the "cyber security" business, it makes no difference if the attack comes from the Midwest or the Middle East, Eastern Europe or northern Arizona, so long as it is disruptive to the smooth and reliable operation of our Critical Information Infrastructure.

The threats we do see manifest themselves in various formats: Denial of Service attacks (DoS); hacking; "phreaking"; authentication attacks; identity theft; "phishing" and malicious code (virus, Trojans, worms etc.). To try to articulate a specific threat at any given time is almost impossible – the attacks come from nowhere with no warning. What we do know and what we can identify are the vulnerabilities. Reducing vulnerabilities must be our focus. We once had vulnerability identification and remediation done on an annual basis, then semi-annual and we now have reached a point where vulnerability identification and remediation needs to be done "on demand" at a near real-time basis. The technology currently exists to facilitate this through web-based services. The Department of Defense, who has long been a leader in the public sector in cyber security, had shown that over 98% of successful incursions into DoD systems COULD have been prevented by eliminating known vulnerabilities.

We also have a new category of threats that exploit a single machine now connected to the wonderful broadband capabilities that cable modems and DSL connectivity provide us. The criminals that exploit these single system attacks can harness resources formerly found only in massive enterprises. These single system attacks use automated tools to allow them to take over tens of thousands of broadband machines and have a greater affect than the major Distributed Denial of Service (DDoS) attacks we all suffered in February 2000. DDoS attacks continue to be a favor target of worms, Trojans and viruses.

The ability to use strong authentication and encryption when logging into systems and even doing simple daily tasks like sending email provides yet another vector of vulnerabilities that can be exploited. One of the common ways to takeover a system is to use common hacking tools to "hijack" someone's electronic identity and become an insider. Once inside these people use other tools to identify other vulnerabilities to give themselves greater privileges until succeed in controlling the system. None of us would intentionally send sensitive information through the mail system on the back of a postcard but effectively we do that every day using email. Although easy-to-use technologies such as PKI ("Public Key Infrastructure") are available to protect sensitive data, they are mostly ignored..

The concept of "zero-day vulnerabilities" is closer to reality then ever before. In the recent past as vulnerabilities were made public, it often took months before the ability to exploit the vulnerability was available. The window between vulnerability and exploitation is closing rapidly, from weeks to hours. Formerly, the technical skills to create an exploit were limited to the "elite," but we now see exploit tools to write viruses, Trojans and worms that can be easily modified by novices, often referred to as "script kiddies."

The last point on threats is the new creation of what we call "blended threats," a malicious program that seeks out not just one vulnerability but also any one of a number of potential vulnerabilities and looks to exploit each one in turn. Two of the most virulent of these were called "Code Red" and "NIMDA," neither of which have we

identified the criminals that launched these attacks nor the motives behind these attacks. NIMDA is especially troubling since it was launched one week after the September 11th attacks.

PRIVATE PUBLIC PARTNERSHIPS:

During the formulation of the National Strategy to Defend Cyber Space, we at the White House held a series of town hall meetings with private-sector partners. These town hall meetings were open to the public and well-attended, with speakers ranging from CEOs of major financial institutions and exchanges, to subject-matter experts in cyber security. Many of these town hall meetings were webcast so those that could not attend in person could participate over the Internet.

Private sector companies have also held free seminars around the country to increase awareness of citizens. Many of the sessions focused on informing the elderly, one of the segments of our society that has received great benefit from the online world. Just this past holiday shopping season there was mass media campaigns to educate consumers on how to safely and securely enjoy the richness and robustness of the online e-commerce world.

In the category of formal education, the National Security Agency (NSA) has a program identifying universities to be designated as centers of academic excellence in information security. This NSA program not only ensures the education of the next generation of information security professionals, but also guarantees that each university has sound cyber security practices in place. The academic excellence program provides awareness education for students, who make up a large number of online users and consumers. The NSA also administers the Cyber Corp program with the National Science Foundation and OPM, providing scholarships for students in cyber security.

Another major improvement in the past two years is the way security enhancements are now standard parts of software and hardware. One very visible example is the hardware provided to use wireless technology. Broadband technology (Cable modem, DSL, satellites etc.) has given us capabilities and speeds that were before only available to corporations. We now see firewalls and the ability to download anti-virus software being built into wireless modems. More importantly, firewalls and encryption are now turned on by default rather than waiting for users to install these protections.

The major computer operating systems now have auto-update features and will soon be turned on by default in future versions. Some products that have services that can be exploited are now being shipped with these vulnerable services turned off by default, and thus, making them more secure. Many online email services block potentially malicious code and do a much better job of blocking Spam that contains malicious functions.

Anti-virus vendors have done an amazing job in speeding up the detection, analysis and updates for many of the viruses that are found in the "wild." Many of them even provide free online virus scans as a public service to assist consumers.

There have been a number of government actions that have taken place; most notably the creation of the President's Critical Infrastructure Protection Board and the release of the National Strategy to Defend Cyberspace. This critical document provides a framework for many of our successful private-public partnerships, including home users and small/medium enterprises.

I would also contend that the consolidation of cyber security-related organizations into the Department of Homeland Security (DHS) under the Infrastructure Protection Director has been a positive action. Bringing together the NIPC (FBI), Fed-CIRC (GSA), CIAO (Commerce), Energy Information Assurance Division (DoE) and the National Communications System (DoD) has created a center of excellence that, with the help of focused leadership, will move to implement our national strategy. This new organization is called the National Cyber Security Division.

Recent action taken by DHS to create the US CERT at Carnegie Mellon University has the potential to significantly enhance security for all users. The US CERT is designed as a focal point for a cyber security response network and providing a notification network as threats and vulnerabilities are discovered.

The goal of US CERT is to ensure that there is an average response time of no more than 30 minutes in the case of any attack. The very specific nature of this goal is designed to deliberately focus the US CERT on building broad participation by the private sector.

The US CERT will undertake the following major initiatives:

- Develop common incident and vulnerability reporting protocols to accelerate information sharing across the public and private response communities;

- Develop initiatives to enhance and promote the creation of response and warning technologies; and

- Forge partnerships to improve incident prevention methods and technologies.

The Department of Justice (DoJ), the U.S. Secret Service and the FBI have significantly decreased their response times and increased the priority of cyber crime investigation. FBI Director Mueller has placed cyber crime as a top five priorities of the FBI, and the Secret Service has added a number of electronic crime task forces to investigate and prosecute cyber criminals. All of DoD's criminal investigative organizations are leaders in investigating cyber crimes and include among their ranks some of the best investigators in the world. DoJ, through its Computer Crime and

Intellectual Property Section, has chaired the G-8 Subcommittee on cyber crime and has been a significant driving force in combating cyber crime worldwide.

Since there are no borders when it comes to cyber space, and criminal attacks on consumers can come from all corners of the world, the State Department has conducted bilateral and multilateral discussions to ensure that there is international cooperation in cyber security.

I have had the distinct pleasure of working with Commissioner Orson Swindle of the Federal Trade Commission, who has been a beacon of light for the protection of consumers' privacy and security. With his help in the creation of the FTC's "Dewey" program and his tireless support for town hall meetings, he has truly created a "culture of security" globally.

While there will be no silver bullets in enhancing cyber security, the private sector continues to grow its capabilities and make solid improvement in securing their part of cyberspace. Two of the earliest examples of private-public cooperation for "Cyber Crime/Cyber Security" were the High Tech Crime Investigators Association (HTCIA) and the Information Systems Security Association (ISSA). Both organizations date back to the 80's and are dedicated to sharing information on cyber crime and information security. They still exist today and their membership and value have increased significantly over the years.

Most recently, the private sector has created a coalition that I see as an excellent example of efforts to enhance consumer cyber security. As you are undoubtedly aware, identity theft is a major problem. While the vast majority of ID theft occurs in the physical world, we have seen an increase in the activities of criminals to commit the same types of crime online. The most recent method is what we call "phishing" or "spoofed" emails. The criminals will send out thousands of emails telling people that there is an error with their online account and ask them to fill in an "update form" or their account will be closed. This form has the look and feel of major e-commerce sites -- there was even a fake email from someone pretending to be the FBI and the FDIC asking unsuspecting users to enter personal information into a fake web site or their bank account would be closed.

To combat this many of the major players in the e-commerce space banded together to create the Anti-Online ID Theft Coalition. The Coalition boasts many private sector members, with the Information Technology Association of America providing support as the executive director. The Coalition has four major goals: 1) to build technology to reduce the likelihood of these mails ever reaching their intended victim; 2) to provide awareness training to consumers so they can more readily identify these criminal acts; 3) to share information on new scams amongst the various security teams; and, 4) to insure accountability by working with law enforcement to identify and prosecute these bad actors.

In a larger perspective with the federal government, Sector Coordinators representing each of the major sectors of our economy have been appointed to fight potential cyber attack. A Sector Coordinator is an individual in the private sector identified by the sector lead agency to coordinate their sector, acting as an honest broker to organize and bring the sector together to work cooperatively on sector cyber security protection issues. The Sector Coordinator can be an individual or an institution from a private entity. These private sector leaders provide the central conduit to the federal government for the information needed to develop an accurate understanding of what is going on throughout the nation's infrastructures on a strategic level with regards to critical infrastructure protection activities. The Sector Coordinators and the various sector members were key to the creation of the National Strategy to Defend Cyber Space.

In addition, there have been a number of new private sector Information Sharing and Analysis Centers (ISACs). An ISAC is an operational mechanism that enables its members to share information about vulnerabilities, threats, and incidents (cyber and physical). In some cases, an ISAC Manager may be designated, who is responsible for the day-to-day operations of the ISAC, to work with the Sector Coordinator or the sector coordinating body with support from DHS and the lead federal agencies.

Despite these security enhancements, we can be certain that the nature and sophistication of attacks will evolve. There are clear challenges we must continue to address.

First, we must renew our commitment to enhance consumer awareness of basic cyber security practices. The most recent attacks demonstrate that home users can be used as an effective pathway to launch attacks, or as a gateway into large enterprises. We need to build on the public/private initiatives to promote cyber security with a focused and aggressive outreach effort to all consumers.

Second, while we build an effective response network we must not lose sight of the innovation frontier. Technologies on the horizon hold the potential to dramatically and decisively transform our cyber security challenges. Self-healing computers, embedded technologies that enable devices to recognize and defend against attacks, and devices that enhance both security and privacy are within our reach with an aggressive technology development agenda. This effort must be industry-led in collaboration with our best Universities. Most importantly, it must be synergistically linked with our response initiatives.

Finally, we must recognize that cyber security is no longer merely about products, services and strategies to protect key operations. What is at stake in the effective implementation of advanced cyber security technologies and strategies is nothing less than the ability to unleash the next wave of information technology-led growth in jobs and productivity. Cyber security is an essential enabler to the advent of the next generation Internet and all it holds for how we work, live, and learn.

In the early part of December 2003 the private sector held the first national security summit in Silicon Valley. In attendance were private sector and public sector leaders including DHS Secretary Tom Ridge. This Summit was co-hosted by the ITAA, the U.S. Chamber of Commerce, TechNet and the Business Software Alliance, with the support of DHS.

The work of this summit has continued through the creation of task force work programs that will drive toward solutions to secure and defend cyber space. I am happy to report that much progress has been made and when the results of the various task forces are announced in early March we will again see the progress being made. The task forces bring together, distill, and integrate expertise regarding cyber security metrics, software development and maintenance, public outreach initiatives, and, of course, public-private partnerships in information sharing and early warning systems.

RECOMMENDATIONS:

While much good work has been done over the years, there is still work that needs to be done. My recommendations today fall into three major categories: 1) Cyber Crime investigations; 2) identity management; and, 3) vulnerability remediation.

Cyber Crime Investigations

For the past three years, we have seen a significant increase in the number of cyber crime investigations undertaken by all levels of law enforcement, federal, state, local and international. Although we have had success in a number of investigations, I would recommend to the Committee to look again at the federal agencies and their coordination and investigative responsibilities.

I am often asked by my private sector counterparts who to call to report cyber crimes. At one point, there were pretty clear guidelines of which federal agencies handled intrusions, frauds, financial crimes, denial of service, child exploitation, etc. Today, some federal agencies handle all or some parts of all of these investigations with varying levels of success. When agencies are asked who should be contacted, one of the answers has been "wherever you get the best service," this puts the private sector and the law enforcement agencies in somewhat of a competitive position which could result in investigative information not being shared broadly and not linking key information that could potentially solve some of these crimes. I would hate to see a hearing some day to identify why agencies did not "connect the dots" in a cyber attack because we do not have a centralized clearing house to analyze, correlate and disseminate information relative to cyber attacks. The creation of a centralized responsibility would go a long way to facilitate solving of these events.

Identity Management

In the area of identity management, static user ids and passwords are no longer sufficient to provide strong ("2-factor") authentication for identity. We have created a system where we must use complex passwords to login to various systems. We also have to change those passwords frequently creating another challenge for mere human beings to remember these complex passwords. This is made even worse by the need to use different passwords for different systems that few people voluntarily choose to do. This is a known weakness often exploited by criminal hackers. As we make identity management secure in the physical world it is not a stretch to presume organized crime and terrorists will then resort to online identity theft to evade detection and apprehension. The government can be a leader in accelerating the creation of digital identity management that would work just for government services and online e-commerce. The nation could be well served to have 2-factor authentication in place by the end of 2004. The form factor to be used can be smart cards, USB "dongles," credit cards and ID cards with Smart Chips built into them or one-time passwords found with some secure ID devices currently in use by some. The DoD has incorporated digital identity on the military ID card called the Combination Access Card (CAC)

Vulnerability Remediation

My last recommendation is in the area of vulnerability identification and remediation. As I mentioned earlier, annual security audits are not sufficient anymore, we need to implement a program where we have an ongoing vulnerability assessment that reports in real time the status of the "state of security" and provides this information in a format that is actionable and comprehensive. Many of us are looking to the development of a "security dashboard" that provides this information to executives so we can prioritize our resources and operationalize security into daily IT operations. Requiring government agencies to develop a program such as this will provide a baseline by which the private sector can develop similar efforts.

The remediation of these vulnerabilities also requires a comprehensive patch management program that so that enterprise-wide programs are not left vulnerable to many system-wide types of attacks.

Reduction and remediation of vulnerabilities will better provide a Critical Information Infrastructure that is more robust and resilient from whatever threats come our way.

Senator Kyl, Senator Feinstein, this concludes my prepared remarks. I thank you again for the opportunity to come before this Committee and welcome any questions that you and the Committee members may have.

Biography of Howard A. Schmidt

Howard A. Schmidt joined eBay Inc. as Vice President and Chief Information Security Officer in May of 2003. He retired from the federal government after 31 years of public service. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001. He assumed the role as the Chair in January 2003, until his retirement in May 2003.

Prior to the White House, Howard was chief security officer for Microsoft Corp., where his duties included CISO, CSO and forming and directing the Trustworthy Computing Security Strategies Group.

Before Microsoft, Mr. Schmidt was a supervisory special agent and director of the Air Force Office of Special Investigations (AFOSI), Computer Forensic Lab and Computer Crime and Information Warfare Division. While there, he established the first dedicated computer forensic lab in the government.

Before AFOSI, Mr. Schmidt was with the FBI at the National Drug Intelligence Center, where he headed the Computer Exploitation Team. He is recognized as one of the pioneers in the field of computer forensics and computer evidence collection. Before working at the FBI, Mr. Schmidt was a city police officer from 1983 to 1994 for the Chandler Police Department in Arizona..

Mr. Schmidt served with the U.S. Air Force in various roles from 1967 to 1983, both in active duty and in the civil service. He had served in the Arizona Air National Guard from 1989 until 1998 when he transferred to the U.S. Army Reserves as a Special Agent, Criminal Investigation Division. He has testified as an expert witness in federal and military courts in the areas of computer crime, computer forensics and Internet crime.

Mr. Schmidt had also served as the international president of the Information Systems Security Association (ISSA) and the Information Technology Information Sharing and Analysis Center (IT-ISAC). He is a former executive board member of the International Organization of Computer Evidence, and served as the co-chairman of the Federal Computer Investigations Committee. He is a member of the American Academy of Forensic Scientists. He serves as an advisory board member for the Technical Research Institute of the National White Collar Crime Center, and is a distinguished special lecturer at the University of New Haven, Conn., teaching a graduate certificate course in forensic computing.

He served as an augmented member to the President's Committee of Advisors on Science and Technology in the formation of an Institute for Information Infrastructure Protection. He has testified before congressional committees on computer security and cyber crime, and has been instrumental in the creation of public and private partnerships and information-sharing initiatives.

Mr. Schmidt has been appointed to the Information Security Privacy Advisory Board (ISPAB) to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.

Mr. Schmidt holds a bachelor's degree in business administration (BSBA) and a master's degree in organizational management (MAOM) from the University of Phoenix. He also holds an Honorary Doctorate in Humane Letters

Feb. 24, 2004

Statement for the Record of
Dan Verton
Author, Black Ice: The Invisible Threat of Cyber-Terrorism (McGraw-Hill/Osborne, 2003)

On
"Virtual Threat, Real Terror: Cyberterrorism in the 21st Century "

Before the
Subcommittee on Terrorism, Technology and Homeland Security
United States Senate Committee on The Judiciary
Washington, D.C.

Good afternoon Chairman Kyl, Ranking Member Feinstein and Members of the Subcommittee.

I want to thank you for the honor of appearing before you today to discuss what I believe is an urgent national security matter and I applaud your leadership in this area.

Although I do not consider myself a technical expert, I have a professional background in intelligence and information security, and I'm the author of a recently published book by McGraw-Hill titled *Black Ice: The Invisible Threat of Cyber-Terrorism* that goes into detail regarding the subject of today's hearing and has been endorsed by some of the nation's leading authorities in critical infrastructure protection, terrorism and information security, including the president's two former chief cyber security advisors, Richard Clarke and Howard Schmidt. My statement for the record, which I will summarize for you now, is based primarily on my research for Black Ice and some of my more recent work in this area.

I would like to address the following three questions:

1. **What is the nation's current level of vulnerability to cyber-terrorism?**
2. **What is al-Qaeda's capability to conduct cyber-terrorism?**
3. **What are the potential implications of a combined physical and cyber-terrorist attack against U.S. critical infrastructures?**

1. What is the nation's current level of vulnerability to cyber-terrorism?

Before any meaningful discussion can be conducted about the nation's vulnerability to cyber-terrorism, it is important to understand that there is no longer any separation between the physical, real world, and the cyber-world. Computers and computer networks control real things in the real world. And many of those "things" are critical infrastructures, such as electricity, drinking water and real-time financial transactions that have implications for both public safety and the national economy.

And this understanding must lead us to a new, more flexible definition of the term cyber-terrorism. We can no longer view cyber-terrorism with blinders on, choosing only to consider the acts of somebody sitting behind a computer and hacking or disrupting the operation of other computers or networks as cyber-terrorism. If we learned anything from 9/11 it was that traditional physical forms of terrorism can have massive cyber ramifications that can severely impair the functioning of the nation's economy – an economy that is almost wholly dependent on the uninterrupted operation of a fragile, privately owned and operated digital infrastructure.

Likewise, it is just as important for us to recognize that there is no longer such a thing as an insignificant vulnerability. When vulnerabilities exist, regardless of how minor we may think they are, they open the door to the unexpected and the unanticipated. This is particularly true in the realm of information technologies, where hidden interdependencies exist throughout the nation's critical infrastructures.

And it is an unprecedented level of interdependency that accounts for the nation's current level of vulnerability to cyber-terrorism, in both its physical and its electronic forms. Today every infrastructure or sector of the economy is potentially the Achilles heel of other infrastructures and economic sectors. For example, there is little question about the critical role of electric power in the operation of all sectors of the economy, the dependence of the electric industry on natural gas, the dependence of reliable telecommunications on electric power, the dependence of financial, government, and emergency services operations on both electric power and telecommunications, and the potential impact from prolonged failures of these infrastructures on drinking water and transportation systems. And the interdependence and potential for the type of cascading failure I am describing here stems from the confluence of the physical world and the cyber world.

Perhaps one of the most important areas where an unprecedented level of vulnerability has existed for years and still exists today is in the widespread adoption of wireless technologies. Although there are proven methods and security systems available for protecting wireless networks, they are not always understood and deployed properly, if at all. In my research I have found evidence of unprotected wireless networks in use at the following infrastructure settings: hospitals; airline baggage checking systems at some of the largest U.S. air carriers; railroad track heating switches; uranium mining operations; water and wastewater treatment facilities; security cameras; and oil wells and water flood operations.

Supervisory Control and Data Acquisition systems, or SCADA systems, are in many ways the crown jewels of some of the nation's most important industrial control settings, such as the electric power grid. But they are not – as their name might imply – built upon secret, proprietary technology. To the contrary, modern design specifications for SCADA systems, which I have documented through both personal interviews with experts and through open-source research on the Internet, presents us with the frightening reality that the SCADA systems being used in our nation's critical infrastructures are nothing more than high-end commercial PCs and Servers running Microsoft Corp. operating systems. In other words, the genie is out of the bottle and has been for years in terms of understanding how to disrupt or corrupt the operations of SCADA systems. Today, it's simply a matter of gaining access. And as I have also documented in my research, gaining access to SCADA systems for the purpose of causing widespread chaos, confusion and economic damage is increasingly becoming a mere formality for professional hackers, virus and worm writers, and terrorist-sponsored saboteurs.

The energy industry has acknowledged the existence of these linkages and the imperative of protecting SCADA systems from unauthorized access. In December 2001, for example, the American Gas Association and the Gas Technology Institute met in Washington, D.C., to discuss the need for improved encryption to protect SCADA communications between key nodes in the natural gas grid. One of the slides used during the two days of presentations highlights the threats posed to SCADA communications from the use of commercial computer equipment, open communication protocols that are widely published and available to anybody, linkages and reliance on the public switched telephone network, and the ability to steal the hardware.

In addition, a recent network architecture plan released by a major company in the water and wastewater industry included the following requirements for its SCADA systems: Peer-to-peer networking over TCP/IP (Transmission Control Protocol/ Internet Protocol—in other words, the Internet); software changes that can be downloaded from any node on the network; dial-in capabilities to all software functions; and a link to the existing pump station.

Consider the following additional examples, which I document in my book, Black Ice; The Invisible Threat of Cyber-Terrorism:

The U.S. railroad system's increasing use of wireless technologies may present one of the most immediate dangers to both national security and local safety. Given the system's long, winding network of radio, telephone, and computer assets, voice and data communications networks provide vital links between train crews, trackside monitoring and repair staff, and rail control centers. Total control of the massive network is accomplished through a communication system that integrates trackside maintenance telephones, trackside transponders, security cameras and monitors, passenger information displays, public announcements, the public telephone network, radio bases, and control center consoles. However, wireless SCADA systems are increasingly providing the management glue that keeps all of these systems running together. In the colder regions of the country, underground heaters keep the rails from freezing in winter. These operations are also being controlled and monitored by wireless SCADA computers. The use of

modern technology in this case means that in the case of a failure, railroads no longer have to dispatch technicians in the dead of winter to remote locations where heating switches are usually located. However, it also means that the security of these switching operations may now have a new series of security challenges to deal with. This is of particular concern given the dangerous nature of some train cargo.

The City of Brighton, Michigan, is one example. Brighton is a city of only 6,500. But that population skyrockets to more than 70,000 each day due to a thriving business district and a boom in hotel space. However, beneath the streets of Brighton is a **water and wastewater system** that is controlled in part by wireless technology. The remote terminals monitor pump run time, pump failures, flood sensors, high water level alarms, and power, as well as site intrusion alarms and manually activated panic buttons. The utility also planned to equip work vehicles with a controller connected to a laptop computer. "With critical data now available at just the click of a mouse, the laborious, time-consuming, and often hazardous, need for utility workers to make daily rounds to check pump status at each of the lift stations is a thing of the past," claimed marketing material from one of the contractors responsible for installing the equipment. The mobile controller would then allow utility engineers to monitor the waste water system while they're driving around the city.

Uranium mining operations in Wyoming extract uranium from the soil through a process by which water is injected into the ground. Because of the contamination, remote terminals are necessary to control and manage the pumps that move the water and extract the uranium. Commercial PC-based remote workstations now support critical monitoring functions, such as pump failure, pump status, temperature, speed, and even the pump's on/off condition. But the security implications are enormous. When pumps lose power, water pressure starts building up in the plant. Software has been programmed to automatically reset certain pumps to get the pressure out as fast as possible. And it's all being done in the name of cost-effectiveness.

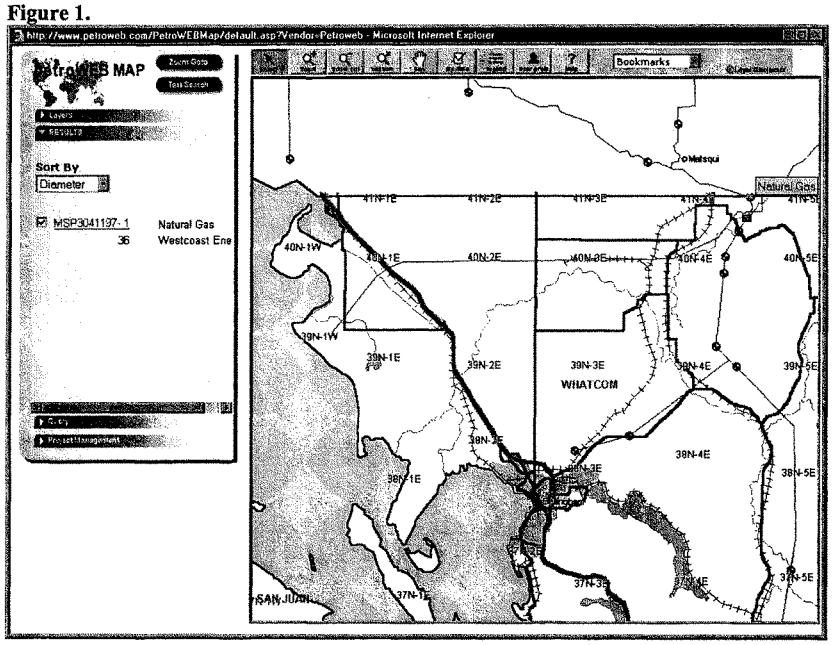
In states throughout the **Midwest, one can find oil wells** arranged in a twelve-mile-diameter circle. They are part of what's known in the vernacular of the oil industry as a **"water flood" operation**. However, with such a large number of pumps and holding tanks to manage, drilling companies are increasingly turning their attention to wireless SCADA systems to monitor critical functions of the operation, including emergency systems that are designed to ensure environmental safety. For example, wireless SCADA systems are used to monitor pressure and flow rates in both oil and water pipelines. When flow rates drop below normal levels, the system is designed to turn on additional pumps. In addition, if pipeline pressure or tank levels exceed normal operating limits the system will turn various pumps off. They are also used to monitor tank levels and overflow pit levels —a critical safety indicator that could have environmental consequences if it fails. And as in the case of the 911 emergency systems, oil well managers and technicians also have remote dial-in connection capabilities.

For the most part, these dire warnings have gone unheeded by the private- sector companies that own and operate these infrastructure systems. Senior executives view such scenarios as something akin to a Hollywood movie script. However, throughout the entire post-September 11-security review process, a process that continues to this day, administration experts and other senior members of the U.S. intelligence community were quietly coming to the conclusion that they were witnessing the birth of a new era of terrorism. Cyberspace, with its vast invisible linkages and critical role in keeping America's vital infrastructures and economy functioning, was fast becoming a primary target and a weapon of terror.

Mr. Chairman, my fear is that the next time we have a massive power failure, such as we experienced on Aug. 14, 2003 it will not be a self-inflicted wound, but potentially a terrorist-induced failure that is quickly exploited by suicide bombings, rampaging gunmen or chemical and biological attacks against those stranded in the subway systems.

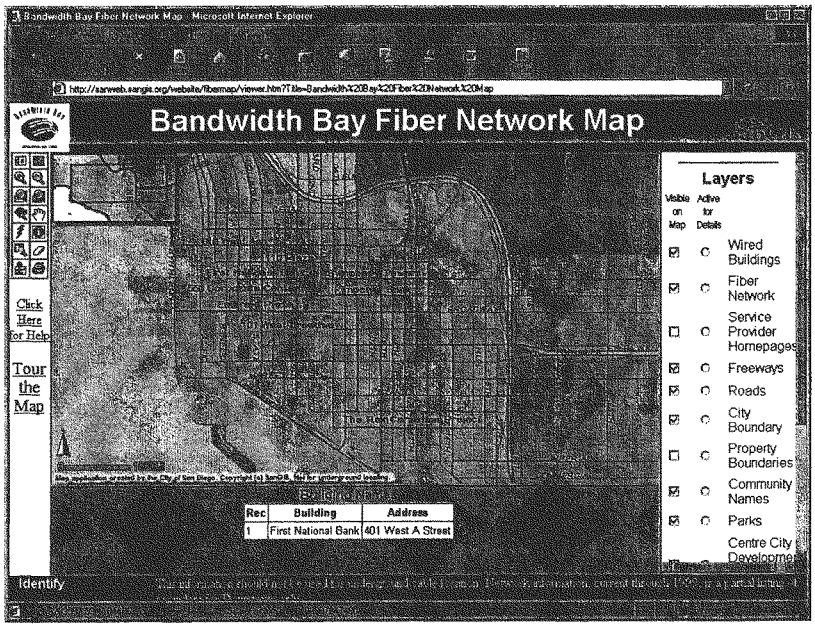
The Genie Is Out of the Bottle

Figure 1.



This is a photo taken from a publicly available Web site that depicts the most sensitive natural gas pipeline interconnection point in the U.S. What's interesting about this Web page is that it is completely interactive, not only allowing the user to zoom into great detail, but also providing latitude and longitude coordinates and detailed terrain/man-made landmarks.

Figure 2



Detailed, street-level maps of metropolitan area fiber networks are also available online, and include building and company names through which these high-speed interconnections pass.

Other Sensitive Data Available on Government & Corporate Web Sites

1. Detailed maps depicting the termination points along the entire Eastern Seaboard for all long-haul undersea fiber lines.
2. Maps depicting the storage locations of all spent nuclear fuel waste in the U.S.
3. Telecommunications network maps from which the location of current and planned critical facilities and nodes can be derived.
4. One telecom company offered location information for all of the company's five data centers, as well as a virtual tour inside a "typical" center, including a description of all security systems used to protect the facility.
5. Detailed descriptions by IT companies of deployment case studies involving SCADA systems.
6. Load-bearing capacities of elevators in large office buildings as well as location of ventilation and air conditioning systems.
7. Number of people employed at certain office buildings as well as maps and interactive photos of building and facility layout.

2. What is al-Qaeda's capability to conduct cyber-terrorism?

My goal in answering this question is to convince you and others in government to think differently about the future, and particularly, about the future of international terrorism. The high-tech future of terrorism is inevitable. And like the events leading up to the Sept. 11, 2001 terrorist attacks (events that dated back 8 years), we are beginning now to see the indications and warnings that international terrorism is evolving its tactics to meet the new operational realities it faces around the world and to better achieve its strategic goals.

Before we can tackle the question of al-Qaeda's capabilities in terms of conducting cyber-terrorism, it is imperative that we as a nation come to terms with the fact that terrorism is in a constant state of evolution. Terrorist tactics and modes of operation change and adapt over time, albeit very slowly and often imperceptibly. It is also imperative that we accept that terrorism has never only been about terror. There have always been and will always be socio-political and economic warfare aspects to international terrorism that speak directly to the potential employment of cyber-terrorist tactics.

Al-Qaeda's view of cyber-terrorism and its history in using information technologies is a case in point. But here, again, we face a significant perception problem. The picture that most Americans form in their minds when they think of al-Qaeda or of terrorists in general is a picture of a mindless horde of thugs living a hand-to-mouth existence in caves in Afghanistan. But this picture says nothing of the educated elite that forms the inner circle of the group's command and control, it says nothing of the technical support available on the open market in the form of out of work intelligence experts from a host of nations, and it says nothing of the threat posed by the continued radicalization of young people all over the world – young people who are studying computer science and mathematics and who may find it more advantageous to strike out directly at the U.S. economy than to strap explosives around their waste and walk into a crowded café.

That said, there is already ample evidence to suggest that the current generation of al-Qaeda terrorists understand the usefulness of attacking the U.S. cyber infrastructure.

For example, L'Houssaine Kherchtou, a 36-year-old Moroccan, was one of al-Qaeda's early trainees in high-tech methods of surveillance during the early to mid 1990s. He attended electronics training conducted in a guesthouse owned by Osama bin Laden on Fey Street in Peshawar, Pakistan. The electronics Lab was run by Abu al-Alkali and Salem the Iraqi. When he arrived, however, he informed his superiors that he did not have any background in electronics. A short time later, a more senior instructor arrived and informed Kherchtou that a degree in engineering was required to attend electronics training. This is not the picture of a mindless horde of thugs. This is the picture of a thinking enemy that values formal training and education.
In November 2002, I interviewed Sheikh Omar Bakri Muhammad, the leader of a London-based organization known as al-Muhajirun. Prior to the September 11, 2001 terrorist attacks, an FBI memo written by agent Kenneth Williams and e-mailed to the

FBI's Washington headquarters on July 10, 2001, noted a connection between Middle Eastern men enrolled in Phoenix-area flight schools and Bakri's organization in London. This should have been no surprise since Bakri, a Syrian-born Muslim cleric, refers to al-Muhajirun as "the mouth, eyes, and ears" of bin Laden and claims to speak on behalf of bin Laden's International Islamic Front for Jihad Against Jews and Crusaders. Furthermore, Bakri was one of several individuals in 1998 to receive a letter faxed from Afghanistan from bin Laden that outlined four objectives for a jihad against the U.S., including the hijacking of airliners. Also included in the fax was a statement urging Muslims to "force the closure of their companies and banks."

But my interview with Bakri in 2002 was the first example of a high profile, radical Islamic cleric speaking about the usefulness of cyber attacks in support of bins Laden's global Jihad. According to Bakri:

• "In a matter of time, you will see attacks on the stock market."
• "I would not be surprised if tomorrow I hear of a big economic collapse because of somebody attacking the main technical systems in big companies."
• "The third letter from Osama bin Laden...was clearly addressing using the technology in order to destroy the economy of the capitalist states. This is a matter that is very clear."

Osama bin Laden has also spoken in these terms. According to Hamid Mir, editor of the *Ausaf* newspaper, "Hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and ranging [sic] from computers to electronics against the infidels."

Bin Laden has also instructed his followers that "It is important to hit the economy of the United States, which is the base of its military power. If the economy is hit they will become preoccupied."

Since the start of the U.S. War on Terrorism, a significant amount of evidence has been unearthed throughout Afghanistan and various other al-Qaeda hideouts around the world that indicates terrorism may be evolving toward a more high-tech future at a faster rate than previously believed.

In January 2002, for example, U.S. forces in Kabul discovered a computer at an al-Qaeda office that contained models of a dam, made with structural architecture and engineering software. The software would have enabled al-Qaeda to study the best way to attack the dam and to simulate the dam's catastrophic failure. In addition, al-Qaeda operatives apprehended around the world acknowledged receiving training in how to attack key infrastructures. Among the data terrorists were studying was information on SCADA systems.

Despite all of the mounting evidence that suggests al-Qaeda is evolving toward the use of cyber-weapons, the terrorist group that started us down this path and that has posed the

greatest threat of all terrorist groups to U.S. national security remains somewhat of a mystery. But the War on Terrorism has helped uncover some of the hidden trends. Al-Qaeda cells now operate with the assistance of large databases containing details of potential targets in the U.S. They use the Internet to collect intelligence on those targets, especially critical economic nodes, and modern software enables them to study structural weaknesses in facilities as well as predict the cascading failure effect of attacking certain systems. But the future may hold something quite different.

The three driving factors behind al-Qaeda's operations—intent, resources, and opportunity—all point to the future use of cyber-tactics.

First, the intent of Osama bin Laden is clear. He wants to cripple the economy of the U.S. as a means to force the withdrawal of U.S. military personnel from Saudi Arabia and curtail economic and military support for Israel. The targeting of corporate America and the digital economy is clear in this regard.

Second, the growing number of technologically sophisticated sympathizers, especially among Muslim youth, is providing al-Qaeda with a steady stream of new talent in the use of offensive cyber-weapons. In addition to the younger generations of hackers and virus writers, al-Qaeda and other radical Islamist movements can count on the intelligence services of various rogue nations who now and in the future will find themselves in the crosshairs of the U.S. military.

Finally, America continues to present al-Qaeda and other radical Islamist groups with ample economic targets in cyberspace, thus driving these groups toward the increased use of cyber-tactics. Unless current trends are reversed and America's digital economy is no longer a target of opportunity, terrorist groups around the world will continue to dedicate time and resources to studying ways to integrate cyber-weapons into their operations.

3. What are the potential implications of a combined physical and cyber-terrorist attack against U.S. critical infrastructures?

The blackout of August 14, 2003 notwithstanding, the danger stemming from this unprecedented level of infrastructure interdependency was proven during the first major infrastructure interdependency exercise, which took place in November 2000 in preparation for the 2002 Winter Olympics in Utah. Known by its code name, Black Ice, the simulation was sponsored by the U.S. Department of Energy and the Utah Olympic Public Safety Command. The goal was to prepare federal, state, local, and private-sector officials for the unexpected consequences of a major terrorist attack or a series of attacks throughout the region, where tens of thousands of athletes and spectators from around the world would gather. When it was over, Black Ice demonstrated in frightening detail how the effects of a major terrorist attack or natural disaster could be made significantly worse by a simultaneous cyber-attack against the computers that manage the region's critical infrastructures.

Without going into the details of the exercise, the conclusions drawn by the exercise participants are startling. Estimates showed the loss of electric power throughout a five-state region and three provinces in Canada for at least one month. Other estimates went as far as several months.

The important lesson is that Black Ice showed the growing number of critical interdependencies that exist throughout the various infrastructure systems and how devastating combined cyber-attacks and physical attacks can be. It proved for the first time that the terrorist's mode of attack is irrelevant when it comes to cyber-terrorism. Terrorist groups that want to amplify the chaos and confusion of physical attacks or directly target the economy can succeed by launching traditional-style terrorist assaults against the nation's cyber-infrastructure.

According to the final report on the lessons learned from exercise Black Ice and a follow on exercise code-named Blue Cascades, government and private-sector participants "demonstrated at best a surface-level understanding of interdependencies and little knowledge of the critical assets of other infrastructures, vulnerabilities and operational dynamics of these regional interconnections, particularly during longer-term disruptions." Moreover, most companies and government officials failed to recognize their own "overwhelming dependency upon IT-related resources to continue business operations and execute recovery plans," according to the report.

As is evident from the following paragraph, the detailed findings of the Hart-Rudman task force confirmed the findings of the Black Ice and Blue Cascades exercises.

Sixty percent of the Northeast's refined oil products are piped from refineries in Texas and Louisiana. A coordinated attack on several key pumping stations—most of which are in remote areas, are not staffed, and possess no intrusion detection devices—could cause mass disruption to these flows. Nearly fifty percent of California's electrical supply comes from natural gas power plants and thirty percent of California's natural gas comes from Canada. Compressor stations to maintain pressure cost up to $40 million each and are located every sixty miles on a pipeline. If these compressor stations were targeted, the pipeline would be shut down for an extended period of time. A coordinated attack on a selected set of key points in the electrical power system could result in multi-state blackouts. While power might be restored in parts of the region within a matter of days or weeks, acute shortages could mandate rolling blackouts for as long as several years. Spare parts for critical components of the power grid are in short supply; in many cases they must be shipped from overseas sources.[1]

---

[1] "America Still Unprepared—America Still in Danger," Report of an Independent Task Force Sponsored by the Council on Foreign Relations, p. 26.

Statement by
Amit Yoran, Director
National Cyber Security Division
Department of Homeland Security

Before the U.S. Senate Committee on the Judiciary
Subcommittee on Terrorism, Technology, and Homeland Security
February 24, 2004

Thank you, Chairman Kyl, Senator Feinstein, and distinguished members of the Subcommittee. I appreciate the opportunity to appear before you today to discuss the important issue of cyber terrorism. I also welcome the chance to provide your Subcommittee with an update on the efforts of the Department of Homeland Security's National Cyber Security Division (NCSD) to defend our Nation against the menace of cyber threats.

The NCSD, established by the Department in June 2003, represents a crucial component of the Information Analysis and Infrastructure Protection (IAIP) Directorate. Under the leadership of Under Secretary Frank Libutti and Assistant Secretary Robert Liscouski, the IAIP Directorate leads national efforts to protect the Nation's critical infrastructures from attack or disruption. In support of this larger mission, NCSD serves as the focal point for:

- Enhancing the Nation's cyber readiness and response
- Analyzing cyber threats and vulnerabilities
- Disseminating threat warning information through alerts and warnings
- Coordinating incident response

Placement of NCSD in the IAIP Directorate ensure the integration of physical and cyber security approaches into a common, holistic risk management framework. Through the integration of physical and cyber protection capabilities, IAIP works to protect America from all threats – physical and cyber – and to understand the interdependencies that impact our critical infrastructures. Under the leadership of Assistant Secretary Liscouski, we are considering the full range of risks to the Nation, including loss of life, disruptions of infrastructure services, economic impact, and national security implications. Recognizing that future terrorist attacks may not be limited to a cyber or physical act, but rather a combination of the two to amplify impact, the Office of Infrastructure Protection is organized to examine threats and vulnerabilities across multiple dimensions:

- Integrating and mapping vulnerabilities to threats;
- Assessing sector-specific and cross-sector vulnerabilities; and
- Understanding national, regional, and local impacts.

Moreover, close linkage with the Office of Information Analysis led by Assistant Secretary Patrick Hughes, the primary threat information intelligence gathering and analysis capability of DHS, promotes the ability to map threat information with cyber vulnerabilities. This mapping allows for the effective prioritization of potential risks so agencies may implement remediation efforts as quickly as possible to limit the impact of computer incidents.

Since June, the NCSD has worked closely with our partners in the federal government, private sector, and academia to coordinate responses to major cyber security events, such as the Blaster worm, the

SoBig virus, and most recently the vulnerabilities identified in the Microsoft Windows operating system. Even though the NCSD has only been in operation for eight months, with each event, we are demonstrating our ability to quickly build capability and provide value to our stakeholders while building trust, credibility, and technical excellence that will serve as the basis for enhanced service delivery in the future.

For the remainder of my remarks, I will provide an overview of the cyber threat environment facing the Nation and the activities NCSD is undertaking with its partners to reduce our national vulnerability to these threats.

Nature of the Cyber Threat

As members of this Subcommittee have heard on numerous occasions, cyber threats continue to be a significant national and global concern. The most recent computer vulnerability identified in the Microsoft Windows operating system just two weeks ago, allowed attackers to potentially take control of a home user's computer. It is not uncommon for these types of vulnerabilities to surface in complex operating environments. The pervasive deployment of leading operating system within the United States means that vulnerabilities of this type can significantly impact the Internet and our critical infrastructures. Therefore, the US-CERT monitors these issues and generates alerts when appropriate.

When vulnerabilities are identified, viruses are launched, or when other types of cyber attacks are reported, it is often difficult to immediately identify and understand the underlying motivations for such attacks. Is it an isolated cyber attack, for example, a part of a terrorist plot, a criminal enterprise, or a teenager surfing the Net in search of a thrill? The difficulty is that the vulnerabilities and techniques that are exploited in the interest of cyber crime or even cyber hacktivisim are the same vulnerabilities and techniques that are at issue when discussing cyber terrorism.

Therefore, NCSD employs a threat-independent strategy of protecting the Internet and critical infrastructures from all types of attacks. While staying acutely aware of how terrorists might exploit the Internet, we face challenges in distinguishing between the malicious acts of a terrorist versus other types of attacks as an event is occurring in real-time. Rather than only focusing on specific attack profiles, we are developing programs and initiatives that apply to the gamut of attack approaches. In other words, our mission extends to protecting cyber systems across the entire threat spectrum, regardless of an actor's intent. If we attempt to "stovepipe" our protection efforts to focus on the different types of attackers who may use the cyber infrastructure, we risk the possibility of limiting our understanding of the entire threat environment.

While maintaining a threat-independent approach, the NCSD recognizes that DHS and the Federal government must remain vigilant in the identification of all types of cyber attackers. Components of the IAIP Directorate and our federal partners in law enforcement, defense, and intelligence devote considerable time and energy to identifying groups and individuals with the capability to launch a cyber attack and to determining the individuals responsible for an attack in the aftermath.

National Cyber Security Programs and Initiatives

As we have already discussed today, cyber attacks can appear with little or no warning, propagate quickly across cyberspace, and impact multiple infrastructures with devastating results. To lead efforts to analyze cyber threats and vulnerabilities, issue warnings, manage incidents, and coordinate response and recovery, we have established the United States Computer Emergency Readiness Team (US-CERT) to serve as the national focal point. NCSD, through US-CERT and other activities, supports three key mission areas: Analysis and Warning, Incident Management and Response, and Outreach. All of these areas support the core mission of IAIP: to make America safer through the reduction of vulnerabilities across all the critical infrastructures.

Analysis and Warning

Our top priority at NCSD is, where possible, to prevent a cyber attack from occurring and to limit its scope and impact on the critical infrastructures. A centerpiece of these efforts is the National Cyber Alert System, which is an operational system delivering to Americans timely and actionable information to secure their computer systems. Our government has a fundamental duty to warn the public of imminent threats and to provide protective measures, or at least the information necessary for the public to protect their systems. NCSD makes cyber security information products available to all computer users. These offerings alert users to security vulnerabilities, their potential impact, and actions required to mitigate the risks of exploitation. Since I was named Director of NCSD in September, we have already issued several alerts and a series of periodic "best practices" and "how-to" guidance products.

A key objective in developing the National Cyber Alert System was to provide cyber security information that is understandable to all computer users, technical and non-technical. The Internet touches all our lives, and the knowledge necessary for effective self-defense in cyberspace should be universally accessible. I am pleased to report that Americans appear to be exhibiting a keen interest in the system, which has already reached millions of citizens. On January 28, the day we inaugurated the system, the US-CERT site was bombarded by more than one million hits. Within days, more than 250,000 direct subscribers received National Cyber Alerts to maintain their cyber vigilance. For your reference and for your constituents, I would urge you to visit www.uscert.gov to subscribe to a number of our information products that facilitate the protection of your computer systems.

As referenced earlier, just two weeks ago US-CERT became aware of multiple vulnerabilities in the Microsoft Windows operating system. The most serious of these vulnerabilities allowed the potential for attackers to gain control of another user's computer through the Internet. US-CERT determined the unique nature of this particular vulnerability, when coupled with the considerable media attention surrounding its potential impact, warranted the release of a national alert. In response, US-CERT developed and released both a technical and non-technical alert distributed via the National Cyber Alert System. Importantly, the non-technical version provided easy-to-understand information to computer users about how to apply a patch in order to fix the vulnerability.

Providing timely and actionable alerts empowers home Internet users to secure their systems, and will significantly enhance our Nation's overall cyber security posture. Moreover, our alerts can enhance user response time across the public and private sectors, thereby reducing the economic impacts of virus and worm exploits. One year ago, many home users would not have heard about operating system vulnerability, like the one we learned about two weeks ago, until an attack that

exploited the vulnerability made news headlines. The National Cyber Alert System reduces the warning time to minutes and hours, and we are committed to making improvements to both the warnings and the response time in the future.

In addition, thousands of additional subscribers receive our cyber alert data in a redistributed form from sources like the National Cyber Security Alliance/StaySafe Online. That alliance, whose members have committed their time and resources to regularly educating the home consumer and small businesses on good security practices, and others like it serve as a conduit to enable even greater numbers of subscribers benefiting from NCSD products. Consistent with our mission, NCSD is also partnering with the National Association of State Chief Information Officers, the Multi-State ISAC, the American Society for Industrial Security, and other security-focused groups to touch as many government agencies, private corporations and small businesses, universities, and individual citizens as possible.

Consistent with law and policy, our division also works with the Office of Management and Budget and the National Institute for Science and Technology regarding the security of Federal systems and coordinates with federal law enforcement authorities, as appropriate. To this end, we have established the Chief Information Security Officers (CISO) Forum to provide a trusted venue for the government's leading information security experts to collaborate and share experiences, capabilities, and lessons learned. NCSD also established the Government Forum of Incident Response and Security Teams (GFIRST). This activity focuses on the sharing of information on computer incidents at both the operational and technical levels. Participants represent key personnel from across the 24x7 cyber security teams servicing U.S. Government departments and agencies.

NCSD is also working with other components of DHS to capture the knowledge from field assessments with State and local governments and the private sector. Through close collaboration and integration within DHS and throughout the Federal government, the NCSD is carefully examining the cyber dependencies of key facilities and assets to determine what, if any, impact might be caused by a cyber attack. On the opposite side of the coin, NCSD is studying the potential impact of physical attacks on cyber operations.

Incident Management and Response

A pillar of the *National Strategy to Secure Cyberspace* was the need to create a focal point to coordinate and facilitate federal government interaction with private industry on a 24x7 basis. In response, the Department has established the US-CERT. This represents a significant accomplishment for the Department—for the first time since computer security emerged as an issue with the release of the Morris Internet worm, our national response to cyber incidents is coordinated by a single federal entity. US-CERT, in collaboration with the private sector and leading response organizations, provides a coordination center that links public and private response capabilities to facilitate communication across all infrastructure sectors. Specifically, US-CERT works on a daily basis with the Internet and computer security community and leads national efforts to analyze and reduce cyber vulnerabilities, disseminate cyber warnings, and coordinate incident response activities.

In addition to the operational partnerships that comprise the US-CERT, we have also established the Cyber Interagency Incident Management Group, or Cyber IIMG, within the federal government. The Cyber IIMG coordinates intra-governmental preparedness and operators to respond to cyber incidents and attacks. This organization brings together law enforcement, defense, intelligence, and other

government agencies that maintain significant cyber security capabilities and, importantly, possess the necessary statutory authority to act. The Cyber IIMG is developing cyber preparedness and response plans to ensure that during a cyber crisis, the full range and weight of federal capabilities are deployed in a unified and effective fashion.

To ensure the key players in the federal community can communicate during a crisis, NCSD is continuing to widen the reach of the Critical Infrastructure Warning Information Network, or CWIN. For those not familiar, CWIN is a private communications network designed to serve as a reliable and survivable network capability with no logical dependency on the Internet or the public switched network. In the event a significant cyber attack disrupts our telecommunications networks and/or the Internet, CWIN provides a secure capability for Cyber IIMG members to communicate.

I know there is great interest, particularly in the media, about how the U.S. Government might prepare for and respond to a "Digital Pearl Harbor" and an electronic September 11th scenario. The National Strategy to Secure Cyberspace stated the required technical sophistication to carry out such an attack is very high, thereby lowering its probability of occurrence. Nonetheless, it is important for us to understand and prepare for any contingency. In this vein, DHS is extending the reach of CWIN's survivable architecture beyond federal agencies by working with private sector communications backbone providers to establish CWIN nodes at their Network Operations Centers. The goal is to expand the number of CWIN nodes to 100 by the end of 2004, a significant increase, making it a robust and resilient capability that supports national cyber operations and response during times of crisis.

NCSD is actively looking for ways to test the veracity of our national response capabilities. In October 2003, we conducted *Livewire,* the first ever national-level cyber exercise to baseline our response capabilities to cyber attack. This exercise involved over 300 participants representing over 50 organizations across the federal, state, and local governments and the private sector. The cyber attack scenarios were developed to stress cyber interdependencies across our critical infrastructures and test our ability to collaborate across the public and private sectors. NCSD is currently working with its partners in anticipation of a follow up cyber exercise in FY05.

Outreach

An expansive and effective outreach program supports every aspect of our Division's efforts to improve and sustain cyber security. The NCSD leads and advocates the implementation of user awareness efforts; education and training programs at the K-12 and collegiate levels; and initiatives to reach out to all of our stakeholders. We realize that every link in the security chain is vital, from the Department of Homeland Security and Fortune 100 companies to the local county offices and small businesses that drive our economy. Parents and children, teachers and doctors, Internet surfers and the occasional computer user—all must be informed about the dangers of cyberspace and the need for vigilance. A key to success is aggressively pursuing an outreach agenda that recognizes a need to communicate with each of these key communities in a clear, consistent, and understandable fashion. One of our top priorities at NCSD is to communicate to the public about cyber threats and vulnerabilities in a manner that informs, reassures, and offers practical advice and solutions.

One of our most important constituencies is the private sector. Approximately eighty-five percent of America's critical infrastructure is owned and operated by private companies, and technology developed by industry continues to fuel the growth and evolution of the Internet. In December 2003,

NCSD co-hosted the National Cyber Security Summit. This event allowed the Department of Homeland Security to work side-by-side with leaders from industry to address the key cyber security issues facing the Nation. Based on the dialogue from that event, five industry task forces were launched, focusing in the areas of—

- Increasing awareness
- Cyber security early warning
- Best practices for information security corporate governance
- Technical standards and common criteria
- Security across the software development lifecycle

Perhaps most importantly, the Summit served as a call to action. It represented a logical transition point from national strategy development to implementation of concrete actions that both the public and private sectors could adopt to improve the security of America's cyber systems. The task forces are diligently preparing recommendations for solutions across these five key areas. The industry task forces are diligently preparing options for potential solutions in these five key areas, and NCSD stands prepared to receive and consider swift implementation of appropriate recommendations.

In addition to the National Cyber Security Summit, NCSD is working with a host of industry groups to better understand and address their issues and concerns with respect to cyber security. These groups include, amongst others, the National Infrastructure Assurance Council, the President's National Security Telecommunications Advisory Committee, and the private sector Information Sharing and Analysis Centers. We are also working closely with the research and academic communities to better educate and train future cyber analysts. These partnerships include NCSD participation in the National Science Foundation's Scholarship for Service (or "Cybercorps") program and the National Security Agency's more than 30 Information Assurance Centers for Academic Excellence.

Conclusion

At DHS the question we ask ourselves every day is "How are we making America safer today," because, in the end, this is our key metric for success. In preparing to testify today, I reflected on how far we as a country have progressed on cyber security in the past decade. The accomplishments are truly remarkable. In that time, we have created a Cabinet-level agency to bring together government, industry, and academia to manage national cyber incidents. Congress passed the Government Information Security Reform Act and the Federal Information Security Management Act, both of which have driven enhanced accountability for security of government information systems. Government agencies, private corporations, and our research community have developed, fielded, and improved security technologies, such as firewalls and intrusion detection systems, to better protect our networks. Across government, industry, and academia, organizations have created the role of a Chief Information Security Officer, or CISO, and developed computer emergency response teams to manage computer-based events. More than 30 universities and colleges are teaching information assurance courses, training our Nation's next generation of cyber defenders.

These accomplishments, when viewed in total, represent considerable progress toward making better cyber security a reality. NCSD recognizes the importance of building on these successes every day and continuing to galvanize the cyber security community, public and private. Central to our success

will be furthering and reinforcing the National Cyber Security Division's reputation as a center of excellence founded on trust, credibility, and technical excellence.

Since June, I believe we have done much to further this goal. NCSD has established US-CERT, which integrated three different 24x7 federal cyber centers into one organizational entity and leveraged the vast capabilities of Carnegie Mellon's CERT/CC. We have developed a National Cyber Alert System that will reach out to all citizens and businesses, regardless of size, geography, and technical skill. We partnered with industry to create five task forces focused on key issues related to the future of cyber security. I think you will see that with each passing cyber incident, our Division will improve and refine our processes to better meet the needs of government agencies, businesses, and our citizenry.

At the same time, NCSD must continue to look forward and embark on a series of tactical and strategic cyber security initiatives designed to reduce critical infrastructure vulnerabilities. If I learned one lesson from my experiences working these issues in the private sector, it is that cyber security is an ever-moving target. Technologies, tactics, and players change quickly, and our challenge is to keep pace and to identify new areas of discovery. Software assurance, for example, represents an area of increasing importance. How do we encourage software developers to produce code with fewer embedded vulnerabilities? How do we evaluate a particular piece of code? In a world where software development is often outsourced, do we even know who wrote the source code? These types of strategic imperatives will shape the future of NCSD's programs and initiatives.

Again, I wish to thank the Chairman, the Ranking Member, and the members of the Subcommittee for this opportunity. I look forward to answering your questions.

○