

**The Information Technology Association of America (ITAA)
and
the Center for Strategic and International Studies (CSIS)
present**

"Strengthening Homeland Cyber Defense"

October 18, 2001
9 am - 12:30 pm
B1 Conference Center
1800 K Street, NW
Washington, DC

**Comments by The Honorable Robert Bennett
U.S. Senator**

SENATOR BENNETT: Thank you very much. I'm delighted to be with you and with this group. CSIS has played a leading role in helping people understand all of these things.

John Hamre, as Deputy Secretary of Defense, led the way in the Defense Department to get them to do what they had to do with respect to Y2K. The good news was that out of the Y2K experience the Defense Department did its first only inventory of all of their computers.

They didn't know what computers they had until we started prodding them. He was a little more graphic in his description of what we were doing. And that's the good news.

The bad news is that as a result of that inventory we found out if you had a 386 machine in the Defense Department you had a really hot item.

(Laughter.)

The procurement system in the Defense Department needs a little bit of work.

Now, I refer back to Y2K because we get a feedback from September 11th that illustrates something that, frankly, I had not thought of. We keep — we kept talking through Y2K that we have to avoid stovepiping. We have to think horizontally. Duane Andrews' comment we have to think strategically, we all agree with that. And then there are things that rise up and hit you with what I used to refer to in my business as a BFO, a blinding flash of the obvious.

(Laughter.)

When September 11th hit and the New York emergency response team went into action, the people who ran that team — and I've been in the center where they have it, with all of the emergency groups gathered together, much like the Y2K center that we built here in Washington, and with great foresight dismantled immediately after Y2K occurred, I called OMB and said, "You know, you really ought to hang on to that." And they said,

"No, no, we're going to — we don't need it anymore. We're going to break it up, and we'll give all of the computers to FEMA."

I mentioned that in one of our appropriations hearings, and the Director of FEMA said, "We got computers?"

(Laughter.)

You know, where did they come from? Quick, let's check. So somehow something like, what was it, \$15-, \$20-, \$30 million we spent to put that response center together for Y2K, and six months later it was gone. And nobody knows where it went. Nobody knows where the equipment went. Just kind of disappeared.

Well, in New York it didn't disappear because they have ongoing emergencies in New York. And after the September 11th incident, the folks in New York said, "You know, if we had not done what we did to get ready for Y2K, we would not have been physically capable of responding to the September 11th bombing."

The redundancy that was built into the system made it possible for us to recover very quickly from the loss of assets that were established in lower Manhattan with other assets coming into play quickly because we were prepared for failure, and we were able to swing into action much more rapidly than we would have been able to otherwise.

And that's when the BFO occurs to me, that cyber security — we talked about thinking strategically. Cyber security is not its own stovepipe. Information warfare is not its own stovepipe. These things are connected.

And I went back to the briefing I received when we had the first World Trade Center attempt, and the fellow who briefed me made a comment. He said, "This is going to sound terrible, but in terms of preparedness for the nation the main thing wrong with the first attempt on the World Trade Center was that it didn't kill more people, because it lulled us into a false sense of security as to where we are with respect to terrorism."

And then he described for me what the terrorists had in mind. You have those two buildings side by side. Down at the bottom of one of them in the basement and first floor area was where the bomb was placed with the expectation that when it went off it would cause that building to collapse into the second building and take both of them down.

It was a fizzle. They weren't able to pull it off technically. But that was their plan. Plus, and here's where the thinking strategically comes in, they were hoping to introduce some kind of nerve agent into the ventilation system so that it would be pumped out into the building. When the rescue officers showed up, they would be overcome and killed, so that the rescue operation would fail.

That was their grand design. They weren't able to pull it off. But you notice when they went at it the second time they flew the airplanes into the center of the building. A

structural engineer in Senator Craig's office ran into his office when that first plane hit and said to him, "That building is coming down." He said, "What do you mean?" She said, "I know the structural composition of the building, and they have put that airplane in exactly the right place to cause the kind of structural failure that will bring the whole building down."

And, of course, the rescue people got in there before the building came down, and they were all killed.

So there was a strategic thought went into that whole situation. It wasn't just, "Let's fly an airplane into a building to get maximum television exposure. Let's think the thing through to get the maximum terror through the whole process." And that's what will happen when cyber terrorism is linked with the other acts of physical terrorism when people on the other side are thinking strategically.

When the next major physical attack occurs, whether it's nuclear or another horrific fire-bombing situation, wouldn't it increase the damage enormously if there were a simultaneous cyber attack on the computers that control the information response?

And we're thinking, gee, shut down the computers. That'll be terrible. But think strategically for just a minute and say, "Shut down the computers in connection with other terrorist acts." In the same hearing that was referred to, I asked the witness from the CIA if, in fact, the first attack on the United States wouldn't be a cyber attack and outlining all of the things that could happen, and he said, "That's because you think the way you do, Senator."

He said, "The first attack" — and this is eerily prophetic — "is likely to be something that is very spectacular on television, because their goals would not be met by shutting down the computers. You can't show that on television around the world and get people's attention. That would be invisible as a public event."

So he said, "The next — the first terrorist attack will probably be something very spectacular and very obvious on television." As I say, he gave us that testimony less than 60 days before the 11th of September.

But think strategically and realize how the two can be tied together to produce maximum terror, maximum fear. Not only has something very spectacular blown up, but we can't do anything about it because all of our computers are shut down. I think that's the area where we're going to be thinking.

Now, with that delightful image in front of us, I want to shill for my bill.

(Laughter.)

And I just happen to have a chart here. I'm not sure that all of you can see it. But basically this is what we're talking about with the legislation that we're offering, and we hope it's moving in the direction I have just described.

Over here you have the U.S. Government. Over there you have private industry. And as is demonstrated by the circular nature of private industry, it's not just one industry but virtually all aspects of industry, and they need to talk to each other, because if you are looking for intelligence with respect to cyber attack you need to pick up a pattern, so that an attack in the banking system that has the same fingerprints as an attack on the telecommunications system will begin to tell you something.

This is not a disgruntled ex-employee taking it out on his employer who fired him. This is a coordinated attack that is hitting in various places throughout industry. And that comes to one of the aspects of my bill, which is that we're going to relax the antitrust rules that will allow people in private industry to talk to each other in this area without being afraid that the Justice Department will come around and say, "No, what you're really trying to do is fix prices. The FTC is after you. What you're really trying to do is an unfair trade practice."

No, if it's channeled in sharing information about attacks, you can — you can be shielded from the pressures of the antitrust laws. That kind of gathering intelligence and sharing intelligence is wonderful and necessary, but intelligence alone doesn't do it. You have to have an analysis.

Let me tell you a quick, brief story from the world in which I live, with which you may or may not identify. But let me talk to you about the necessity of analysis in a political campaign.

Gathering intelligence is done for a political campaign by the professional pollsters. They get on the telephone, and they call everybody and they come back and tell you very authoritatively, this is what people believe. Therefore, you shape your message or your campaign to go in the direction that will get you the most benefit.

And as far as the pollster is concerned, that's all there is to it. And the pollsters love to pontificate and say, "Here are the numbers. This is what you should say. Here are the numbers. This is what you should do. And so on. Here's the intelligence."

I had an interesting experience with respect to that in an earlier campaign. We were running my father's campaign for the Senate in Utah in 1968, corresponding with the gubernatorial campaign that was going on at the same time. And to save a little money we hired a single pollster to do the poll for both campaigns.

Now, he did it in three sections. He did a senatorial image poll, an issues poll, and then a gubernatorial image poll. So we in the Senate campaign got the issues poll and the senatorial image, the gubernatorial campaign got the issues poll and the gubernatorial image. And we ran the campaigns.

After it was over, we had won, our gubernatorial candidate had lost. The pollster that did the work called me up and he said, "Bob, we ran something like 37 campaigns last cycle, and after it was all over we toted up wins and losses, and then we did a little survey in the office. And we wanted to pick the best run campaign of all of the campaigns we did, and I'm happy to tell you you came out as being the one who had the best run campaign."

We then did a little survey as to which was the worst run campaign. The gubernatorial race in Utah came out as the worst run campaign, and you were both working off the same set of data.

Now, how is that possible? And the answer is, you collected the intelligence. We did the analysis. And the fellow who was doing the analysis for the gubernatorial campaign didn't know what he was doing. And if I may be so immodest, I did.

(Laughter.)

This is the difference. So now you come to these arrows going back and forth. It's not enough on the far right of the chart for industry to talk to itself and other components of industry and get the intelligence. There has to be an analysis, and there is a huge whole in the analysis if the intelligence is just the private sector or just the public sector.

Those two have to talk, and the logical place for the analysis to be done is in the Federal Government. And that analysis, obviously, has to be done expertly, has to be done by senatorial types rather than gubernatorial types.

(Laughter.)

And it has to be shared. And this comes to the other part of the bill, because if information, intelligence, comes to the government for analysis, and then under the Freedom of Information Act the government reveals that to the terrorists, that's really not too smart.

So what we're saying is that you can share this kind of information with the government. The Freedom of Information Act will not apply. And the government will do its analysis and then share that analysis back, and you will begin to get the kind of strategic view that we are talking about.

Now, there are those who say to me, "Oh, this is terrible. The Freedom of Information Act protects the public's right to know. And you have to prevent — you are striking a blow against the First Amendment and freedom and all of the rest of that from the public's right to know."

And I say, "Look at my voting record. I have protected the First Amendment as much as anybody, fighting against McCain-Feingold and other attacks on the First Amendment." The fact is if you do not put this kind of legislation in place, private industry will not tell the government.

So the public is not going to get this information to know either way. You are making absolutely no difference to the public's access to this information. If you pass my bill, you are making a significant difference to the analyst's right to this information and to the beginning of the strategic understanding of where we are.

So with that, I will now sit down and respond to your questions. But I leave you with an underscoring of what was said earlier — we have to think strategically in this whole area, and that means those of us that are proud of the fact that we think strategically about cyber terrorism have got to recognize that we can be stovepiped as well. And there are a whole — there's a whole new paradigm out there that we have to address and think through.

Thank you very much for your kind attention.

(Applause.)