S. HRG. 107-201

WIRED WORLD: CYBER SECURITY AND THE U.S. ECONOMY

HEARING

before the

JOINT ECONOMIC COMMITTEE
CONGRESS OF THE UNITED STATES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

June 21, 2001

Printed for the use of the Joint Economic Committee

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2001

cc 76-591

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, D.C. 20402

JOINT ECONOMIC COMMITTEE

[Created pursuant to Sec. 5(a) of Public Law 304, 79th Congress]

HOUSE OF REPRESENTATIVES

JIM SAXTON, New Jersey, *Chairman*
PAUL RYAN, Wisconsin
LAMAR SMITH, Texas
JENNIFER DUNN, Washington
PHIL ENGLISH, Pennsylvania
ADAM H. PUTNAM, Florida
PETE STARK, California
CAROLYN B. MALONEY, New York
MELVIN L. WATT, North Carolina

SENATE

JACK REED, Rhode Island, *Vice Chairman*
EDWARD M. KENNEDY, Massachusetts
PAUL S. SARBANES, Maryland
JEFF BINGAMAN, New Mexico
JON S. CORZINE, New Jersey
ROBERT G. TORRICELLI, New Jersey
ROBERT F. BENNETT, Utah
SAM BROWNBACK, Kansas
JEFF SESSIONS, Alabama
MIKE CRAPO, Idaho
LINCOLN CHAFEE, Rhode Island

CHRISTOPHER FRENZE, *Executive Director*
ROBERT KELEHER, *Chief Macroeconomist*
PATRICIA RUGGLES, *Minority Staff Director*

CONTENTS

OPENING STATEMENT OF MEMBERS

Representative Jim Saxton, Chairman 1
Senator Robert F. Bennett 1
Senator Jack Reed, Vice Chairman 4

WITNESSES

Panel I

Opening Statement of Dr. Lawrence K. Gershwin, National Intelligence Officer for Science and Technology, National Intelligence Council, Central Intelligence Agency; accompanied by Brian Shaw 5

Panel II

Opening Statement of Steven Branigan, Vice President of Engineering and Co-Founder, Lumeta Corporation 22
Opening Statement of Peggy Lipps, Senior Director of Security and Risk Management Initiatives, BITS 27
Opening Statement of Duane P. Andrews, Corporate Executive Vice President for Science Applications International Corporation (SAIC) 30
Opening Statement of Albert J. Edmonds, President, EDS Federal Government Information Solutions 34

SUBMISSIONS FOR THE RECORD

Prepared Statement of Senator Robert F. Bennett 45
Prepared Statement of Senator Jack Reed, Vice Chairman 47
Prepared Statement of Senator Jon S. Corzine 48
Prepared Statement of Representative Lamar S. Smith 49
Prepared Statement of Dr. Lawrence K. Gershwin 50
Paper entitled "Mapping and Visualizing the Internet" by Steve Branigan, Bill Cheswick and Hal Burch 62
Prepared Statement of Catherine A. Allen, Chief Executive Officer, BITS 74
Prepared Statement of Duane P. Andrews 83
Prepared Statement of Albert J. Edmonds 87
Prepared Statement of Frank J. Cilluffo 95

WIRED WORLD: CYBER SECURITY AND THE U.S. ECONOMY

Thursday, June 21, 2001

CONGRESS OF THE UNITED STATES,
JOINT ECONOMIC COMMITTEE,
WASHINGTON, D.C.

The Committee met, pursuant to notice, at 10:00 a.m., in Room 562, Dirksen Senate Office Building, the Honorable Jim Saxton, Chairman of the Committee, presiding.

Present: Representatives Saxton, Smith, Dunn and Putnam; Senators Reed, Bennett, and Corzine.

Staff present: Christopher Frenze, Colleen J. Healy, Brian Higginbotham, Paul Nicholas, Corine Bradshaw, Dianne Preece, Betsy Holahan, Patricia Ruggles, and Matthew Salomon.

OPENING STATEMENT OF REPRESENTATIVE JIM SAXTON, CHAIRMAN

Representative Saxton. Good morning. The Joint Economic Committee (JEC) deals with many issues, and we think they're all important.

Obviously, the issue of cyber security in the U.S. economy is something that is gaining in importance with each new generation of technology, and with each increase in capability that we make in technology.

This issue is of great importance and of special interest to Senator Bennett and so I'm very pleased to be here to open this hearing this morning, and to turn to Senator Bennett at this point for any opening statement he may have.

OPENING STATEMENT OF SENATOR ROBERT F. BENNETT

Senator Bennett. Thank you very much, Mr. Chairman. I appreciate your support of this hearing and the activity regarding it, and I'm also grateful to the Vice Chairman, Senator Reed, for his willingness to participate in the hearing and his support.

This is something that a lot of people might initially think is far afield from the Joint Economic Committee, and say, "well it has to do primarily with the military and why are you looking at it?"

The reason we are looking at it is because cyber threats to the U.S. economy don't stop at the door of the Pentagon, and many people are making it clear that future threats to the United States will be aimed at the private sector and at crippling the U.S. economy, rather than crippling the U.S. military.

So an attempt for us to find out whether the current policies governing cyber security and cyber protection are sufficient is very much within the purview of the Joint Economic Committee.

Technology in general and the Internet specifically have been of great benefit to the economy. They have driven our economic growth in the last 10 years. At the same time, they open up a whole new series of threats that we have not traditionally had.

Traditional notions of national security focus on keeping our borders secure, and every military operation begins by looking at the map.

As you see today – and we have demonstrations in the back – and it's on the cover of the books that have been made available to members of the Committee, the map of the Internet knows no borders. The map that is displayed here and that will be displayed later in the hearing is worldwide, and the first thing that hits you as you look at that map is that there are no oceans, there are no mountains, there are no natural barriers.

You don't see the Internet in the same way that you would look at a Rand McNally map. Secondly, the recognition that 85 percent of the critical infrastructure in this country is owned by the private sector. When the commander at the Pentagon picks up the phone to give an order to a commander in the field, he's connected with Verizon.

And it goes over the private sector-owned facilities in telecommunications, energy, banking, transportation systems, all of the things that are necessary for us to keep the economy going are now vulnerable in ways that they never have been before, and in this interconnected world, it is the private sector and the private economy that is on the front line.

Now the threat comes from a variety of sources and I have ranked them in their seriousness.

The first one, and the one that we are most often confronted with is the world of the hacker, and many of the hackers are frankly nothing more than a nuisance. They want to break into a site in order to prove that they can. They usually leave behind some pornographic symbol or screen saver, just to prove that they've been there. That's called "defacing the site."

They want to be able to say that, well, you call up the White House or you call up a Congressional site, or you call up a corporate site, and there is a piece of pornography proving that we were there and we have defaced the site. And once they've done that, they are satisfied.

Now, those who do this not only create a nuisance but sometimes create economic devastation far beyond anything they had anticipated.

The "Love Bug Virus" is estimated to have cost several billion dollars worldwide, and the individual who did it had no intention of producing that kind of economic problem.

Above the hacker, in seriousness, you now have what has come to be known as the "hactivist." This is someone who has a cause and he'll break into your site for that cause. He will leave behind propaganda, or he will try to change your information that would lead people to his position.

Whether his cause has to do with environmental activism or political activism or anarchy or whatever it might be, the hactivist is a little more

serious threat in terms of the economic devastation he can leave behind than the ordinary hacker.

Then we get to the level of criminal activity. There's the freelance criminal who simply wants to steal money, or sometimes steal your identity to use that to make money. Sometimes he wants the corporate identity as well as the personal identity so that he can order things or get money transferred, but his purpose is criminal and financial.

Then there's organized crime that gets a little more sophisticated than the freelance criminal. Organized crime not only wants to steal money, they want to steal information, information that can then be turned into money. And organized crime wants to monitor what's going on with respect to law enforcement.

We saw examples of that in Seattle during the World Trade Organization (WTO) meeting where people determined to upset that meeting wanted to know what law enforcement was doing, and they broke into the law enforcement networks in an effort to find that out. And that of course has tremendous implications for the economy.

If law enforcement can't deal with that and if organized crime is involved in significant efforts to change money and information and corporate identities around the world, they can have tremendous economic impact.

Then you get above that to serious espionage. Again, this is divided into corporate espionage. People who want to find out information in advance so that they can manipulate your stock price, so that they can beat you to a market by stealing your trade secrets, to national espionage where other countries want to know what is going on in the U.S. economy in such a way as to manipulate it or defeat it or otherwise hold hostage America's policymakers in terms of the amount of damage that they could do to the economy.

And then finally there is the ultimate threat and we've made the newspapers now with respect to that possibility. This is Tuesday's *USA Today*. The main story, "Cyberspace is the Next Battlefield, U.S. Foreign Forces Prepare for Conflict Unlike Any Before," and this is the Nation State that would say, we are going to attack the Americans not in the traditional military way, but we're going to attack them by attacking their economy through the Internet, and hold American presidents and policymakers hostage by what we can threaten to do.

If we can break into the Federal Reserve's Fedwire and shut down all commercial activity, all financial activities in the United States, we can break into the telecommunications system and say that nothing can happen unless you meet our geo-political demands, that is a vulnerability to the economy and to the country that it is very much worth looking at.

So, Mr. Chairman, again, I thank you for calling this hearing. I think we've assembled a panel of witnesses that are going to be very informative and probably have a greater understanding of this than we could have had in any other forum. And I'm very grateful to you for your support.

Thank you.

[The prepared statement of Senator Bennett appears in the Submissions for the Record on page 45.]

Representative Saxton. Thank you very much, Senator Bennett. Senator Reed.

OPENING STATEMENT OF SENATOR JACK REED, VICE CHAIRMAN

Senator Reed. Thank you, Mr. Chairman.

First, let me thank you for convening this hearing, Mr. Chairman, and also thank and commend Senator Bennett, not only for his sponsorship but for his active advocacy for such a hearing. It follows on his great and visionary work with respect to Y2K undertaken together with Senator Dodd. Senator Bennett has established himself in the Congress as not only a thoughtful but a very active observer on the issue of cyber security.

Today we are joined by a distinguished group of witnesses who will try to elucidate a very complex and a very difficult field. As a Member of the Armed Services Committee as well as the JEC, I know there is an extraordinary confluence of national security and economic issues that are engendered by the issue of cyber security.

Indeed, I will excuse myself shortly to go back to the hearing with Secretary Rumsfeld.

But as Senator Bennett so eloquently pointed out, we are all today critically linked by computers and as we move further to a web-based economy, not only does that offer great opportunities but great vulnerabilities. The extent to which we understand these vulnerabilities and the extent to which we are prepared to respond to these vulnerabilities will make our economy more vigorous, and we'll be stronger as a nation.

I note that after our aircraft was forced down over China, if you read the press, there was a series of attacks on our computer systems traced back to China. So today, the response to a diplomatic impasse and, in some respects, a military impasse, is not just the traditional one but can be a very novel one of cyber attacks or at least cyber disruptions.

And so this hearing is extremely timely, very important, and I think it will be a useful forum and baseline to begin further considerations. Again I commend you, Mr. Chairman, and Senator Bennett.

I would, for the record, like to submit my formal statement.

[The prepared statement of Senator Reed appears in the Statements for the Record on page 47.]

Representative Saxton. Thank you, Senator Bennett.

I would just say at this point that we have to be out of this room at 12:30, so I would like to move forward, if other Members would agree to place their statements in the Record.

In that case, thank you very much, and I will introduce our first panel.

We will hear from Dr. Lawrence K. Gershwin, National Intelligence Officer for Science and Technology. Dr. Gershwin works for the Director of Central Intelligence as his principal advisor on global science and

technical developments. Dr. Gershwin will place cyber threats in the context of globalization for the next, and will provide an overview of the current and projected threats to federal and private sector community networks.

I also understand that Dr. Gershwin has agreed to stay, following his testimony, to answer any questions that may come up during the rest of the hearing.

Dr. Gershwin, the floor is yours, sir.

OPENING STATEMENT OF DR. LAWRENCE K. GERSHWIN, NATIONAL INTELLIGENCE OFFICER FOR SCIENCE AND TECHNOLOGY, NATIONAL INTELLIGENCE COUNCIL, CENTRAL INTELLIGENCE AGENCY;

ACCOMPANIED BY BRIAN R. SHAW, DEPUTY NATIONAL INTELLIGENCE COUNCIL, CIA

Dr. Gershwin. Thank you, Mr. Chairman, and Members of the Committee for the opportunity to discuss cyber threat and critical infrastructure issues.

I have a longer statement for the record that I'll submit, and I'll just summarize my remarks here.

Late last year, the National Intelligence Council published a report called "Global Trends 2015" which presented our best judgments of the major drivers and trends that will shape the world of 2015.

We anticipate that the world will almost certainly experience quantum leaps in information technology and in other areas of science and technology.

Information technology will be the major building block for international commerce and for empowering non-state actors.

Most experts agree that the information technology revolution represents the most significant global transformation since the industrial revolution beginning in the mid-18th century.

The networked global economy will be driven by rapidly and largely unrestricted flows of information, ideas, cultural values, capital, goods and services, and people. That is true globalization.

This globalized economy will be a net contributor to increased political stability in the world in 2015, although its reach and benefits will not be universal. In contrast to the industrial revolution, the process of globalization will be much more compressed. Its evolution will be rocky, marked by chronic financial volatility and a widening economic divide.

As the Director of Central Intelligence testified to the Congress earlier this year, no country in the world rivals the United States in its reliance, dependence and dominance of information systems. The great advantage we derive from this also presents us with unique vulnerabilities.

Computer-based information operations could provide our adversaries with an asymmetric response to U.S. military superiority by giving them

the potential to degrade or circumvent our advantage in conventional military power.

Attacks on our military, economic, or telecommunications infrastructure can be launched from anywhere in the world, and they can be used to transport the problems of a distant conflict directly to America's heartland.

Hostile cyber activity today is ballooning. The number of FBI computer network intrusion cases has doubled during each of the past two years. Information derived from the Internet indicates that since last September, the number of hacker defacements on the world wide web have increased over tenfold.

Meanwhile, several highly publicized intrusions and computer virus incidents have fed a perception that the networks upon which U.S. national security and economic well being depend are vulnerable to attack by almost anyone with a computer, a modem, and a modicum of skill. This impression of course overstates the case.

Information from industry security experts suggests that U.S. national information networks have become more vulnerable, and therefore they are more attractive as targets of foreign cyber attack.

Mainstream commercial software, whose vulnerabilities are widely known, is replacing relatively secure proprietary network systems by U.S. telecommunications providers and other operators of critical infrastructure. Such commercial software includes imported products that provide opportunities for foreign implantation of exploitation or attack tools.

U.S. government and defense networks similarly are increasing their reliance on commercial software.

Opportunities for foreign placement or recruitment of insiders have become legion. As part of an unprecedented churning of the global information technology work force, U.S. firms are drawing on pools of computer expertise that reside in a number of potential threat countries.

Both the technology and access to the Internet are inexpensive relative to traditional weapons and require no large industrial infrastructure.

Hackers since the mid-1990s have shared increasingly sophisticated and easy-to-use software on the Internet, providing tools that any computer-literate adversary could obtain and use for computer network reconnaissance, probing, penetration, exploitation or attack.

Even with technology and tools, however, considerable tradecraft also is required to penetrate network security perimeters and defeat intrusion detection systems.

Tradecraft also will determine how well an adversary can achieve a targeted and reliable outcome and how likely the perpetrator is to remain anonymous.

Let me talk about some of the groups that will challenge us on the cyber front. Senator Bennett has already enumerated many of these, but let me expand on that.

First on hackers. The most numerous and publicized cyber intrusions and other incidents are ascribed to computer hacking hobbyists. Such hackers pose a negligible threat of widespread, long duration damage to the national level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets, such as critical U.S. networks, and even fewer would have a motive to do so.

Nevertheless, the large, worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage including potentially extensive property damage or loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such attacks.

Let me now talk about hactivists. A smaller foreign population of politically active hackers, which includes individuals and groups with anti-U.S. motives, poses some threat, but most international hacktivist groups thus far appear bent on propaganda rather than literally on damage to critical infrastructures.

Pro-Bejing Chinese hackers over the past two years have conducted mass cyber protests in response to events such as the 1999 NATO bombing of China's embassy in Belgrade.

Pro-Serbian hacktivists attacked a NATO website during Operation Allied Force.

Similar hacktivism accompanied the rise in Israeli/Palestinian clashes beginning last year, and several thousand webpage defacements and some successful denial of service attacks were associated with the recent EP-3 incident.

International corporate spies and organized crime organizations pose a threat to the United States through their ability to conduct industrial espionage, and large-scale monetary theft, respectively, and through their ability to hire or develop hacker talent.

Computer network espionage or sabotage can affect U.S. economic competitiveness and can result in technology transfer to U.S. adversaries.

Because cyber criminals' central objectives are to steal, and to do so with as little attention from law enforcement as possible, they are not apt to undertake operations leading to high profile network disruptions such as damage to U.S. critical infrastructures.

However, rampant criminal access to critical financial databases and networks could undermine the public trust essential to the commercial health of U.S. banking institutions and to the operation of the financial infrastructure, itself.

Let me now speak about terrorists. Traditional terrorist adversaries of the United States, despite their strong intentions to damage U.S. interests, are less developed in their computer network capabilities, and in their propensity to pursue cyber means than are other types of adversaries that we've talked about. They are likely, therefore, to pose only a limited cyber threat.

In the near term, terrorists are likely to stay focused on traditional attack methods. Bombs still work better than bytes. But we anticipate more substantial cyber threats in the future as a more technically competent generation enters the terrorist ranks.

Finally, let me talk about national governments. National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm U.S. interests. These threats range from propaganda and low-level nuisance webpage defacements to more serious espionage and very serious disruption with loss of life, to extensive infrastructure disruption, the entire spectrum.

Among the array of cyber threats, as we see them today, only government-sponsored programs are developing the capabilities with the future prospect of causing widespread, long duration damage to U.S. critical infrastructures.

The tradecraft needed to employ technology and tools effectively remains an important limiting factor, particularly against more difficult targets, such as classified networks or the critical infrastructures.

For the next five-to-10 years or so, only nation states appear to have the discipline, commitment, and resources to fully develop capabilities to attack critical infrastructures.

Let me talk some about future tools and technology. Incremental deployment of new or improved security tools will help protect against both remote, and to some extent, insider threats. However, the defense will be at some disadvantage until more fundamental changes are made to computer and network architectures, changes for which improved security has equal billing with increased functionality.

For attackers, viruses and worms are likely to become more controllable, precise, and predictable, making them more suitable for weaponization.

Advanced modeling and simulation technologies are likely to assist in identifying critical nodes for an attack, and conducting battle damage assessments afterwards.

Overall, I would say that the future is quite uncertain for us in terms of how technology will apply to this business of enhancing the ability of attackers to attack us, but we should expect some major changes, some of which will be unforeseen.

The implications are that despite the fundamental and global impact of the information revolution, the reliance of critical U.S. activities on computer networks and the attention being devoted to information operations, uncertainty remains whether computer network operations will truly evolve into a decisive military weapon for U.S. adversaries.

Nonetheless, a recent CIA report, entitled, *"Preserving National Security in an Increasingly Borderless World,"* suggests that the information age and advanced technology will embolden our adversaries to target what they perceive as our vulnerabilities rather than to engage U.S. forces directly.

Weapons of "mass effect," such as denial of services attacks, are likely to proliferate in the coming decade. As the technology revolution accelerates, civilian technology will increasingly drive military technology and the civilian sector will increasingly become the point of attack for enemies of the United States.

Whether or not foreign computer operations mature into a major combat arm, however, they will offer an increasing number of adversaries new options for exerting leverage over the United States including selection of either non-lethal or lethal damage and the prospect of anonymity.

Adversaries will be able to use cyber attacks to attempt to deny the United States its traditional continental sanctuary with attacks on critical infrastructures. They could exploit U.S. legal and conceptual controversies relating to defending privately operated networks with U.S. government resources and the separation of the U.S. domestic and foreign security establishments.

Adversaries also could use cyber attacks to attempt to slow or disrupt the mobilization, deployment, combat operations, or resupply of U.S. military forces. Attacks on logistics and other defense networks would be likely to exploit heightened network vulnerabilities during U.S. deployment operations, complicating U.S. power projection in an era of decreasing permanent U.S. military presence abroad.

Whatever direction the cyber threat takes, the United States will be confronting an increasingly interconnected world in the years ahead.

As the CIA report points out, a major drawback of the global diffusion of information technology is our heightened vulnerability. Our wired society puts all of us – U.S. business in particular, because they must maintain an open exchange with customers – at a higher risk from enemies.

In general, information technologies' spread and the growth of worldwide digital networks mean that we are challenged to think much more broadly about national security. We should think in terms of global security to include the dawning reality that freedom and prosperity in other parts of the world are inextricably bound to U.S. domestic interests.

Thank you, Mr. Chairman, that concludes my oral testimony, and I'd be happy to entertain some questions.

[The prepared statement of Dr. Gershwin appears in the Submissions for the Record on page 50.]

Representative Saxton. Thank you very much. Just let me start with something that peaked my interest. As you walked us through the line of problem makers, and you started with hackers and referred to them as perhaps the least worrisome or bothersome – and I think you actually referred to them as hobbyists – and the hacktivists as propagandists, and gave the examples, and then the international industrial organizations, it seemed like you were moving from the lower threat to the higher threat categories of folks here.

And then when you got to terrorists, you surprised me—

Dr. Gershwin. Right.

Representative Saxton. – by saying that they don't currently present that much of an issue. And that surprised me.

Can you explain why that is? Given the fact that they are very active around the world, and have elaborate training schools, are well-funded, sometimes by governments and certainly acquiring the capability to be dangerous actors in terms of this subject. Why do you say they are not?

Dr. Gershwin. First of all, I want to bring up, to help me out with the questions and answers, Dr. Brian Shaw, my deputy, but I'll try to field this first question.

Yes, we've noted for a while that, in some sense, our judgments about terrorists seem counterintuitive and controversial.

The issue is that – and frankly our work is based on a great deal of classified work that we've done that I really can't talk about so much here – in looking at the terrorist threat, we've been struck by how little attention we have seen thus far and how little skill we have seen thus far in the terrorists in terms of information technology.

They are beginning to use it for communication among themselves and things of that sort but thus far, and we look at terrorist organizations very, very closely, we simply have just not seen this particular cyber attack capability develop.

We do believe that it's partly a generational thing – and so we do expect, frankly, five to 10 years from now that the terrorist cyber threat will be much more significant than it is today as the teenagers come into the leadership ranks.

But terrorists really like to make sure that what they do works. Thus far, based on their own skill levels, we would say that they are probably not very confident that the kinds of attack tools that they could use – in cyber threat, would give them the kinds of results that they like.

They do very nicely with explosions, so we think largely they're working on that. They're also working on weapons of mass destruction as well. But again, there, we haven't yet seen much from them in terms of actual accomplishment.

The fact is that we think that at this point now, the terrorists are really focusing primarily on more traditional means of attack. But, again, let me just say that this is a difficult area and we can see the possibility of a terrorist organization six months from now focused very heavily on cyber threat issues that we just never even saw before, we didn't even know they existed, and that could completely change the picture.

So we're giving you kind of a snapshot of where we are today but it could change rapidly.

Representative Saxton. Thank you. Senator Bennett?

Senator Bennett. Thank you, Mr. Chairman. And Dr. Gershwin, thank you very much for sharing this with us.

Talk to us about the threat of the "virtual insider." That's a term that a lot of people don't understand, but you and I have had this conversation, and I'd like to get that out now more publicly as a result of this hearing.

Dr. Gershwin. Well, if you can elaborate a little bit on the virtual insider.

Senator Bennett. The person who can get into the network system unrecognized, get down to root level, and then he owns the system as if he were your own Information Technology (IT) person, and can go virtually anywhere in your system undetected. He's an insider. How easy is it for that to happen? How often do you think it does happen, and so on?

Dr. Gershwin. The issue is the lack of adequate security in many of our networks, which means that a reasonably dedicated intruder using technology and tools, many of which are widely available, can over a period of time figure out how to get inside a network, establish himself as equivalent to a full-fledged member of that network, essentially with the kind of access, we call it root access, that gives him the same type of access that a system administrator would have. And essentially embed themselves in the network in ways that are undetectable to a large extent from anyone involved.

What that means is that then they are "owning the network," they are capable of essentially reading all of the communications traffic, extracting information from databases and so on, anything that goes on within that operation.

There are all kinds of networks that we have, many of which are open, but many of which are rather private. But nevertheless, a skilled intruder is capable of getting into a lot of private networks, establishing themselves as a member, and then extracting information for either espionage, to take the information back to enhance whatever organization they're working for, to perhaps understand this network in order to set it up for future attack, computer network reconnaissance, but to do this in such a way that they are practically undetected unless we use very elegant tools to try to figure it out. And that's hit or miss.

So this is a serious problem, it's a growing problem, we are very attentive to it, and I'm sure there's been some public discussion of these issues which have achieved a certain amount of notoriety. Brian, did you have anything?

Mr. Shaw. I would just add that there are two dimensions to the insider. One is vulnerability in the software itself, and whether or not systems are being upgraded and protected with the known vulnerability patches that are available. That is an uneven process.

That's one of the angles. The other angle is in fact that common software is constantly being exploited for known vulnerabilities and these are being communicated across the Internet so the attack upon those known vulnerabilities is constant.

So between those two, there are many gaps and many seams in which these insiders and these attackers can fit their way in.

Senator Bennett. Quickly, before my time is up, I noted in your written testimony, you referred to an independent group of security professionals that created the Honeynet Project, placing virtual computers on the Internet to evaluate threats that currently exist and the average computer they found placed on the Internet will be hacked in about eight hours.

But university networks are even worse with unsecured computer systems being hacked in 45 minutes. Could you comment why the universities are easier to get into than some others, or is it just a matter of more interest in the university?

Dr. Gershwin. Let me let Brian answer that one since Brian found this information out for me.

Mr. Shaw. University networks are, by their very nature, very fluid with the turnover in student body happening every semester, with the maintenance of large numbers of accounts, and thus it becomes a very easy system in which to obtain passwords, obtain legitimate accounts, and thus using automated worms and automated tools, to be able to establish a presence on a university network.

University networks, also by their very nature of collaboration and academic pursuit, are very extensively connected away from themselves, so these connections become wonderful nodes for exploitation as a target, as well as an opportunity for much of the hacker world.

Senator Bennett. Thank you, Mr. Chairman.

Representative Saxton. Thank you, Senator Bennett.

Senator Corzine?

Senator Corzine. Thank you, Mr. Chairman, and I appreciate very much your holding this hearing and Senator Bennett for your leadership in promoting this.

Coming recently from the private sector, a lot of the issues that you talked about in the protection, particularly in the financial industry, the topic is very apt and one that a great investment in time was put.

But I take it that from your testimony, Dr. Gershwin, that you feel like either by act of omission that the private sector is not doing enough to countervail the kinds of threats that you describe in your testimony. Am I reading that right, or is it more that we don't have the tools that may be available in the classified sector, to protect us? What do we need to do? What's the prescription that would accelerate that kind of protection that will deal with the economics?

The second question I had, Senator Bennett sits on the Banking Committee with me, and we were discussing the *Export Administration Act*, and how much are we our own problem with respect to the interconnectedness which is a reality, but is also the technology that's developed in the United States. How much are we feeding it into the world, and are there things and steps that we should be taking, in your view, that may have some sense of restriction of trade but go beyond where we are today to protect ourselves?

Dr. Gershwin. With regard to the second question, I'm not sure I can be of much help. For a variety of reasons, you know, I'd rather not deal with that question here today.

The first question, however, is, I think a good one.

Mr. Shaw. Well industry is taking very strong steps within their spheres. The challenge that we're facing is the collaboration between industry and government on how to protect ourselves across a shared network.

I would not characterize U.S. industry as being deficient in this area. I think the issue is how we collaborate between government and industry and how we cooperate.

Dr. Gershwin. Yes. I don't want you to give the impression that we're saying that industry isn't doing enough. I've been struck by the willingness of the industrial folks to talk with us about a lot of these issues.

Frankly, I think part of the problem is that we in the government have just not worked out enough mechanisms to work closely with industry on means to protect both the government and the U.S. infrastructure itself.

This is an on-going problem. I think a lot of strides are being made, but I think that we could do a lot more.

Senator Corzine. Are there specific steps that you think are missing in that process other than the general sense of collaboration that should be imposed?

Dr. Gershwin. I think if we were in a better position to share experience, both we in the government with what we know, including some of our classified information, and for industry to share with the government what it in fact is experiencing in the way of attacks and probes and so on, we've had some of that, but I think a more broad sharing of that information would probably enable us to put together a better composite picture of what the true threat is, what the nature of the ongoing threat is, particularly in terms of trying to attribute who is behind it and why are they doing it.

I mean, it's one thing to register a lot of activity and to count up statistics on how many probes and what are going on. We have enough tools and techniques today to be able to do some work in figuring out who is doing this and why. That's really critical because some things are just being done casually and you can defend against that.

But more systematic determined opponents, which is I think the real threat that we have, we need to understand that better and I think industry has information that would be helpful to us.

Senator Corzine. Is there a centralized focus for this in the government that should be reaching out or could be reaching out that needs either more authority or funding or resources?

Dr. Gershwin. I couldn't speak so well to the authority and the resources. I know that the National Security Council staff has taken some steps recently to strengthen their role in this process. There is significant interagency debate taking place on how to do that.

And within the Pentagon itself, I think there's been a lot of work in that area. But I think it's going to play out probably over the next few months in terms of more serious judgments about how the country should go on that.

[The prepared statement of Senator Corzine appears in the Submissions for the Record on page 48.]

Representative Saxton. Thank you very much.

Congresswoman Dunn?

Representative Dunn. Thank you very much, Mr. Chairman. I am absolutely fascinated by your testimony, Dr. Gershwin.

I have a lot of questions, some of which have already been asked, but I feel like, as you talk about teenagers who really know what they're doing moving into the next generation, being the heads of companies and so forth, or people who could attempt to invade companies or governments, it really makes me nervous.

I think Senator Corzine's question about partnerships is very important.

Do you believe now that departments of the government are working well together and are developing partnerships that will be helpful to us in our defense, at least at the government level, and who are those partners in the government that you're working with?

Dr. Gershwin. Well, I can't speak for the whole government effort because frankly we're from the intelligence community, but we ourselves work very closely with the Defense Department, the Justice Department, and the FBI, with the White House. In terms of those partnerships, I think we've had a great deal – and Department of Energy is an example – we've had a great deal of information sharing on the types of incidents we're concerned with, the types of threats.

Increasingly, we're getting help from the Department of Energy's National Laboratories looking at these issues, and they have a lot of very good technology and techniques that we can use to effect.

The FBI has been extraordinarily helpful in sharing information with us and trying to develop a better understanding of foreign threats.

In terms of collaboration with industry, I think the Defense Department has done an extraordinary effort through a number of mechanisms to work with telecommunications executives. The White House has had an on-going committee of telecommunications executives that, for a number of years, has been advising the White House and the government on these issues. That has gotten stronger.

The Defense Science Board has taken a number of looks at these issues, and that involves a great many of the industry people, both in national security and telecommunications and in information technology.

So I think the collaboration has been good. As with many issues, there is just a lot more that I think we can do.

Representative Dunn. And I certainly think into the future, as we become more dependent on the Internet and cyberspace, for example, there are going to be more and more problems associated with this.

I'm wondering if partnerships shouldn't be more effective, for example, in the areas of trade where we are working on H1B visas to allow our high tech companies in the United States, Microsoft from my neck of the woods, to be able to bring employees from other nations.

I start thinking in terms of cyber moles and things like that. Are we protecting enough in the activities that the private sector is doing in cooperation with the government to make sure that we're not opening ourselves up to this sort of threat?

Mr. Gershwin. Well, as I alluded to in my testimony, there's certainly some potential for problems there. One of the issues I think is that while we may be working with American companies on issues, at some point there are subcontracts and subcontracts from there, and at some point, you usually lose track of just who is doing the work for you.

And at some point, if foreign adversaries are interested in penetrating into U.S. systems, that's one of the ways to do it is to just get hooked up into a series of contracts where they have some ability to affect the final products to their advantage.

It's an issue that we are attentive to. I don't have any good answers to that, but it's certainly something that's on the screen.

Representative Dunn. Do you think the private sector is as alert and aware as they need to be to this potential threat?

Dr. Gershwin. Frankly, I would have to say no. I think not because I think that while that par of the private sector that's really in the national security business is quite aware, the civil sector I think tends not to regard this as a threat because it hasn't been manifested in any ways that have caused a great deal of damage to anything yet.

There's a certain tendency I think, as I alluded to in my testimony, to look to functionality rather than security as the primary objective. You really want things to work and achieve your business objectives and unless you have a serious threat to your security that's been manifest, you're probably going to be less attentive to security issues until it really hits you in the face.

But that's a general observation and certainly not true for everyone. But I think that one of our concerns is to make sure that this issue comes more to the attention of the civil sector of society, which is increasingly vulnerable to foreign threat and is really overall tied up into U.S. national security in ways it has not been historically in the past.

Representative Dunn. Are there activities going on now that would create the educational opportunity in the work that you're doing? Are you seeing summits being held or meetings being held? Things like this hearing that I think are very good to wake people up.

Should we be doing more in our positions representing constituents than we're doing now, and what would be your thoughts on how we could do that educating process?

Dr. Gershwin. There certainly have been more forums. There's just a plethora of meetings, forums, international as well as national, on the issues, and frankly I've seen it internationally now, which is pleasing, because I think some of our allies are becoming more attentive to these issues as well.

I'm not sure I have any concrete suggestions for what to do but frankly hearings like this help a great deal because largely this issue has been buried as a national security issue and almost retained in the classified arena, and that doesn't get it out around the public nearly as well as open sessions like this do.

Representative Dunn. This seems to me to be a very good topic for summits like the World Economic Summit that takes place in Davos every January, where world leaders are attending along with members of the business community.

Thank you very much, Dr. Gershwin.

Representative Saxton. Thank you, Ms. Dunn.

Mr. Putnam?

Representative Putnam. Thank you, Mr. Chairman, and I thank Dr. Gershwin for his testimony which is, as has been said, outstanding.

Recently the Hart-Rudman Commission prepared a report for National Security in the 21st Century, and one of the many recommendations in that report was the establishment of a directorate of critical infrastructure protection, which would combine the information sharing and analysis centers, the Commerce Department's Critical Infrastructure Assurance Office, the FBI, what are your thoughts on that recommendation, and does that send us in the right direction?

Dr. Gershwin. It's a little hard for me to really comment on that again coming from the intelligence side of the house.

I can see certainly some benefits in centralizing more the functions that we are talking about, but on the other hand, we work very effectively with, even in the existing setup, with the large number of organizations that are dealing with it.

It is really somewhat outside my purview to judge whether that's a good recommendation. I think it's an interesting idea which ought to be explored. I know within the government at least there's been a lot of discussion about it, and a lot of differences of view as to how's the best way to go.

I would just as soon reserve judgment on that one.

Representative Putnam. To the extent that you can comment, has there been a hierarchy identified of targets, both governmental and commercial, and does our level of preparedness match that risk level?

Dr. Gershwin. I'm not sure that it's really been done as systematically as you put it. I'd like to be able to say, yes, clearly we have done all that. I'm not convinced that we really have.

Brian, do you know?

Mr. Shaw. Well, if I understand your question, the hierarchy of targets really depend on the attacker's agenda and what the intent was. So it would be extremely difficult to have a list of targets unless you had some idea of whose interest it was to make those types of exploits.

Representative Putnam. Well, certainly you've mentioned that terrorists, up until fairly recently, have had very little interest and still have only slightly more than that interest in cyber warfare due to their own abilities. But there was also the sense that there wasn't enough bang for the buck in the shutting down of a power grid or whatever the case may be, that they didn't get the attention that they felt their particular cause merited.

But as international awareness of cyber terrorism grows, and the effects of it continue to grow as well as the costs and the damages, I think that it certainly will move up higher on their wish list, and it will replace the truck bomb as an effective method of getting their message out.

Dr. Gershwin. I don't think I'd agree that it would replace the truck bomb; it might complement the truck bomb. They may want to go after certain targets with a combination of explosive, as well as cyber attack.

As the terrorists move into this area, what I would expect to see first is using both techniques together.

Again, it's hard to get immediate results from a cyber attack, to know how well you did, to know how well the target may have defended itself. To get the kind of feedback on whether you've succeeded in your objectives.

And terrorists tend to want quick gratification and publicity. But I think it's correct that you will see cyber attacks in the future, at least coming out of terrorists as part of their agenda. I think it will still be a while, but I could be wrong.

Representative Putnam. I think your testimony was interesting in that just like Americans, even terrorists have to have their children and grandchildren program the VCR. I think that's essentially what you were saying.

How do we enhance the cooperation between the government and the private sector when you look at the commercial assets that are so vulnerable when you start talking about power grids and stock exchanges and commodity trading and airline hubs and things of that sort?

How do we improve that without, as you pointed out in your testimony, violating that governmental commercial line?

Dr. Gershwin. One thing I would recommend doing is during the Y2K experience, we had a remarkable collaboration of government and industry. We both learned a lot.

I'm not sure how well all of that has been followed up. I mean, there were a lot of mechanisms established during Y2K that were very effective. And, you know, some of those mechanisms still exist; some probably don't.

But for me at least in being engaged in that issue, that was a remarkable experience in working with the private sector which I'd never experienced before.

And it was a very successful endeavor. The problem was that there was a date associated with it, and for cyber threat, there's no date associated with it. It's going to be ongoing and increasing.

I don't really have good, concrete recommendations but I do think that a sense of the nation as having an infrastructure that truly is a critical national asset, and that that is part of our true national security problem, is not yet apparent to enough people.

And I don't know that the industry itself necessarily thinks of itself quite that way. I think that's going to be important to have that happen. That requires obviously leadership at all ends.

Representative Putnam. That was one of the key findings of the Rudman Commission, which was that Americans are far more vulnerable to attack on American soil in a greater variety of ways then they realize, that exacerbates whatever eventual attack does come.

And I would like to think that that collaboration could occur now, rather than waiting until we've had our first major attack and then we respond to a crisis.

Dr. Gershwin. Yes. I think we have enough information now that we ought to be able to move out on that as opposed to waiting. That's correct.

Representative Putnam. We've talked a lot about the fact that terrorists have not yet evolved into this. But are we aware of state-sponsored cyber attack programs around the world, to the extent that you can comment on that?

Dr. Gershwin. I can't go into it a great deal but, yes, we are aware. There have been some public acknowledgments about foreign countries. Some countries are writing about the importance of the issue, the next wave of military operations and things of that sort. We've certainly seen that from countries such as China, Russia.

We work very intensely in the intelligence community in trying to understand the nature of these foreign programs. Most of our information is at a classified level. But, yes, there are certainly a number of countries that today have active programs. We watch them fairly intensely. Some of them are aimed at the United States specifically, others are probably aimed at others. And the number of countries on that list will grow.

Representative Putnam. Thank you, Dr. Gershwin. Thank you, Mr. Chairman.

Senator Bennett (presiding). Congressman Smith?

Representative Smith. Senator Bennett. I understand opening statements have been made a part of the record, and if so, I would like to include mine.

Senator Bennett. That's correct, and it will be without objection.

[The prepared statement of Representative Smith appears in the Submissions for the Record on page 49.]

Representative Smith. Thank you.

Dr. Gershwin, on the House side, the Crime Subcommittee just completed a series of three hearings on cyber crime, but we did not hear from the CIA. So your testimony was both interesting and informative from our point of view.

You mention in your testimony, in regard to hackers, that most were frankly not successful although the threat of malicious and successful hackers was increasing.

In regard to terrorism, you said the greater threat today was from bombs, not bytes, but the threat there was increasing as well, so I gather from your testimony that you feel the threat of cyber crime, while maybe the danger is not immediately as great as it might be, it's going to continue to increase.

If that's the case, I wanted to ask you what type of cyber crime you felt was the greatest threat both to government and to business if there is a difference between the type of cyber crimes that are the greatest threat.

Dr. Gershwin. That's a tough question. I'm not sure I'm really well-qualified to answer since cyber crime is not the part of the cyber threat activity that I spend most of my time on.

I think it is correct to say that cyber crime is on the increase. It's too lucrative an area for people to stay away from. You know, people go for the money and cyber crime is the new way to rob banks. It's much more effective than armed robbery.

Again, I think our private infrastructure is obviously the target because that's where the obvious money is. But the specifics on how countries would go about it or how – it's not so much countries, I suppose, it's really individuals or groups – how they would go about it is not an area that I am pretty familiar with.

I don't know, Brian, if you can say much about it. But we do have specialists that pay attention to that. Unfortunately they are not with us today.

Mr. Shaw. If you expand the list of cyber crime all the way from propaganda to infrastructure take down, all of these are illegal things to do. At the current time, propaganda and espionage seem to be the most doable things and the most currently occurring activities.

It's much more difficult to take out infrastructures on a limited basis. It's extremely difficult to take down large scale infrastructure networks.

So if there was a current vulnerability, it would be to the theft, espionage, and propaganda level.

Dr. Gershwin. Actually, yes, and I should have said that criminal behavior ought to include illegal presence in a computer network when you're not authorized to be there and acting, as Senator Bennett pointed out, as a virtual insider, I'm not sure what the legalities are but it doesn't

sound very legal to me for somebody to be able to manipulate a computer network that they have no business being in.

To me, that's the kind of cyber crime that we spend most of our time dealing with.

Representative Smith. Dr. Gershwin, my next question, you may not be entirely objective but I think you will be, and that is do you think that our law enforcement activities, whether it's monitoring or surveillance or whatever it might be, are keeping up with the threat of cyber crime? Or do we need to do more?

Dr. Gershwin. The law enforcement side of it unfortunately is not the area that I am in, that's really more of a domestic law enforcement concern, which is not, since we are in the intelligence business –

Representative Smith. Well, I was thinking particularly of the CIA and your activities there.

Dr. Gershwin. I see. Let me rephrase the question some, in terms of is the intelligence community keeping up with the foreign threat, in terms of being able to pay attention to it.

Yes and no. Yes in the sense that it is a high priority issue for the intelligence community. All of the major agencies are ramping up their efforts significantly. I know for a fact, from looking at just the size and magnitude of the efforts, the type of people being brought in to work on it, that there's a huge increase in effort going on throughout the intelligence community to pay attention to this.

Is that keeping up with the threat? In some ways it is because of the effort. On the other end, I think the attackers have some significant advantages in terms of developing new tools and techniques.

Often in our case, what we will be able to do is figure out what's going on only after something has happened. For us, the obvious thing is to be able to detect cyber activities before they are manifested. That's very hard to do and that I don't feel as comfortable about.

Once events have taken place, and once programs have become evident, we have lots of ways to figure out a lot more about it but I don't feel very good about our ability to kind of anticipate.

Representative Smith. This question may also be going beyond your testimony today, but perhaps not beyond your expertise. And that is that do you have any suggestions for Congress for any changes in legislation that we need to make, or any additional legislation?

The reason I say that is you probably know much of our legislation dealing with cyber crime dates to the mid-1980s and clearly is out of date.

But do you have any specific recommendations for additional legislation or any other suggestions for actions that Congress can take to help counter cyber crime?

Dr. Gershwin. I don't have any specific suggestions. I have one concern that Congress can help on because I think it's just a real problem, and that is the difficulty in understanding the source of cyber threat as to whether it's foreign or domestic.

Our system, both the intelligence and law enforcement, has a lot of rules and regulations having to do with who has jurisdiction. And that was good for the old ways of people doing business. In the cyber world, it is extremely difficult to tell early on and even ultimately whether cyber threats are foreign, domestic, or a combination, because the evidence for that is just difficult to attribute.

So I think we continue to have struggles and difficulties in terms of who is really responsible for what, and legislation perhaps can help in that area. That's not my expertise.

What I do know is that this is a cause of consternation for us, as it has been in the past for terrorist issues.

Representative Smith. That really answers my question. It goes to jurisdiction and we can try to improve upon that. Thank you, Dr. Gershwin and thank you, Mr. Chairman.

Senator Bennett. Thank you. And Dr. Gershwin, we appreciate your testimony and we appreciate your willingness to sit with us through the next panel so that you'll be available for questions with respect to their testimony.

Thank you very much, both of you.

Our second panel now will come forward and our first witness will be Steven Branigan, Vice President of Engineering and Co-Founder of the Lumeta Corporation.

Mr. Branigan is a leader in Internet mapping, will graphically show us what the Internet looks like, and illustrate some security-related issues.

He's accompanied by Mr. Cheswick, who is the technical genius behind these maps. The two of them have been in my office, and it was very, very informative.

Also, on the panel is Peggy Lipps, Senior Director for Security and Risk Management Initiatives at BITS which stands for the Banking Information Technology Services. It's part of the Financial Services Roundtable.

Ms. Lipps will outline how the financial services industry is approaching cyber security and infrastructure protection.

Then Mr. Duane Andrews, Corporate Executive Vice President and Director of Science Applications International Corporation, former assistant secretary of defense. He brings a wide range of expertise to this area, and he will discuss the need to reconsider the federal government's approach to the infrastructure protection and some of the issues that Congressman Smith was raising.

Our final witness will be Albert Edmonds, President of the Federal Government Information Solutions. He will address the type of partnerships that would best serve the nation's interests in ensuring the protection and productivity of cyber networks.

We will then question the entire panel, along with Dr. Gershwin.

Thank you very much, all of you, for coming. Mr. Branigan, we'll start with you.

PANEL II

OPENING STATEMENT OF STEVEN BRANIGAN, VICE PRESIDENT OF ENGINEERING AND CO-FOUNDER, LUMETA CORPORATION

Mr. Branigan. Good morning, Senator. Thank you. On behalf of both William Cheswick and myself, we would both like to thank you and your staff for all the assistance in helping us prepare to be here today, and we're very grateful to have the opportunity to be in front of you to speak on the issues of cyber security.

William Cheswick and I, along with Hal Burch, have authored a paper on Internet mapping that we would like to submit for the record.

Senator Bennett. Without objection.

[The paper entitled "Mapping and Visualizing the Internet" by Steven Branigan, et al, appears in the Submissions for the Record on page 62.]

Mr. Branigan. Thank you.

What we would like to do today is to deliver orally a summary of this paper, along with a visual summarization as well, through the magic of Power Point.

This started – and a lot of the pioneering work on Internet mapping had started – due to a conference called the "Highlands Conference" sponsored by the Department of Defense that William Cheswick, which was run by Dick O'Neil, still is run by Dick O'Neil actually.

And at this conference, they were looking at issues that would be affecting the infrastructure and seeing what can we do today to help prevent and to help defend against attacks in the future.

One of the big issues that came out of there were the denial service attacks, and this was back in the middle 1990s that this was identified as one of the big risks to the infrastructure. Both the denial of service attack and, subsequently, the distributed denial of service attacks, both of these attacks are very difficult to defend against because at the heart of the attack, there is a lying of the source of the address. So you really have difficulty in tracing it back to where this attack comes from.

Other motivations for the mapping that we're about to go through today were to observe the growth of the Bell Labs in the AT&T Internet. Both Bill Cheswick and myself were members of Bell Labs research before we moved to Lumeta, and we wee able to watch both the Internet from there and the corporate intranet as well.

Discussions with both CIOs and CFOs, as we've been sort of out on the trail trying to talk about Internet security and the things we can do to improve on Internet and corporate security, yielded a lot of interesting information for us, and also curiosity about the size and the growth of the Internet.

Before we press on to ours, we want to just cover a couple of other maps that do exist. This is just a map of the backbone of the Internet

done by John Quarterman that had seen some of our work. He's also done some work showing network connectivity between the U.S. and South America.

Something that seemed interesting to us at the time, this map was from 1996, was a lot of the connectivity between sections in South American seemed to go through the U.S. In fact, the U.S. seemed to have such a strong amount of Internet backbone.

There was a period of time where many countries, in order to connect to other countries on their continent, would have to go through the U.S. to get there.This of course is our first version of the Internet map which we probably called smashed peacock against the windshield, if I remember this correctly.

One of the other ones I'd like to point out that we would like to demonstrate for you right now, if we could, is the Australian map. One of the things we did, this was our first look at an Internet map and it seemed too confused and too tight, so we tried to clean it up a little bit and yielded something such as this.

Yes. Yes, please, sir.

Mr. Cheswick. This is a map, a recent map showing Australia and China on the Internet. Australia is the black area on there and China is the red. You can get some idea of the relative presence on the Internet.

It turns out that Australia's been on the Arpanet for a very long time and they're very well-connected.

Mr. Branigan. Now on this map, if I may, if you can imagine, this is just about the global Internet as we've seen it. And to get an idea, if you can look at a single point here, behind that would be approximately 250 computers up to 65,000 on average. So it should give you some idea of the size and scope of the Internet.

One of the two goals we have today is to show you the size of the Internet and the other one is to show you the complexity of the corporate Intranet and the challenges they have to go through.

So that was one of the things that was very surprising to us is to actually try to visualize something that is almost as large as the universe in some ways. It's quite large.

One of the things I want to show you, and this is an older slide, we haven't had time to make the update historically, but I will show you the top ones from June 1st, as well. We looked at top ISPs by our measure, which our measure was the number of routers that we found on the Internet that belonged to certain ISPs.

And we tried to make the font smaller but found impossible. Cable and Wireless and Alternet were the top two. Now, as of a couple days ago, that's changed. Alternet seems to be, by our count, the largest Internet service provider.

Now these are important things to know because they are actually providing the backbone of the Internet itself. They provide the connectivity between many corporations. They are the infrastructure. These are the companies that are the infrastructure of the Internet today.

The two that are in green here, Apnic and Ripe, these are actually Asia Pacific and the European networks, and we didn't subdivide those further, for the purposes of this one.

One of the other statistics we wanted to show you briefly is we'd love to get a feeling for which countries seem to have the largest parts of the Internet. We find that that's not as easy to do as you may think.

Looking here, you'll see the top ones are dot net and dot com. Dot net and dot com aren't always attributed to a single country. Many times they are attributed to the U.S. but they can be in use by other places.

If you'll look further down, you'll see Australia is very large. If you were to look at this as the metric, the U.S. does not take up much of the Internet, which is not a true statement. The U.S. takes a very large section of the Internet.

So that's where we can start seeing we have some issues, trying to figure out if we look at a source of an attack, how do we track it back to the proper country for jurisdiction more or less, figuring out who's the actual culprit for a security incident.

One of the other things I want to display for you is this graphic to show you how, as you reach out node by node, router by router, on the Internet. How the complexity grows, and how there can be, if there's one bad person, this is where they can be hiding, somewhere out on a network of this size.

So you can see why it can be very difficult, once someone launches an attack, how it can be very difficult to find them.

One of the other things we wish to cover today – on our next slide, what we wish to cover today is to look at a corporate Intranet, as we turned our attention toward looking at corporate Intranets to see how they are organized, how they are architected and how well they can be identified and managed in their growth.

This is one typical corporate Intranet or enterprise network that we looked at. Everything that's in blue on this slide is something that they knew about that we discovered during a mapping of their corporate Internet.

Everything that's in red is something that they weren't aware was inside their firewalls or on their Intranet, or as we were hearing today, a place where a virtual insider can reside and then move throughout a corporate network from those points.

In this case, this is approximately 15 percent of a network. And these are not single hosts. Again, these, every one of these end points that's on here can represent up to 255 computer systems that are possibly vulnerable and unmanaged.

And so we found that this was a very striking way to see some of the challenges that corporations are facing today as the are managing corporate Intranets that they need in order to be competitive, in order to get products to market on time, to communicate efficiently, to be global, corporate Intranets are very necessary.

However, they are also, because of their growth, because they need to be up all the time, failure is not an option, they are very difficult to manage and they are very difficult to secure. And so we have been working on developing tools to help corporations secure those.

And this again is another corporate network where over on the side there, you can see this is another obvious leak where it's allowing the corporate network to leak out to the Internet, is not going through a firewall. There were two leaks. This is one here and the one that I will, this cluster up here is all because this one point is serving traffic that it should not be, and now it's opened up a second network.

So it can give you a feeling for how one misconfiguration can change the security of an entire network.

A couple of samples of one client network that we wished to go through to show you, as we looked at the visualization, we found it very important to look at the visualization to help us see things that we would not otherwise see.

This is just showing a map that we start at a point, a point down here, this is where we started, and as we get further away from the central point, the nodes will get darker. It was just giving us a feeling where the backbone of their corporate network is and it's right here.

And when we look at it through what they knew about versus what they did not know about, what's in orange is what they did not know about or did not tell us that they knew about.

And you can see here, there are some links that were attached to their corporate network that they were unaware of.

Finally, what we wish to touch on too is, this is an Intranet for a company that was undergoing divestiture. The stresses that corporations and their networks feel come from acquiring new companies and integrating their networks or having made a decision to divest a certain part of a company and then taking that network and separating it from the rest.

If you were to see here the green, this is one section of a company that needs to be removed from another because they are about to spin out, and the same for the pink section here. You can see there's significant work if you look at these blue lines. They are part of the parent company, yet, the pink is part of the new company that needs to be split.

So in divestiture, there's a lot of work that needs to be done in order to do it securely and correctly.

This is possibly the smallest company that we've done to date. So it makes for a very simple report.

And so with that, I would like to conclude my oral testimony.

Senator Bennett. Do you have the video that you showed me in my office on the Yugoslav situation?

Mr. Branigan. Yes, I do.

Senator Bennett. Let's take another minute to show that. I think the Members would find that interesting.

Mr. Branigan. Okay. There are two things I'd like to touch on with this. One is that on the advice of Steve Belvin (PhD), Bill Cheswick had started looking at the Yugoslavia network during the NATO conflicts back in 1999. Starting around March 27th, what we did was we looked at how many routers we could find that were available in Yugoslavia, and we found about 75, and on average you would see it was around 75 up until May 2nd, and then on May 3rd some events happened and routers start to disappear.

And so what we're going to do now is show you a video of what we've seen with that, which is – let me try that again. Okay, there we go.

So what we have here is in the magenta, we have what is Yugoslavia. Everything that's in blue was between our test host over in New Jersey over into Yugoslavia. And things that started to show for us that were very interesting were the following:

First of all, this spot here, you can see there's a lot of change to this network over the time. Another one is that you'll see this is a point where one router disappears and seems to fail over to another one.

Secondly, is that this is a point that seems to be served very well.

The final point that was of interest to us during our view of this is this point where this pointer is right now does not disappear. It seems to have the power and the reliability of the U.S. infrastructure, yet it is clearly part of what we felt was Yugoslavia.

When we decided to take a closer look at this point, we found out that the last Internet access point before we reached it, was somewhere in Maryland, and found out, at that point, that most likely what we uncovered was either an embassy or consulate or something that was actually on U.S. soil but is still part of the Yugoslavian government and Yugoslavian network.

So from that point, it was very interesting to see. The last things I would want to focus on some details. We looked closer at it, knowing which were the points for all the routers that we saw. This one has some labeling on it.

You'll see that down at this point here is that point that doesn't disappear, and this is router that's going to take significant damage.

This was May 2nd, 1999 before NATO publicly declared that they were changing their attack to go after the power grid and the infrastructure. And this was May 3rd.

So again, May 2nd to May 3rd, when you look at that in some detail, you can see the significant amount of change that occurred there.

Now one would also think that with this type of information, this is the type of information that can be used for cyber warfare or other things. Because this is pointing out where some of the most vulnerable routers can be.

And now it doesn't matter as much where it's physically located. All I need to know is it's network address. And this is the part that's most troubling. Because now, if these points are vulnerable, with taking out

this router, if I can take it out virtually instead of by shutting off the power, I can shut of a large section of the network.

Senator Bennett. Thank you. That fascinated me when you presented it in the office, and I think it's appropriate to have it as part of the record.

Ms. Lipps, thank you.

OPENING STATEMENT OF MS. PEGGY LIPPS, SENIOR DIRECTOR FOR SECURITY AND RISK MANAGEMENT INITIATIVES, BITS

Ms. Lipps. Thank you, Senator Bennett.

I am Peggy Lipps. I am Senior Director of Security and Risk Management Initiatives for BITS, the Technology Group for the Financial Services Roundtable.

I'm here to present testimony on behalf of Catherine Allen, CEO of BITS, who regrets not being able to be here in person.

I believe you have my written statements for the record, and I will take this opportunity to summarize the main points.

BITS was established to focus on critical issues at the interface of technology, commerce, and financial services. BITS is not a lobbying organization. We serve as a not-for-profit consortium for business and technology strategy, and are a sister organization to the Financial Services Roundtable.

My testimony today focuses on three major topics: the seriousness with which our industry takes the issue of critical infrastructure protection, the leadership role that BITS and the financial services industry is taking in this area, and what we believe Congress can and should do to address the issue of critical infrastructure security.

Online delivery of financial services depends on large and complex public as well as private networks. The financial services industry is dependent on the other core infrastructures, electric power, telecommunications, transportation, and they depend on financial services for their core operations.

But no one sector can address these issues alone. Appropriate cross sector actions include interdependency, vulnerability analysis, information sharing, awareness building, identification of research and development gaps, and contributions to the development of an informed and integrated national plan that both industry and government can use as a business case for action.

Some examples of the industry's efforts to address these issues and to create and build a strong public-private partnership, include: (1) Partnership for Critical Infrastructure Security, or PCIS, which promotes reliable provision of critical infrastructure services through cross-sector coordination. BITS is a founding member. (2) Critical Infrastructure Assurance Office, or CIAO, which was created in response to Presidential Decision Directive 63 to assist in the coordination of the federal government's initiatives on critical infrastructure protection. BITS has

been involved since its inception. (3) the Financial Services Information Sharing and Analysis Center, or the FS/ISAC, which is a facility for anonymously gathering information on threats, vulnerabilities, incidents, resolutions and solutions. The FS/ISAC is currently focusing on ways to share financial cross-sectorally and, (4) the BITS Financial Services Security Laboratory, which was established to test e-commerce products against the financial services community's strong security requirements.

BITS uses a cross sector approach to addressing these issues, focusing on inclusion, education, and proactive involvement. Once we have addressed an issue within our sector and have fully vetted it with key stakeholders such as technology providers and government, including industry regulators, we use vehicles such as the PCIS to share our results and information with other sectors.

BITS uses a risk management model. I will focus on technology, process and the insurance components.

In the technology realm, our goal is to ensure that the technology products developed for our industry incorporate features and functionality that comply with financial services security criteria.

Some examples of those efforts include, again, the BITS Financial Services Security Lab that provides a BITS Tested Mark to products that meet the industry's security criteria, and the BITS Wireless Technologies effort, which is a process to address security and end-to-end reliability with the carriers, device manufacturers and solution providers.

Regarding processes, we focus on the development of self-regulatory guidelines. An example is *The BITS Voluntary Guidelines for Aggregation Services*.

A year ago, this new consumer service, which provides a consolidated picture of a consumer's on-line financial information was seen as a major risk.

Today, due to the *Guidelines*, which build in the necessary security and confidentiality criteria, the service can be delivered in a safe and effective manner for the consumer.

Another example is the BITS *Framework for Managing IT Service Provider Relationships*. The financial services industry, as well as other industries, increasingly rely on third party service providers to support on-line delivery of their products and services.

BITS is publishing guidelines for selecting and managing IT Service Providers based on industry best practices that meet regulatory requirements and provide a framework for service providers and financial institutions to establish appropriate controls.

And lastly, the role of insurance is critical because even with the best of processes, people and products, no system can be one hundred percent secure.

Increased concerns over security vulnerabilities are driving a need to review the role of insurance. BITS has organized an initiative to help define and fill the gaps and we have been working with the Critical

Infrastructure Assurance Office (CIAO) to address the role of public and private sector involvement.

As we work within our industry sector and with other sectors, we have encountered some obstacles to cross sector cooperation that we would like to bring to your attention. We believe we can overcome most of these but some may require assistance from Members of Congress.

I'll mention four of the most important.

First, awareness of the growing impact of our nation's dependency on automation and interlinked networks and the significant interdependency among critical infrastructures is not universally understood.

The PCIS, working with the CIAO, has developed a broad outreach plan that will target several key groups from CEOs and government officials and their staffs, to auditors and systems administrators.

Second, there are significant real and perceived barriers to information and vulnerability assessments. The *Freedom of Information Act* (FOIA) was designed to provide information to the public on government actions, but some companies are reluctant to share vulnerability information with the government for fear of a competitor's subsequent FOIA request or the reporting of erroneous information.

Third, the Internet knows no borders, but the various national defense and law enforcement organizations around the world are bound by archaic, physical limitations. Physical jurisdiction is irrelevant in coping with crimes conducted across borders in minutes and seconds.

And, fourth, market forces alone will not provide sufficient research and development to meet sector economic security or national security needs.

The PCIS is conducting a gap analysis of existing and planned critical infrastructure protection research by industry, academia, and government. The government could use that report to provide incentives or directly fund the needed research to close that gap. Further, attacks on our critical infrastructure may require cohesive and comprehensive plans.

We propose that you consider the following thoughts in approaching this critical issue of infrastructure protection.

First, support private-public sector partnerships in the ways that we have described today.

Second, align laws and regulations. We have taken the responsibility to make coherent industry-based recommendations available throughout the financial services sector.

Third, promote regulatory equality to ensure that all entities offering financial services are required to adhere to the same meaningful standards for security and privacy.

The leadership that BITS, the PCIS, and other members of the financial and security communities have taken reflects the seriousness with which we regard this issue of critical infrastructure protection.

We believe that the strong public/private partnership that is emerging is the right approach, and we look forward to working with you and the Committee on these vital issues.

[The prepared statement of Ms. Lipps appears in the Submissions for the Record on page 74.]

Senator Bennett. Thank you very much.

Mr. Andrews?

OPENING STATEMENT OF DUANE P. ANDREWS, CORPORATE EXECUTIVE VICE PRESIDENT FOR SCIENCE APPLICATIONS INTERNATIONAL CORPORATION (SAIC)

Mr. Andrews. Good morning Senator Bennett, Members of the Committee. I'm pleased to be able to support your examination of cyber security in the U.S. economy. This is a very difficult and multi-faceted challenge.

This morning, I would like to briefly highlight a few of the major issues related to cyber security that I believe require attention. For perspective, I've been involved with cyber security matters for some time, both in government and industry.

Currently, my company, Science Applications International Corporation, provides support to the Department of Defense and several civil agencies, including the supporting the government's FEDCIRC Incident and Reporting Handling Services.

We also support commercial firms. We founded and still have an interest in a commercial security firm, Global Integrity, that developed and operates the first Information Sharing Analysis Center, or ISAC, for the financial services industry, as well as ISACs for global firms and in Korea.

I personally am active as a member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee, commonly known as the NSTAC.

In 1994 and again in 1999, I was a commissioner on both of the Secretary of Defense/Director of Central Intelligence-sponsored Joint Security Commissions that addressed cyber security. And I chaired a 1996 Defense Science Board Task Force on Information Warfare Defense.

And finally, as Assistant Secretary of Defense for C31 in the previous Bush Administration, I initiated the Defense Information Assurance Program and the Department of Defense's information warfare program.

The report of the first Joint Security Commission in 1994 included the observation that "the security of information systems and networks [is] the major security challenge of this decade and possibly the next century."

And it went on to say that there is insufficient awareness of the grave risks we face in this arena. That was in 1994. And in the seven years since that report, there has been progress. ISACs are enabling some industry sectors to share information on cyber threats.

Presidential Decision Directive 63 organized efforts to address the critical infrastructures of the United States, and similar efforts are underway in several other countries.

The Department of Defense has established a Joint Task Force for Computer Network Defense and has assigned operational control to the CINCSPACE firewalls are in widespread use and there has been modest improvement in training the work force on how to react to cyber events like viruses.

However, in my view the rate of progress has been slower than the growth of the potential threat, and overall we have lost ground over those seven years. A number of nations are developing information warfare skills. Technology has gotten more complex. We have had deregulation of the telecommunications industry, and are entering an era of converged services for voice, video, and data.

And our commercial software packages are so large and complex that we cannot be sure what they contain.

Further, the Internet, which has become so important to our economy, is getting too big to monitor effectively. And Senator Bennett in our previous briefing highlighted that quite well.

The failure to act is another major contributor to why we have lost ground. For a decade, we have had study after study, and report after report, pointing out that our economy and our national security depend on the flow of information and that this flow is at risk.

Numerous scenarios have suggested that the interconnection of systems and the cascading effects that can result from attacks can cause major disruptions to our economy, and to our national security systems.

These studies have also shown that we don't have to spend the gross national product or wait a decade to significantly improve our security posture, and that we can take sound steps to protect systems and networks without trampling on civil rights.

So the question is: Why haven't we taken the necessary steps to address the cyber threat? And I can think of four factors that contribute to this.

One. This is technically complex and very hard to understand. A high geek factor, as some have pointed out. And that makes it hard for policymakers to engage. I found, when I was in the Pentagon, it made it very hard even for military leaders to understand how important this particular threat was. So it's a very difficult one and it's difficult from a technical complexity.

Two. Every dollar that would go into protection, detection, and reaction is a dollar that comes out of some mission or business function. I can tell you how popular you are when you stand up in the Pentagon and suggest cutting back forces, planes, ships, tanks in order to pay for cyber security. So it's a problem.

Three. There is no oversight mechanism that holds federal agencies and critical business functions accountable.

And four, we are treating this more from a tactical point of view than as a major strategic problem.

To amplify, let me start with infrastructure protection. This effort traces back to Section 1053 of the *National Defense Authorization Act*, the Kyl Amendment, and from 1996. This legislation called for the President to submit to Congress a report setting forth the results of a review of national policy on protecting the national information infrastructure against strategic attacks.

Subsequently, the President's Commission on Critical Infrastructures was established. The Commission delivered a report. The recommendations in the report led to the creation of the National Infrastructure Protection Center (NICP) and related activities.

In my view, the Commission, in its report, did not fully come to grips with preparation for the strategic attacks, the kinds of attacks we've been talking about today, as called for by Congress. But rather it turned to more tactical matters, things that were easier to deal with and ones that we could get our arms around.

In April of this year, the General Accounting Office released a report entitled "Critical Infrastructure Protection." Excellent report. "Significant Challenges", part of the report, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities" was the title.

While highlighting some progress in investigation and response support, the report notes several areas that need attention, particularly in aspects of national security.

I understand the current Administration is addressing the government's critical infrastructure protection strategy and the specific requirements of the NIPC, and I hope they will fully address the challenges and shortcomings identified in that GAO report.

The decision to place the NICP in the Justice Department led to law enforcement assuming the role as the front line of cyber defense. Once again, this focused efforts at the tactical level. Today, by default, the NIPC considers a cyber intrusion to be a crime. This has led to a lot of focus on hackers and on computer viruses. Clearly, these activities require attention, but I do not believe that they rise to the level of a strategic attack on the national Information infrastructure.

This is not to fault the important work or dedication of law enforcement entities as they fight crime in the cyber arena. It is just that law enforcement is not a sufficient response to this strategic challenge. More importantly, because of the tactical focus, as a nation we are not addressing the architectural strategies and the recovery capabilities that can both deter and ensure that we can recover from such strategic attacks.

The Defense Science Board Task Force on Defensive Information Warfare Operations, in their summer study last year, and which was released in March of this year, notes, "current policies and legal interpretations at the NIPC, the FBI, and the Justice Department, have

prevented timely and effective information sharing about potential national security risks."

Today, there is no effective process in place to rapidly shift from a law enforcement posture to a national security posture, nor is there a coordinated effort to be able to rapidly restore vital functions that are essential to the national defense or to the national economy.

These are areas that require attention. Further, I believe the Department of Defense should be required and empowered to take all appropriate steps to engage and repel intruders from its computers and networks without having to first resort to the criminal justice system.

When warranted by circumstance, the DoD should also be prepared to participate in the protection of networks of critical importance to the national economic security. Maintaining an agile, robust ability to defend the nation must have priority over criminal prosecutions.

Let me briefly turn to accountability. For over 10 years, the Federal government has promulgated sound information security policy in OMB circular A-130. If this policy had been followed over the years, the protection of information in the government would be in much better shape than it is today. I suspect industry would have followed the government's leadership and also improved its security posture. However, I am unaware that anyone has been held accountable for not following this clear policy.

Another major challenge that requires attention is the sharing of information about cyber incidents between businesses, between governments, and between government and business in the academic communities.

The GAO report that I talked about earlier cited a number of challenges that remain. I urge both government and industry to move more freely to share information that reveals our cyber weaknesses.

I understand that legislation is being considered to protect information exchanges on cyber incidents. Ms. Lipps mentioned the *Freedom of Information Act*. I certainly urge us to look seriously at what you can do to help protect the information that businesses would share with the government.

And I think that antitrust protection is another area that is being examined and would certainly help facilitate from a business point of view sharing of information with the government. Both of those would be very useful steps.

So in conclusion I believe we must begin to address cyber and Internet issues from a broad strategic point of view and not get overly focused on the equities of any particular government constituency.

I believe we need to take a fresh look at the challenge of strategic attack to our Nation's cyber infrastructure, and I believe the government needs to better clarify the issues and better characterize what that threat would be so that industry can help the Nation secure its infrastructures.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Andrews appears in the Submissions for the Record on page 83.]

Senator Bennett. Thank you very much. I would say to you and Ms. Lipps, I am working on a FOIA bill which we hope to introduce relatively quickly. Your testimony here is very helpful.

Mr. Edmonds.

OPENING STATEMENT OF ALBERT J. EDMONDS, PRESIDENT, EDS FEDERAL GOVERNMENT INFORMATION SOLUTIONS

Mr. Edmonds. Mr. Chairman, Ms. Dunn, it is a pleasure to be here this morning to discuss this important topic. I am Al Edmonds, President of Electronic Data Systems's (EDS) Federal Group. I am responsible for the federal business as it relates to the civilian side, military, and the GSA Federal Government.

EDS is a global services company that provides strategy, implementation and hosting for clients managing the business and technology complexities of the digital economy.

We bring together the world's best technologies to address critical client business imperatives. With over 120,000 employees in 55 countries, EDS serves the world's leading companies and governments.

The *USA Today* article brought home to me very clearly that we need to reinforce the fact that the cyber security is a global issue and not just a domestic issue. This is a global Internet that we're dealing with.

The threats to our national security and our economic security may come from any place in the world. Our economy and national security establishments are global, linked together by business trading partners and formal governmental alliances like NATO.

We must be cautious not to think about these issues in only a domestic context. The future of the digital economy hinges on a secure Internet. It is just that simple.

Our Nation's national security is faced with new risks, as are public safety, law enforcement, and economic security.

When I say "economic security," I am referring to the security needed to protect the commercial entities and industries that make up the U.S. economy. National security and economic security are closely related.

So while the benefits of the Internet continue to accrue enormous benefits to U.S. citizens and companies, we as a nation continue to face the reality that the Internet is vulnerable to attack. We saw just last year the huge costs related to a denial-of-service attack.

The 'I Love You' virus was estimated to cost approximately $8 billion. I think that is conservative. It was just a forerunner of what we can expect in the future as more countries become interconnected.

The FBI reports that of 90 percent of 273 companies that they surveyed there were at least 90 percent breaches on those attacks.

This is an estimate of a $300 million loss. I think that is also conservative because most companies will not tell you how much they really lost, especially in an industry like the financial industries.

Although the economic cost of last year's denial-of-service attack may be considerable, I think the big impact is not only the loss of those dollars but the trust that you lose in the Internet when it gets attacked like this, and the reliability and safety of the net itself.

Add the threat of cyber terrorism to a daily dose of viruses, fraud, and money laundering, and it is not hard to see how any other issue needs more attention from Congress and the administration than the Internet.

As a matter of fact, the Internet really has become the crime background of the new economy. There are many, many instances where we know that organized crime, both domestic and foreign, have used the Internet as their backbone.

The cost of protection is going to be high. The market analyst firm IDC predicts that spending on cyber security will increase 21 percent annually to $17 billion by the year 2004.

I would also suggest that you do not be misled by the recent failure of dot coms. Governments and industries around the world will continue to invest in infrastructure, applications, and transition to the Internet because the benefits are absolutely huge.

Companies are using the Internet to develop new business models that provide lower cost and lower prices. That is good for U.S. companies who must find ways to maintain their competitive edge in the global economy.

The Internet continues to be a way for industry and government to lower costs and to reach customers and trading partners.

So it is pretty clear to all of us that no nation can afford to have its telecommunications systems at risk. No nation can afford to have its financial system attacked by criminals. No nation can afford to have its medical records available to everybody to peruse. None of us can afford to have our energy distribution distributed by hackers.

The Internet has transformed how well we live and how we work and govern, but because it is so valuable to all of us it must be secure, reliable and always available.

So how do we solve these cyber security issues? What role should the Federal Government play? What actions should Congress take? What should industry do?

I have a short list of 10 recommendations that I would like to run through quickly.

My Chairman and CEO, Dick Brown, has been a leader in numerous CEO groups that have developed many of these recommendations.

First, we must make greater investments in information assurance technology and services. There is clearly an increased need for more investment by industry and governments in information assurance technology and services to improve cyber security and fight cyber crime.

Second, partnership and cooperation. U.S. industry and the Federal Government with law enforcement and national security must continue on the current path to work together in close partnership. Cooperation and partnership are the keys to success because the government cannot solve these problems alone, nor can industry.

Third, industry leadership. Because the Internet is mostly owned and operated by business, industry leaders must take the cyber lead on security. Industry leadership means more attention to sharing information about risks and vulnerability, greater investment in information assurance services, and driving business-to-business security standards.

Fourth, information sharing and analysis. This is a vital role for industry to create industry information sharing and analysis centers, as Mr. Andrews just mentioned, to share information about cyber attacks. We have one for IT, we have one for the financial industry. We need these same kind of centers for all the rest of the major industries.

If the Federal Government removes certain barriers – we talked about the FOIA, antitrust – industry will be willing to share information, but they will not do it without those things being adjusted.

If this kind of information is shared with each other and with the government, the entire community of users will be stronger and better able to fend off attackers and lower the risks of operating on the Internet.

I believe that the information sharing is critical to addressing the cyber security issues.

Fifth, lead by example. The Federal Government must lead by example to be a model in this cyber security area.

Sixth, we need to develop federal policy in close coordination with the U.S. state governments and other nations. The Federal Government needs to preempt some of these laws so that we don't have 50 different rules on information security and cyber security but have one that we can probably make.

We need to work on the shortage of skilled personnel because that shortage of skilled personnel has caused us to go and try to do this job with all kinds of people, and we don't really know the quality of the people doing some of the work in systems administration.

We need to avoid cost shifting between the Federal Government and industry and industry to the consumer. We need to make sure that everybody has a piece of the action and has a stake in the game.

And, Mr. Chairman, there is no substitution for privacy and security. We need them both. We do not need to trade out one for the other.

And finally, as our regulatory bodies deliberate over oversight to all these different industries, we need to encourage them to pay more attention to cyber security and the infrastructure and try to prod their constituents to do more in this space.

The digital economy has erased national borders, removed economic barriers, and allowed enterprises to become truly global. The digital

economy has linked business with their customers and suppliers in ways never before imagined. It also promises great prosperity. But we must be vigilant. We must depend on security and trust.

Together we can provide both. We can get through this with close collaboration of government and industry. Let's all make cyber space safe for all of our constituents.

Thank you, Mr. Chairman, for the opportunity to talk about this. This is very, very important. Thank you.

[The prepared statement of Mr. Edmonds appears in the Submissions for the Record on page 87.]

Senator Bennett. Thank you very much for your testimony.

Let me make a comment. All of the witnesses and some of the questions have all addressed the question of how the government is structured and what are we doing about it.

I do not think it violates a confidence to say that Dr. Condoleeza Rice has been in my office and has discussed this with me and Senator Roberts, who is concerned about it from the Armed Services Committee, and I was very encouraged and heartened not only by her commitment to this, but more importantly her knowledge.

I have had the experience with Y2K, and now with this issue of having to educate people as to where we are, and that is one of the reasons for this hearing, to educate you and hopefully through the press and the general public.

Dr. Rice was educating me. She knows this issue very well, not only from her academic background and her understanding of national security issues but also from her experience as being a board member on a number of companies, so that she sees this from the industry side as well as the government side.

I am very heartened by her leadership down at the White House and her determination to see that this gets an appropriate high level of activity.

I did not want to break in on the questioning of my colleagues, but several of my colleagues raised the issue of what is going on and I wanted to share that and make it part of the record of what is going on now.

Mr. Branigan, your maps illustrate the Internet right up to an entity's firewall. Do we have any way of understanding the size of the networks which may exist beyond the firewall?

Mr. Branigan. If I could, I would like to have Mr. Cheswick join me at the table.

Senator Bennett. Okay, please, Mr. Cheswick.

For example, is there one machine, or a thousand machines on the other side of the firewall.

Mr. Cheswick. We can usually tell the size of a corporation by the amount of space that has been allocated to them. But they can also use private space.

So it is actually quite difficult to tell, and any estimate you hear about the number of computers on the Internet is just that. It is a wild guess. There is no way to really go and find out.

Senator Bennett. How many bad network connections does it take to compromise the company's network and place its intellectual capital or financial information at risk?

Mr. Branigan. Just one.

Senator Bennett. I was afraid of that.

Mr. Branigan. A number greater than zero, but not much.

Senator Bennett. Okay.

Mr. Cheswick. Often zero, if you have an insider who is bad, and that is often the case.

Senator Bennett. Do you have any information, any of you – you talked about the insider who is bad – I talked about the virtual insider, somebody who breaks in but does not have a legitimate reason to be there. What about the insider, the disgruntled employee, somebody who feels he did not get the bonus he was entitled to, did not get the promotion, is going to leave but by george he is going to leave something behind?

Do we have any information anywhere about how serious – it is obviously a serious problem when it happens – how often it happens? Do we have any kind of wild guess as to the percentage of challenge that this has in terms of security?

Are we focusing so much on preventing other people from getting in that we are missing the possibility that somebody already has the password and can be the bad actor?

Mr. Andrews, you look like you want to take that one.

Mr. Andrews. Well I am just reflecting from commercial clients that we have had. We feel that, and have seen, that really the insider, the real insider, or the disgruntled employee is actually a greater risk than the virtual insider.

Most companies receive more damage, more of a threat from insiders, true insiders, than from what has been seen in the past as the external threat.

Now that external threat is growing, but I think today the statistics overwhelmingly would show that it is the real insider, that disgruntled employee, maybe just a good-intentioned employee doing dumb things, or someone selling for economic reasons, selling access or data to a company's internal systems.

Senator Bennett. Mr. Andrews, you talked about the need to organize this as a strategic issue and I agree absolutely with that. I made my reference to Dr. Rice as she is trying to raise it to the strategic level.

Without angering – I hope I do not anger my friends at the FBI – I was a little critical at the decision of the Clinton Administration to put the primary focus on the FBI for exactly the reason you have described. It makes it a tactical issue rather than a strategic one.

Would you comment on where it ought to be? Is the National Security Director, Advisor, Condoleeza Rice, the right place for it? Or if you were king for a day, or president for an hour, where would you put it?

Mr. Andrews. I think there are varying responsibilities in the Federal Government. I think that you need leadership in the White House, and I think that Dr. Rice is doing an outstanding job in beginning to address this very difficult problem.

I have been in discussions where she has made presentations and discussed this issue, and she really is trying to get her arms around it.

She has the Critical Infrastructure Assurance Office, Dick Clark, under her that has been trying to address it. So you do need leadership from the White House.

But in the end you have got to have accountability in the agencies of government to implement. The Department of Defense has got to protect its systems. Other agencies have got to be able to ensure that it can work effectively with its constituencies and protect its systems.

So I think that there needs to be accountability established from the top down. But then we need to hold those officials in the agencies responsible for protecting their systems.

Senator Bennett. I appreciate that comment very much, and you remind me of the experience that really brought me to this whole issue, which was my experience with respect to Y2K.

John Koskanan was appointed the Y2K czar in the administration, but he very quickly and very wisely did what you have just said. He would go around to the Cabinet officers and say: You have a Y2K problem and I am not here to fix it. You fix it. I am here to monitor you, to be a resource to you, to prod you and help you.

But, no, Y2K will not be solved by the Y2K czar. Y2K will be solved by the Cabinet officer.

I remember in the Y2K discussions John Hamry, who was the Deputy Secretary of Defense and got this assignment from Secretary Cohen, he said to me: "Until you started kicking on us, we had never done an inventory of how many computers we have in the Defense Department. We did not know."

And in order to do Y2K, we had to do that kind of thing. Now that is not something that could be driven out of the White House. As you say, that is accountability for the Cabinet officer himself or herself to do within that Cabinet agency.

The good news is we came out of Y2K with a Defense Department inventory of all of their computers. The bad news is, looking down that inventory we discovered, given the length of the contracting cycle at the Defense Department, the procurement cycle, if you have a 486 machine in the Department of Defense you've got a real hot item—

(Laughter.)

Senator Bennett. – because most of the stuff is older than that.

My time is up. Congresswoman Dunn.

Representative Dunn. Thank you, Mr. Chairman.

Thank you for the fascinating testimony, all of you. It is an eye-opening experience for me. I think I would like to ask a general question first.

Are there other nations in the world that we are working with very closely on this problem of cyber terrorism? Are there other nations that are as dependent on the Internet as we are in the United States?

What is happening out there? And is the collaboration with other nations adequate?

Mr. Edmonds. Yes, Ms. Dunn—

Representative Dunn. If Dr. Gershwin wants to join the panel, that might be one he would like to talk about, too.

Mr. Edmonds. We have global customers in EDS, and a lot of government. My job before the current one, I was the global government for EDS, and each one of those governments are very concerned about protecting their information. They are concerned about cyber crime.

They also look to us a lot from the U.S. to lead the way, and our corporations, almost all of them, global, have to deal with this every day.

They also have to deal with protecting the equities of that country's information versus the U.S. information is another issue. That is very, very important. But it is pretty much a global discussion.

There are forums all around the world on this subject constantly. You can look at the schedule of events for most people in this business and they have at least a half a dozen conferences around the world on cyber security.

Dr. Gershwin. Let me add to that a little bit.

There is certainly growing attention in other countries, although as Mr. Edmonds explained I think they do really depend on the United States a lot to lead the way. We have really got more information and more experience on this than most other countries.

But I see, for instance we had a conference recently in Europe and at that conference there was a great deal of interest expressed by some of the participants, in cyber security issues, more than I might have expected.

So I think it is a growing realization. I know the Defense Department has had a number of exchanges with Western European countries on these issues and has done some gaming experiences to try to sensitize people to the significance of infrastructure.

It is very important when people understand that it is infrastructure and not just military information systems, that everyone's infrastructure is really the critical issue. I think that is taking hold worldwide, although it is very recent and I would say probably mostly in Europe.

I do not know really how much of that is understood elsewhere. But it is certainly an area that is going to need a lot more attention.

One of the inhibitions I think on making it all work is that there is again a lot of concern about proprietary information, U.S. technology,

foreign technology, whose technical secrets have to be revealed in order to accomplish some of these objectives.

So just as we have some of the domestic issues associated with sharing between U.S. Government and U.S. industry, we have the same kind of problems I think in sharing internationally. Those I think are serious inhibitions in making progress.

Mr. Branigan. If I may, I would like to add, as well. I have been involved with the G8. They have had a Committee on Safety and Security In Cyber Space, and I have been involved with that for the past year.

The member nations have brought industry, in addition with the governments, to try to tackle these issues, as well. What they are trying to do is address some of the jurisdictional problems that you see with cyber crime, and they are making great progress with it. Another organization that both Bill and I are involved with is the New York Electronics Crime Task Force out of the Secret Service up in New York City.

What they are doing is bringing a lot of law enforcement together with industry to talk about these issues in a trusted environment, as well. So there has been a lot of work going on that we have been involved with both internationally, and when you look at the law enforcement side, they are just bringing police from different countries to talk about their common issues.

So some of it is very governmental, and some of it is almost on-the-street level.

Ms. Lipps. Also from a BITS perspective we have been having increased communications with the international trade associations, the payment associations internationally. We have started to work, to some degree, with the Basel Committee on e-banking, which is taking a look at these issues as well.

We have received increased calls regarding the guidelines that we are producing and specific requests for us to share that information across the borders.

Representative Dunn. I think that is fine, Mr. Chairman. Thank you. Thank you, panel.

Senator Bennett. Following up a little on what Congresswoman Dunn asked, I see a tension here. Obviously in financial services we want the money that transfers around the world to be secure. We want the information to the financial institutions to be secure. Because so much banking activity takes place across borders, we want that kind of cooperation.

At the same time, Dr. Gershwin, there are some countries that want information from us that they do not want to pay for. And they want to get into various places, whether it is Moonlight Maze, or Solar Sunrise, or whatever it is, those things that have now been talked about.

So if you were a policymaker in an unnamed foreign country in an indeterminate continent – we will be as vague as possibly can be – one

imperative says let's cooperate with the United States because they are the backbone. We have got to keep all of this information secure. We have got to make sure cyber crime does not happen.

And the other side of the policymakers in the house are saying, yes, but if we break into the labs at Livermore, or if we break into Boeing to find out what they are doing on their latest design, look what an advantage that would give us.

Now, Dr. Gershwin, you are probably the best one to respond to that, but if anybody else has some views, do you see – we are all sitting around now with our feet on the table looking at the ceiling and thinking big thoughts. Do you see that kind of tension possibly coming along in the future?

Dr. Gershwin. Well I think the inevitability is that countries, groups, will always see areas where they can gain an advantage by doing things either clandestinely, having ways to get secrets for nothing, you know, not having to pay for them, being able to extract things through cyber intrusions that they would not otherwise be able to get at, and that is an inevitability. That is not going to go away.

The world is not going to be entirely safe for this kind of phenomenon no matter how much cooperation goes on, no matter how much good will there is.

But there are many very legitimate international functions in the business world certainly for which we have a globally shared interest in protecting, although there may be some outliers in this in terms of countries or groups that do not share this vision.

But, for a very large fraction of the world's business there is I think a globally shared interest in regulating the transaction so that there is greater security and things are on a more level playing field.

So I think there always will be this tension. We are obviously keenly aware of it in the intelligence business because we are obviously very concerned about bad actors, whether it be state actors or non-state actors, and we assume that those bad intentions and bad actions will be going on inevitably.

No degree of sharing and goodwill will entirely stop that from taking place. So we are in the business to stay, of paying attention to those kinds of things.

But I think there is a great deal that can be accomplished probably internationally in the way of sharing information with governments, including governments that are not always friendly to us.

There are many things that we can accomplish with countries with whom we have serious rivalries which can probably help a lot. Because they are all benefitting from the global economy, and there are many aspects of that for which they should want a greater degree of security as well, notwithstanding the fact that they will then take advantage of opportunities to do things that go beyond.

Representative Dunn. Could I just ask one when you are finished?

Senator Bennett. Sure.

Representative Dunn. I was just thinking. You know, this whole discussion is interesting in one way in that it is tough to regulate something that is criminal activity. It reminds me a little of the grey economy.

But does anybody have any idea whether any of this could be handled through trade agreements, for example? Is there anything being done on that front?

Mr. Andrews. I will make a comment. I think that trade agreements are just one tool to help facilitate cooperation.

We have found, as we have tried to defend our commercial businesses against organized crime in the cyber world that there are a number of countries that are very cooperative, even though that are not sometimes our friends in other forums. I would cite Russia for example that has cooperated in several instances in helping us track down criminals that have been attacking from their territory U.S. corporations.

Other countries, some that are our friends, serve as havens for hackers. And because of that, it is very difficult for us to be able to trace back to the source, even if it is a different country, say another European country that is using a second European country as a launching pad for its attacks.

As long as there are those safe havens in the world, it is going to make it even harder for us to be able to hold our friends accountable for not engaging in the dialogue as our friends on the one hand and attacking our industries, or even probing some of our national security systems on the other.

So I think one thing that we can do is use every tool in our tool kit, including trade agreements, to put pressure on those countries that are havens for criminals, and even for hackers, havens for cyber anything, to open their doors up and let our law enforcement and other agencies be able to trace back these attacks all the way through the system to the source.

Mr. Edmonds. I think the real opportunity to make a difference in the international trade area, I think if we could focus on industries, we have found out that industries kind of make up their own rules of engagement across the world.

The energy industry, health care, they all come together to try to find ways to solve common problems. Even our own U.S. Government has a tendency to get along well in those industries.

The financial industries around the world will work on how to protect the integrity of the financial industry by encryption, by regulation, those kinds of things.

So I think one of the things we really ought to have as a parallel effort as we deal with things like trade agreements and all is let the industry, the natural flow of those industries help us do this.

You have conventions around the world in those market spaces. You go to Thailand to have an energy conference with people around the

world and they will talk about the same kinds of problems: protection, integrity of their industry. So I think that is one area we could look at to make a difference and focus. And you can get some Executive Branch of the government to help us with that if we did that.

Senator Bennett. Well thank you all very much.

I just cannot resist one last comment. Dr. Gershwin, in your basic testimony you talked about nation-states developing tradecraft skills, and I got a picture out of all this that I have not had before, that the temptation to use those tradecraft skills to find out what an American company may be bidding for a particularly lucrative contract which would otherwise go to that country's state-supported industry is a temptation that will be very, very strong and adds all kinds of implications to what the future might be like.

Dr. Gershwin. I certainly agree.

Senator Bennett. Okay. Thank you again. We appreciate all of your coming. The hearing is adjourned.

[Whereupon, at 12:10 p.m., the Committee was adjourned.]

SUBMISSIONS FOR THE RECORD

PREPARED STATEMENT OF SENATOR ROBERT F. BENNETT

Good morning, and thank you for joining us today as we take a closer look at the issue of cyber security within our increasingly "wired world." During this hearing, we will explore current and future cyber threats to U.S. economic and national security. We also will examine whether the current policies governing cyber security and critical infrastructure protection are sufficient.

The National Intelligence Council will begin by placing the cyber threat over the next fifteen years in the context of globalization. Next, we have a distinguished panel of four representatives from the private sector who will discuss the following: (1) the unintended security issues related to interconnectivity; (2) industry initiatives to mitigate cyber security risks; (3) the need for the for the United States to focus on cyber security in a strategic way; and (4) how strong public–private partnerships can protect our information infrastructures.

Over the past ten years, the world has undergone dramatic technological changes. As technology systems rapidly evolve, most notably the Internet, so has the risk. The benefits of technology are easy to understand. Improved communication means a growth of commerce, expanded free trade and a more closely integrated world.

However, this increased reliance on information technology creates a complicated set of threats to U.S. national and economic security. The enormous proliferation of connectivity and technology now means that potential adversaries no longer need traditional military tools to attack or disrupt the U.S. economy. The tangled web of networks is a potential launching pad for attacks, espionage and viruses by almost anyone around the world. Computer viruses, like the "Love Bug" can cause global damage and disruption. Some of these computer networks and information systems operate parts of critical infrastructures once only accessible by the military. For example, in early May, hackers appearing to originate in China routed themselves through servers in Oklahoma and California and found their way into the California power grid. While the hackers did not cause any blackouts, the potential damage could have been significant.

The world wired together by the Internet is based on computer network connections and powerful communications nodes that are literally redefining the geography of commerce and communication. When we think of national security, we think of making our borders secure. However, on the Internet, borders disappear. In addition, eighty-five percent of U.S. critical infrastructures, such as telecommunications, energy, banking, and transportation systems, are owned by the private sector. In an interconnected world, the private sector is on the front line.

It is important to remember that the Internet was built for sharing, not security. It is inherently open and decentralized. This openness can be

costly, though. Computer Economics, a California-based research firm, reports that computer viruses in 2000 cost American businesses over $17 billion. Unfortunately, no one really knows what was lost in terms of intellectual property through espionage, hacking, or foreign intelligence services.

If we leave this hearing with one idea it should be this: The physical world that Rand McNally and other mapmakers introduced us to must not dominate our strategic thinking for the next century. Instead, we - Congress, the executive branch and the private sector - must view the emerging geography from a strategic perspective. Attempts to map the Internet reveal a world where physical geography disappears. We must resist the temptation to think about the Internet in a traditional context of geographic boundaries.

Over the past several years, there have been many efforts to understand the security associated with cyber-based threats. All too often, however, the complex issues of cyber security and infrastructure protection are overshadowed by the attention paid to hacking exploits and website defacements. It is time that we finally turn to the more strategic security challenges to our economic and national security. We need to take a fresh look at U.S. cyber security infrastructure protection policy. Thank you.

PREPARED STATEMENT OF SENATOR JACK REED, VICE CHAIRMAN

Thank you Mr. Chairman. As a member of the Senate Armed Services Committee as well as this Committee, I am especially pleased to have the question of cyber security and the U.S. economy addressed today. Of course, the issues of security and cyberspace are myriad and complex – we will barely be able to scratch the surface in a single hearing. But, judging from the list of eminent witnesses who have agreed to appear today, I'm sure that we will learn as much as is possible during our limited time. I welcome all of our witnesses and presenters – thank you for coming before the Committee today.

Advances in information technology and applications were critical to the spectacular expansion the U.S. economy enjoyed during the 1990s. Technological advances in computing and communications, especially the internet, contributed significantly to the resurgence of U.S. productivity in recent years, and they are certain to play important economic roles for years to come.

There is little doubt that increased use of the internet has been a great boon to the U.S. economy. By the same token, however, the expansion of economic opportunities made possible by the advances in information technology and the internet has been attended by an expansion of risks as well. These risks encompass a wide range of interests, from the safeguarding of our national security and the integrity of our financial system to the preservation of the privacy of the individual, with many other interests within this spectrum as well.

We are only beginning to understand the extent of the risks to our critical infrastructure and economic security. The internet maps to be presented during today's hearing bring home the point that internet links can confuse the borders between individuals and other economic entities. Viewed as an entity in cyber space, a corporation has no clear beginning or end. Similarly, national borders are blurred within the context of cyber geography. The internet challenges us to reevaluate our traditional views of how the world works.

And, the new technology challenges us to reevaluate the way government can interact with the private economy. Is the government doing what it can to minimize the risks of cyber threats to our critical defense and civilian infrastructures? How can government best collaborate with the private sector, households and businesses, to ensure the productivity and protection of the economy?

I thank our distinguished witnesses for testifying this morning.

PREPARED STATEMENT OF SENATOR JON S. CORZINE

Thank you, Mr. Chairman, for holding this hearing and thanks to all of the witnesses for appearing here today.

I look forward to their testimony, and learning more about this complex issue. In particular, I want to welcome Mr. Branigan, who is with the Lumeta Corporation, a company based in Somerset, New Jersey.

Mr. Branigan, it's a pleasure to have you join us today.

With the advent, and continuing growing popularity of the Internet, we have learned a great deal and enjoyed many benefits of the new connectivity.

From streamlining supply chains, to democratizing the broadcast media, the Internet has created a communications revolution that has largely benefitted our society.

However, with this growth comes risk.

I am looking forward to this hearing in so much as it will help us to learn more about the growing cyber-security risks that are posed by the connectivity that many of us so enjoy.

Many Americans rely heavily on the Internet – individuals and their families, American businesses and an area that I am highly familiar with, our financial markets, all utilize the Internet as an integral part of their existence.

Because of this, it is vitally important that we learn more about the threat that disruptions, hacking and other invasive practices pose to our citizens, our economy and our national security.

It is imperative that we do all we can to ensure that we are well protected from threats posed to our cyber systems – both domestically and abroad.

Again, Mr. Chairman, I thank you for holding this hearing and I look forward to the testimony from our witnesses today.

PREPARED STATEMENT OF REPRESENTATIVE LAMAR S. SMITH

Mr. Chairman, thank you for holding this hearing on cyber security.

I have a particular interest in this subject. As Chairman of the House Judiciary Crime Subcommittee, I recently held three hearings on the issue of cyber security. The final hearing examined the role of businesses in combating cyber crime.

Crime is still crime, whether it occurs on the street or on the web.

And while other crime rates continue to drop, cyber crime is dramatically increasing.

The economic consequences of cyber crime are enormous. Billions of dollars are lost every year. International software pirates rip off consumers and companies, costing hundreds of thousands of American jobs.

Last May one computer virus disrupted the communications of hundreds of thousands of computers, causing losses estimated in the billions of dollars. And in March, the FBI issued a warning that an organized group of Russian hackers had stolen more than a million credit card numbers from companies' databases.

The internet has fostered an environment where hackers retrieve private data for amusement, individuals distribute software illegally, and viruses circulate with the sole purpose of debilitating computers.

In confronting this issue, the business community faces a dilemma. Do they report cyber crime at the risk of losing the public's confidence in their ability to protect customer information? Or, do they fail to act and risk losses and repeat attacks?

Technology hold the key to the future, and private businesses are leading the way in innovation and products. But if left unchecked, cyber crime will stifle that progress.

I hope to hear from the witnesses on how their companies and businesses are working to enhance cyber security. I also would like to hear about their suggestions for legislation.

Thank you Mr. Chairman.