THE BROOKINGS INSTITUTION

THE CYBERSECURITY AGENDA:
POLICY OPTIONS AND THE PATH FORWARD

Washington, D.C.
Wednesday, October 26, 2011

PARTICIPANTS:

Welcoming Remarks:

DARRELL WEST
Vice President and Director, Governance Studies
Director, Center for Technology Innovation
The Brookings Institution

Featured Speaker:

REPRESENTATIVE JAMES R. LANGEVIN (D-RI)
Co-Founder and Co-Chairman of the House
Cybersecurity Caucus
U.S. House of Representatives

Panelists:

ALLAN FRIEDMAN
Fellow, Governance Studies
Research Director, Center for Technology Innovation
The Brookings Institution

JAAK AAVIKSOO
Minister of Education and Research
Former Minister of Defense
Government of Estonia

JAMES B. LONGLEY
CEO, Diritech, LLC
Former Representative U.S. Congress (R-ME)

MICHAEL R. NELSON
Research Associate, CSC Learning Edge Forum
Adjunct Professor, Internet Studies
Georgetown University

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. I'm Darrell West, vice president of governance studies and director for the Center for Technology Innovation at Brookings, and I'd like to welcome you to this forum on cybersecurity policy options.

Many of you may know October is National Cybersecurity Awareness Month, and cybersecurity has emerged as one of the top policy priorities, both for Congress and the White House. Three weeks ago, House republicans released their cybersecurity plan and it relies on voluntary incentives to get businesses to protect their information systems. Republicans also say they're not planning on funding any new cybersecurity initiatives unless the costs are offset elsewhere in the federal budget.

I think everybody understand the importance of critical infrastructure in terms of our power grid, water treatment facilities, nuclear power, and chemical plants. All these are, of course, of vital importance to our overall economy. The GOP plan argues that Congress should consider limited regulation of particular critical infrastructures in order to protect our cybersecurity.

To help us understand the legislative situation, we are pleased to welcome one of the leading voices in Congress, Representative James Langevin. He's the co-founder and co-chairman of the House Cybersecurity Caucus. He was elected to the House from the second district in Rhode Island in 2000. He serves on the House Armed Services Committee, and is the ranking member of the Emerging Threats and Capabilities Subcommittee. He's also serving in his third term on the House Permanent Select Committee on Intelligence.

In each of these positions he has been a strong believer in national defense and the importance of effective intelligence gathering. I have known Congressman Langevin for nearly two decades, dating back to my time at Brown

University. And it's been wonderful to see him rise from state representative to Secretary of State, and now a leading member of Congress. He's been a terrific leader on a wide variety of issues, from cybersecurity to government reform and stem cell research.

So, it is my great pleasure to welcome Congressman Langevin to the Brookings Institution. (Applause)

MR. LANGEVIN: Well, thank you all very much for the warm welcome. Darrell, thank you for the introduction and the opportunity to be here with you at Brookings. It's great to see you once again through our collaboration and interaction. Darrell and I got to know each other, as he mentioned, when he was at Brown University, and for his capacity I served in government and it's great to reconnect with him at Brookings. So, wonderful to be with you again, Darrell.

Before I begin my prepared remarks I want to thank you all for your interest in cybersecurity. This is something I have been spending quite a bit of time on for important and a variety of reasons. But it's one of the most significant challenges that are facing our country today, and I know will take up more and more of the focus of the Congress -- at least I hope it will -- while we get more and more serious about how to fix the challenges and the problems that we face in cyberspace. Because this really does affect all of us, whether we realize it or not, and there are many people that are still struggling to get their arms around this and I don't think have quite taken it serious enough, unfortunately, or we probably would have fixed the problems by now. But your interest is important, and it's certainly appreciated.

And before I begin, I'm kind of a tech guy, as you can see. I'm riding around with these great iBOT wheelchairs. And no, it is not intense concentration that's keeping me balanced, by the way, so. (Laughter)

Well let me again -- I want to thank the Brookings Institution for inviting me to speak with you today on the safety and security of our critical networks, a topic that I believe needs greater attention and scrutiny by people both inside and outside of our national security sectors.

I have a feeling that a lot of -- I have a lot of company in the room here today when I admit that I've always had the reputation of being a technology nerd. So, I was more than thrilled back in 2007 when I was selected to chair the Homeland Security Subcommittee with jurisdiction over cyber programs.

The field of cybersecurity was a bit new to me at the time, but certainly was right up my alley, and I really did jump in to the issue with great passion. Now four years later, the news right now of course is awash with stories of digital harassment, of major Fortune 500 companies with effective espionage against our defense establishment, and even the potential horrors that a Stuxnet-like attack could wreak upon our pervasively networked critical infrastructure. But despite all this press and the growing awareness that we're facing a serious and urgent problem, we the geeks have to say, have so far failed.

I believe that we should examine some disturbing facts. Now a few short months after major intrusions that put customer's personal and financial information in the hands of criminals, both Sony's and Citi's stock prices barely reflect anything amiss, and the reason for this is more than just good PR. It's because despite all of our efforts, the market still doesn't appreciate how much good cybersecurity is worth.

Now there's a general belief among those who follow the topic that the importance of cyberspace to our national security and economic competitiveness is impossible to overstate, and I agree. We know that beyond the large losses of private data that make the news, the major driver of our economy, our intellectual property is being siphoned off on a daily basis for economic and military advantage by our competitors.

In the defense sector, it's easy to see how losing the plans for new weapons systems can be damaging to business, not only to our national security. However, in the rest of the private sector, which runs the majority of our economy and houses the majority of our creative entrepreneurial spirit, many boardrooms aren't convinced that an investment in strong cybersecurity is more cost-effective than a minor public embarrassment.

Board rooms need numbers and market information. While the market exists, clearly the information on the potential damage that this intellectual property theft to our national competitive leadership in cyberspace is still lacking. A 2010 study found that the average cost of a data breech for a business to be about $7.2, a manageable figure, I suppose you'd say, for a large Fortune 500 company and one that some might simply consider the cost of doing business. But the increasing value of intellectual property makes each of those losses minimal in comparison to the potential long-term damage to America's ability to remain the world leader in innovation.

As my friend Jim Lewis, who I know is in the audience here today, noted earlier this year, "The U.S. spent approximately $368 billion on research and development last year. But the cyber espionage lets others get those results for free." Now to make matters worse, many of these intrusions are possible due to common coding errors or lax corporate attitudes towards security.

Currently, the SEC requires companies to report any material network breech, including the loss of sensitive corporate information that could affect their marketplace earnings or share price. But because this definition is so vague, most of the breeches are never even reported.

And I have to say that I applaud the SEC for recently moving to tighten the rules that -- and I was pleased to see Senator Rockefeller's leadership in highlighting this issue, but there's another side to this information puzzle. One of the key recommendations by the CSI's Commission on Cybersecurity for the 44th Presidency, which I was proud to co-chair, was to reinvent the public-private partnership in cybersecurity. And I think this is going to be more and more important as we go forward. Over-classification, obtuse understandings, or liability -- and frankly, the slow government response -- have plagued America's ability to protect its private sector while fully enjoying the benefits of being home to the top cyber innovators in the world. Now the silent cyber crisis has grown to the point, I believe, where it can no longer be ignored, and we still have a long way to go to respond effectively.

Information sharing efforts by our defense industrial base have spawned new calls to reexamine the benefits of classification versus sharing. Now, we have a classification system that is based on potential damage to national security, but in cybersecurity, oftentimes this reactionary thinking is backwards. Certainly we have to continue to protect sensitive details about how we gather information, protecting sources and methods, how much we know, and where we're most vulnerable. But because the adversaries that we're facing in cyberspace are far more powerful than most civilian defenses, it's often the case that the more people who are secure from a virus or attack vector, the safer that we all are.

Now this preventative strategy can seem contrary to normal security mindset and is one reason why the Department of Homeland Security is a critical partner along with the NSA in reshaping our public-private partnership. Now we in Congress clearly have a role to play. There are legal and liability hurdles to greater information sharing that range from fears of acting as an agent of the government to privacy concerns about (inaudible). What's clear, however, is that the cyber threat information in government hands needs a clearer pipeline, or even network, to enable it to be shared with the private sector. While some of this information may need to remain classified, much of it can and should be shared for the greater good of our country.

Now another area of focus of the CSI's Commission was critical infrastructure. In 2007, my Subcommittee on the Homeland Security Committee began investigating an evolving threat to our critical infrastructure, the threat through cyberspace. Now it became clear to the committee that many in our utility sector didn't fully appreciate the vulnerabilities that they had exposed themselves to by linking their industrial control systems to their corporate IT networks. They didn't understand it then and I don't think they clearly understand it now, quite frankly.

As Stuxnet has shown the world, a serious attack through cyberspace is all too real a possibility. Yet many companies still have not confronted the risk, focusing on reliability over security and profit over protection.

Now the threat of a cyber war against our critical infrastructure may seem far off, but we're already beginning to see the interest among the hacking community in the massive and often shocking vulnerabilities and lax mind set that plague our power, water, transportation, and other utilities. Now it used to take a sophisticated attacker to pull off a distributed denial in service attack. Now, all you need is an Internet connection and tools such as the low-orbit IN cannon, and an angry mob.

My gut tells me that we're going to see a similar progression against our critical infrastructure as time goes forward. Now I believe that it's time for a new take on the public-private partnership, with government taking the lead in issuing standards and guidance for the protection of critical utilities and infrastructure.

Now, I've worked hard to bring this model to the federal level and cybersecurity to the electric grid, but it applies all across other sectors as well. Now I've introduced a bill earlier this year that echoed the White House model for establishing framework to various critical infrastructures, guided by the best practices developed across industries. I've also been interested in the potential creation of a dot-critical infrastructure-type realm, and there are others that are starting to pay closer attention to this in talking about it -- just recently, a key member on cyber from the FBI.

This idea could range from simply a different set of security rules and expectations when operating on a highly critical network, such as those attached to the SCADA systems of nuclear power plants, all the way to a new domain built on the goal of security built in from the outset.

Now, many of my colleagues and many in industry have noted the challenges, of course, in creating a new regime for protecting critical systems in cyberspace, but I believe that the urgency of this effort demands that we take some kind of action. Now the status quo of security through anonymity is clearly gone. Those who would gain political, economic, or military advantage through damage or disruption to critical infrastructure and critical systems are already well aware of the technical vulnerabilities. If we cannot convince policymakers and the private sector that security must be a priority, then we are all going to suffer the consequences.

Now, I was glad to see the House republicans recently offer policy recommendations on cybersecurity that matched the efforts that I've been pursuing with my colleagues in the Senate and the White House. And I believe a balanced approach of incentives and regulation -- but certain sectors haven't yet taken the security serious enough and need more federal oversight in this area.

I'm encouraged by the republican's task force findings, and I commend Mac Thornberry who led the task force for his work, and I'm certainly hopeful that this will be an area where we can see continued bipartisan efforts to move legislation through the Congress by the end of this year. However, we as policymakers must remain actively engaged and continue to educate our colleagues and the public. It's easy to look at a breach of WikiLeaks, or to a lesser extent RSA, and understand how it can threaten our security. But quantifying the impact of the economic damage done to our economy from continual daily fraud and espionage is much more difficult an equation to comprehend.

Now some say it's going to take a cyber-9/11 or digital Pearl Harbor that inflicts severe damage on our power grid, water supply, or financial system to finally convince the public and the markets that cybersecurity is a worthwhile investment. Now I've been fighting to make sure that it does not take an emergency, but I do fear that we're running out of time.

Automated tools are lowering the bar for cyber mischief, while the advanced actors are getting more and more creative every day. And I have to say that we only have to look as far as the new fascination in the hacktivist realm with the PLCs and SCADA systems that control our critical infrastructure, or the recent revelations of intrusions among the energy sector, to guess the targets of future attacks.

Let's move with all haste to ensure that we're ready for the coming storm. Thank you very much, and I look forward to taking some questions. (Applause)

MR. WEST: Part of my personal negotiations with the Congressman was he had to lower himself so he wouldn't tower so overwhelming over me in the Q and A. That would be too much of an advantage for you.

First of all, I want to thank you for coming here. I appreciate your thoughtful remarks on cybersecurity and laying out some specific ideas.

I just have a few questions, and then we'll open the floor to questions from the audience as well. You mentioned the value of information sharing and kind of the lack of reporting of many companies. You know, we have cyber incidents, we have cyber attacks, but often customers don't find out about it and other people don't find out about it. Should there be a mandatory reporting of significant cyber incidents? And what form should those reporting requirements take?

MR. LANGEVIN: Sure. Well as I said, some reporting is required now but it's not specific enough. The SEC is bringing more clarity to that, just recently. But I believe that there should be mandatory reporting.

Now in some ways I think it would be most effective if we had an information sharing regime between the Department Homeland Security and companies, even at the ISP level so that when companies are attacked, we see the attacks coming in to the -- they actually share the information with others so that they themselves can be protected. It's not about trying to embarrass any companies or punish companies that are hacked; it's about trying to obviously contain the damage as much as possible by sharing the information with others so that further damage isn't done.

MR. WEST: Okay. And you mention the fact that House republicans came out with their cybersecurity plan a few weeks ago and that they rely on voluntary incentives to encourage private companies to improve cybersecurity. In your remarks, you talked about the need for a balanced approach between some incentives on the one hand, but also some government regulation. So where do we draw the line? Like, what would a balanced approach look like?

MR. LANGEVIN: Sure. Well, I think that we may look at things like tax credits and incentives for employing better cybersecurity. I know there are some that have talked about some liability protection, and I'm open to considering that but it would have to be in exchange, if you will, for adopting tough standards. For example, tough NYS standards. We don't want to over-prescribe. That can be the danger here, too. And I would say that it would be wrong for us to say that, you know, you have to have X security system on your networks because that provides basically a very false sense of security that you've taken care of the problem.

Cybersecurity is a moving target, it's an evolving threat. We are never going to be able to get to the point where we are 100 percent successful. What we need to do, basically, is close the window of vulnerability. And I believe that we need to adopt -- companies should adopt robust standards, and again perhaps you look at NYS standards for the -- looking at, say, the gold standard of what could be employed to have the best cybersecurity on your systems. But again, we can get to look at that in terms of how we -- whether it's tax credits, whether there are other things that companies need to employ that type of security.

But in some ways that's only going to get us so far, and company's good intentions are only going to get us so far. I know companies want to be secure in cyberspace, they want to protect obviously their ability to deliver a product, but again, good intentions only get us so far.

So in the area, for example, where the most damage can be done I use the electric grid as an example. Clearly here's an area where good intentions haven't gotten us to where we need to be, and I think we need to have some type of a regulation. You know, clearly the -- I'll use the nuclear industry as an example. The NRC has robust authorities to direct and require vulnerabilities be closed. We don't have that same type of a system in the electric grid, in the electric industry. You have FERC basically overseeing the North American Reliability Energy Corporation, and that is basically a self-regulating body. So they have -- they want to make rules changes. They propose rules changes, FERC can either approve or reject those changes but they can't require that a vulnerability be closed.

I believe that FERC needs that authority. We've tried to pass legislation that would give FERC that authority. We haven't been successful in getting that through yet, and in some ways it's been a bipartisan effort. But that's just an example of what I mean by combination of incentives and regulation.

MR. WEST: Okay. You mentioned the possibility of tax credits for companies. And of course, the 800-pound gorilla in Washington D.C. right now is the Super-committee of the pending deficit reduction, and just how that whole process is going to play out. So I'm just curious what you're hearing on that front? And then the possible impact of various deficit reduction cuts on cybersecurity?

MR. LANGEVIN: Yeah. Well this is an area we're going to have to make sure we're getting the best bang for our buck, that we are spending our dollars wisely, that we're not over-duplicating our efforts. And it's going to take obviously a more comprehensive approach of how best to do cybersecurity. And again, when I say tax credits and incentives, obviously that means there's a cost to that. We have to make sure we're engaging the right tradeoffs. But the cost of inaction, I think, can be greater than acting. Something happens on the scale of an attack on critical infrastructure, we'll all be saying, why didn't we move more quickly? Why didn't we invest more wisely in protecting that critical infrastructure?

Another thing we couldn't get to, by the way, is the insurance industry playing a role. And perhaps there's -- if the incentive is built in so that companies get a reduction in insurance costs if they employ the best cybersecurity. But again, it's going to take looking at -- and spending our dollars more wisely, make sure we're not duplicating our efforts, and much more targeted and focused approach on cyber than we've engaged in the past.

That, by the way, is why I think we need a cybersecurity director in the White House, not just a coordinator. I give President Obama high marks for the role that he's played in protecting our cyber networks. As you know, Melissa Hathaway did the

60-day review when President Obama first came in, and as a result President Obama was the first major world leader to make that kind of speech on cyber and how important our cyber networks are, that we'll use all assets of national power to protect it.

He went on to also appoint Howard Schmidt as the cybersecurity coordinator with the White House, and Howard has done an excellent job with the limited authority that he has to bring people together to better protect us in cyberspace. But unfortunately, he does not have the authority that he needs, I believe, to really direct changes being made. Much of the work is in the hands of the Department of Homeland Security right now. Of course, the agency itself is struggling to stand itself up; it's still a young agency. But even they don't have the authority to reach across departments and agencies and direct that vulnerabilities be closed. And in that -- someone, some entity is going to have both policy and budgetary authority to direct other agencies -- whose primary mission is not necessarily cybersecurity -- to make sure that they are acting with all speed and they're doing what they're expected to do, to protect their networks in cyberspace.

MR. WEST: Okay. One last question, then we'll open the floor to comments from the audience. You mentioned the issue of insurance. And of course, in other areas of life we do rely on the insurance industry to guard against risk. You know, fire, theft, and otherwise. So I'm just curious, what potential do you see for a cybersecurity insurance approach to help deal with some of the threats in this area and to help guard against risk?

MR. LANGEVIN: Yeah, so obviously what I touched on earlier is that if the insurance industry -- we can convince them to be partners in this effort, and they'll look at a company and they see the vulnerabilities to a company of inaction. If they can provide some type of an incentive that if a company does X, Y, and Z, maybe adopt NYS standards, then clearly that reduces a company's exposure to a cyber attack. There should be a value there in the insurance field, and being able to hopefully reduce the type of rates that they would have to insure the company.

MR. WEST: Okay. Why don't we open the floor to questions and comments from the audience? If you can raise your hand -- there's a hand up in the back. We have some people with microphones. So if you can pass it over there. And if you can kind of stand up, and if you can give us your name and your organizational affiliation. And we also ask if you'd keep your questions, brief, just so we can get to as many people as possible.

MR. HALL: Okay, brief. Dave Hall, Montgomery College and Cyberwatch. The concern that we have is that we're in the business of training cybersecurity technicians. We've been doing this for about 10 years under NSF grant. And we find that especially in this area where a lot of corporations deal with the U.S. government, they have to go by OEM categories for work technicians, and that sort of thing.

However, OEM recently revised some of its job categories, and there's almost nothing dealing with cybersecurity in those OEM regulations. Some private companies like SANS_ and Cisco Networking Academy have come up with a number of categories for cybersecurity technicians, but OEM seems completely oblivious to this. So, is your group trying to do anything to fix that?

Thank you.

MR. LANGEVIN: Yeah, I don't think we've taken a look at anything that OEM is doing. You know, I'll have to take that for the record and look into that further, because I'm not certain as to what changes they're proposing.

MR. WEST: Okay, we have a question here up front. There's a microphone coming up for you.

MS. MARTINEZ: Hi, I'm Jennifer Martinez from Politico. You mentioned having a dot critical infrastructure realm, and I wanted to see if you could explain that. What it would look like and, you know, how it would possibly function.

MR. LANGEVIN: Sure. You know, very similar to how we have dot mil or dot gov or dot com. I've been suggesting that the idea of a dot critical infrastructure. So that it's much more of a closed network.

There are only certain people that really need to be on or have access to, for example, the electric grid. And right now it's basically in the dot com realm. It very -- you know, free and open access there. But the question is why do certain individuals really need to be on -- I think it should be limited to only certain individuals that need to be on or have access to certain aspects of critical infrastructure.

So I guess what I'm calling for is one of two things: either reduction in anonymity with getting onto critical infrastructure so that there's a very clear purpose on individuals who are easily identifiable who go on to -- or have access to -- dot critical infrastructure; or, we could create a separate, more closed network and the same -- the way that we protect the dot mil network, by having their own domain that we'd also have a dot critical infrastructure.

So that's difficult to do. I don't want to minimize the challenges. It's not as easy as just saying, you know, okay. We're going to give the new address to areas of critical infrastructure. We require a lot of -- both hardware and software, and would involve great expense and, you know, just because we do it here in the United States doesn't mean that other countries are going to follow suit, which is in and of itself a challenge. Obviously in this global environment, of which we find ourselves, and a network world -- it would take international cooperation in a lot of ways to move in that direction. I mean, you can just think, for example, we get some of our electric supply comes from outside the United States. Gas or oil supplies will come from Canada, for example. Those create challenges when you're talking about cross-border interaction. So it's not just as easy as saying we're going to have a dot critical infrastructure for all critical U.S. infrastructure.

But at the very least, I think we should look at moving to much more of a transparent system, meaning reduction in terms of anonymity for those that go on to critical infrastructure networks.

MR. WEST: Question over here?

MR. HALLORAN: Hi, Connor Halloran from Johns Hopkins. You provide a very good top-down approach to cybersecurity, getting institutions to harden their programs and defense. But what about the bottom up? The human factor where people pick weak passwords or allow their personal computers to be accessed, which provides access to sensitive networks and data?

MR. LANGEVIN: Right. Well it goes back to the old saying, you know, you're only as strong as your weakest link. And all of us have a responsibility in this area to make sure that we are putting firewalls on our computers, that we have good computer hygiene, and making sure that we're employing the computer patches on all of our networks. Being careful when you have a, you know, your laptop, that you're -- you know, if an entire network is secure but, you know, your computer is infected and you bring your laptop in and you plug that in to your network at the office, then you know, that exposes the whole network to various vulnerabilities. So individuals have a role to play. There's definitely a public education element to this that, you know -- it's like the whole Smokey the Bear thing. Oh, you can prevent forest fires. Well, this is -- individuals have a role to play, making sure that their own computers are secure.

And there is some that will argue and that we need to look at -- the ISPs or paying closer attention to monitoring how secure an individual's computer is. For example, the idea of not intrusion but if there's a virus detected by the ISPs on an individual's network, can the ISP then notify the individual that, you know, your computer is infected? You know, would you like us to fix it? Will you authorize us to fix that vulnerability? I think those types of partnerships. But again, it's going to hopefully be more of a voluntary realm. And again, at the ISP level. Not government dealing, of course.

MR. WEST: I think the Congressman is exactly right on this about the need for public education, and especially on password security. Because there has been research on consumer behavior, and some of the crazy passwords that people come up with. It's like, one of the favorite passwords is the word "password". You know, that's real original. Or, 123456, because you need a 6-character password. So we just need to do things to help protect ourselves here.

Other questions? In the corner over there.

MR. WILSON: Hi, I'm Cameron Wilson with ACM. A quick question around standards. You mentioned it as something you'd like to see from a policy framework. I just wondered if you could articulate a little more of your vision of what that looks like. And in particular, how -- are these high-level standards or more technical standards? And how you address the issue of a really rapidly-evolving technology with a standards base, and can the federal government keep up with that?

MR. LANGEVIN: Well, you know, clearly if -- as critical infrastructure has become more and more networked, and you get SCADA systems by way -- in example, if there is something on there that allows hackers to easily penetrate SCADA systems and the company's aren't moving aggressively to close those vulnerabilities, then clearly there's a standard that needs to be set that will require that vulnerability to be closed. So, you know, it's -- again, I don't want to be overly prescriptive in identifying standards. And I think we have to recognize that this is -- as a moving target, moving threat, and it has to be more of a nimble, agile system that's going to allow vulnerabilities to be closed in this area.

But you know, I suppose you can think of any list of things that could or should be done to make sure that, you know, you're not allowing people to, you know -- even on the inside -- to connect to the system if their computers aren't secure. And anything that's going to close the vulnerability, I would say, would be a standard that we should move toward.

But I don't want to be overly prescriptive.

MR. WEST: In the very back, standing up, is a question.

MR. SAUL: Thank you for being here today, Congressman. Johnson Saul with Brownstein Hyatt.

I heard Mac Thornberry speak probably two weeks ago now, and he said that the task force, everyone on it would take kind of a piecemeal approach to cybersecurity, breaking out the different recommendations into individual bills, and that the Senate was more likely to take a comprehensive approach. I just wanted to see if there was any cross-dialogue across the aisle or between the Senate and House on how these issues would be resolved, and kind of the political landscape and likelihood of these bills moving forward.

MR. LANGEVIN: So, I mean, I for one would like to see a comprehensive approach to cybersecurity. I'd like to see a major piece of legislation make it through the Congress this year. I don't know how realistic that is.

And so, you know, to that point we're waiting to see what the Senate will do. And I have a good partner on the other side, my colleague Senator Sheldon

Whitehouse from Rhode Island, who has taken a lead role on cybersecurity on the Senate side. And he actually chairs a subcommittee on the Duty-Sharing Committee that has responsibility and jurisdiction over cyber. And there's -- you may have seen press reports recently that members of the White House have met with people in a bipartisan group of Senators. And there's been positive information coming out that they're pressing hard for a comprehensive cyber bill this year. I hope they can.

In the meantime, on the House side, as you pointed out and as we've seen in the press, the republicans prefer more of a piecemeal approach. At this point, I mean, I'll take what we can get. My preference is more of a comprehensive approach.

But just by way of example, I've introduced my own bill this year. In fact, we actually got the bill through the Executive Cyberspace Authorities Act. It would have given more authority and made the White House position -- a director position, Senate-confirmed, given responsibility to the Department of Homeland Security to regulate in the area of the dot com realm. Basically, prescribing more security on its own, or delegating the authority to a regulatory body, if one already existed. That made it through the -- it passed the House in the last Congress as part of the National Defense Authorization Bill that made it through the Armed Services Committee.

Under this Congress, when I proposed it again this year it lost on a -- even though it had some bipartisan support, it fell a few votes short. But it's always where -- you know, the important thing is to get something done this year, whether it's an individual bill that closes vulnerability with respect to critical infrastructure, or would get a more comprehensive approach. We'll have to see what we can get this year.

MR. WEST: If there is a piecemeal approach, what would be the most important part of this to enact? Or the second most important thing to enact?

MR. LANGEVIN: Well, I just outlined what I saw as the most important.

I took what I said as, you know, what is the most important thing to get done, even though I'd like a comprehensive bill. I looked at the Executive Cyberspace Authorities Act which would, again, make the White House position a director's position, Senate-confirmed. And that giving more authority to the Department of Homeland Security, along with the cyber coordinator, to work with critical infrastructure and directing that vulnerabilities be closed. It's all through regulation.

Others would be -- also -- and there's the other thing. Information sharing; get the public-private partnership between critical infrastructure and the anti-government. Whether that's a third-party entity that's set up that would allow for information sharing -- and again, we don't want the -- the NSA obviously has robust tools. They've been working with the Pentagon; they've done an excellent job of working with better securing the dot mil network and the SIPA net, for example. But we don't want the NSA being involved, you know, in the dot com realm. But I think that they have an important role to play with Homeland Security that is the liaison, if you will, to the private sector working with the dot com realm.

MR. WEST: Right here. There's a microphone right there.

MR. BRASH: Oh, there you go. Mark Brash with COC. On the question of information sharing, you said that you suggested that it be mandatory that companies be required to report incidents, vulnerabilities, and the like to either a government agency or some inter-departmental agency. Would you also make it mandatory for the Department of Defense, the CIA, the intelligence communities to companies like Wal-Mart when the CIA's had a breech?

MR. LANGEVIN: Well, let's put it this way. I want there to be the cross-collaboration right now. And by the way, the government agencies -- government department's agencies already through FISMA have to do due reporting, as it is right now. And that's only been minimally effective. There's got to be updates to the FISMA law, the Federal Information Security Act. That Act is, I believe, more than 10 years old and needs, clearly, to be updated. I've tried to do that, and that was actually part of the bill that I was able to get through to the Defense Authorization Bill.

But clearly, I think departments and agencies have to do more and do a better job of reporting their own vulnerabilities and data breeches. And we've been hacked, to a significant degree, and we've lost terabytes of data to hackers, mainly -- probably in the nation-state realm, that have come in and siphoned off significant amounts of data. You know, there's the old saying that on the seventh -- have it said that if somebody was backing up to the Pentagon with trucks and carting out filing cabinets full of data, you know, it'd be tantamount to an act of war. But because it's happening in the digital realm, there isn't that sense of urgency.

So the answer is, yes. I think there should be more information sharing. There should be more reporting of when government departments and agencies are attacked and information is stolen. And it also has to happen, obviously, in the private sector.

By the way -- and I'll just end with this -- the idea of the DIB pilot, the Defense Industrial Base pilot, is a good example of what I mean on that information sharing level. They were -- the NSA is working with the -- basically the Internet security providers to basically share information back and forth so that if we see attack signatures, that that information is shared.

MR. WEST: Other questions? In the very back, there's a hand up. Yes.

SPEAKER: Thank you. I'm Jeong_ from Radio Free Asia. Let me ask you one thing regarding the cyber attack from the other countries, especially North Korea. Last year, North Korea did a cyber attack to the U.S. website -- government website. So, I'd like to ask you are you concerned about cyber attack from North Korea or other countries?

And I think there is no tool to control the cyber attacks. So I think this is a problem to North Korea to develop its cyber attack skills. So, can you give me some comment on this?

MR. WEST: Okay, can you repeat that question one more time? I'm sorry.

SPEAKER: Okay. Cyber attacks from North Korea. North Korea did a cyber attack last year onto the U.S. website with a (inaudible), something like that. Are you concerned about the cyber attack from other countries? And still, there is no tool to control and make it stop, the cyber attack from other countries. There's a problem. So, can you give me some comment?

MR. LANGEVIN: Sure. Well, I'll talk about this in general terms. And that, you know, many of the significant cyber attacks that we've seen have come from outside the United States and very likely, at the nation-state level. And the tools that nation states have are growing in sophistication and seriousness, and they are daily attacks on both -- and I don't want to overuse the word "attack", because you want to kind of develop -- segregate into three categories. There's intrusion, there's disruption, and then the more serious side is attack.

And so far right now, we've seen more of the cyber intrusion and disruptions, and it's been more on the criminal side or the espionage side, which have been the greater problems. We haven't yet seen a significant attack yet that would -- that has, for example, shut down in the area of our nation's electric grid. But it's coming if we don’t take this more seriously. I believe that it's very likely in the near future that whether it's an individual or a terrorist group that wants to cause significant damage to the United

States, that they would engage in attacks not just the stealing of information, which is obviously serious enough in itself. But I'm trying to raise the awareness and ring the alarm bells so that we act before anything significant is done in terms of damage. But clearly there are, you know, nation-states have great interest in developing these tools and capabilities that either have allowed it to go after our research and development work that has already been done by U.S. companies and steals our intellectual property -- and that's doing great damage both to our economic competitiveness, but also does great damage, I think, long-term to our national security.

MR. WEST: And it seems like as the government has improved its cybersecurity, what some of these foreign attacks are doing is now targeting, you know, defense industry companies, think tanks, and other people who interact with government. And so it's almost increasing the vulnerability elsewhere in the system.

MR. LANGEVIN: That's exactly right. And that's the whole premise behind the DIB pilot, was how can the government work more closely with our defense contractors to secure their networks and provide them with robust information-sharing, going back and forth? And even with that kind of collaboration, it allows us broader, in a sense, transparency of the types of attacks and the sophistication of attacks that, again, can be shared with the government and other defense contractors so that everyone is more secure.

MR. WEST: I think we have time for one or two more questions. One question I will pose, kind of a follow-up on the North Korea question. Is there any role for the U.S. military in terms of playing offense as opposed to just playing defense and responding as attacks hit us?

MR. LANGEVIN: Well, let me put it another way. I'm going to kind of sidestep your question a little bit and say I think this is a role in which the international community has to be more engaged and working with our allies, partners around the world, more that we work together. The more we share information across borders, the more secure that we will be. And there's going to be -- I know that's going to be an ongoing discussion and interaction as we go forward.

But you know, clearly the one thing that we need to be -- the further out we can be from our own systems and our own borders, if you will, you can see things coming before they actually are executed and put into effect, if you will, the more secure we will be. But obviously, you know, the government has robust capabilities in these areas and we want to use them most effectively to protect our own networks.

MR. WEST: Okay. I want to thank you for coming to Brookings and sharing your thoughts. Thank you very much.

MR. LANGEVIN: Thank you. (Applause) (Pause)

MR. FRIEDMAN: So, I'd like to thank the Congressman and his staff for making time for us this morning. And to follow up on some of the challenges and actually addressing the cybersecurity threats we face with a developing policy agenda, we have an excellent panel this morning that not only has approached technology policy governance from a wide-range of perspectives, but each of these panelists has done so for multiple careers themselves.

We're going to begin with Jaak Aaviksoo, who is the Minister of Education Research for the Republic of Estonia. Before that, he was the Defense Minister of Estonia. Prior to that, the Minister of Culture and the Minister of Education before that. But even before he got involved in government, he was an academic in his own right as a researcher in optics and physics.

As Minister of Education he was deeply involved in promoting technology inside the Estonian educational system, and as Minister of Defense he was involved in understanding defensive cyber operations for the Estonian military, and creating the establishment of NATO's Cooperative Cyber defense Center in Estonia.

We also have the Honorable James Longley, who before being a Congressman was a lawyer. He was a Marine who played a large role in understanding the shape that information plays in military humanitarian operations. And following his service in the House, he has been actively involved in a wide range of technology policy issues, including he was a senior technical analyst for the U.S. Army's Space and Missile Defense Technical Center. He was a senior advisor to the last few directors for the Missile Defense Agency, and he is now the manager of Dirtech, LLC, a technical consulting firm.

And finally, we have Mike Nelson, who is a research associate for the Leading Edge Forum, a think-tank inside CSC. And I believe he's still adjunct faculty at Georgetown. Prior to joining CSC, he was visiting faculty at Georgetown and a pioneer in shaping how research and teaching have been done inside the field of Internet studies. Prior to joining the faculty at Georgetown he was the director of Internet technology and strategy at IBM, but before that he was involved in technology policy in the government, both at the FCC as the director of technology policy and he began his governance service as special assistant for information technology in the White House, where he worked with Vice President Al Gore. And all of that came after he was a geophysicist at MIT. (Laughter)

So, we have an incredibly experienced panel here who can really bring a lot of different perspectives. And I'd like to start off -- we've just heard the American political perspective -- getting some insights from the outside, starting off with Jaak. Can you share some of the lessons that you've learned as you've developed coherent policy inside Estonia? And maybe a comment on how the Congressman offered his insights.

MR. AAVIKSOO: Well, thank you.

I'd like to start from the events that took place in Estonia in April 2007. As a former academic, after elections I ended up in the post of the Ministry of Defense. And on the third week in office after a decision to relocate a Soviet war memorial, which was a controversial issue, in addition to street riots and protests we saw massive distributed denial of service towards Estonian banks, as well as online use and a number of other government services.

Taking into account that e-banking counts for more than 90 percent of all transactions and the service was disrupted for hours and several weeks in a row, and online views were not accessible, this clearly was perceived as an event of national security level. Not only in Estonia, but also outside. So I think that was a first event of its kind, and after that I've seen in several contexts the discussion of possible cyber wars and cyber attacks, cyber policies developed, and so on and so forth. So, cyber attacks and cybersecurity, cyber defense has been there since four years clearly on the front page, in a way.

What were the first lessons we learned from those attacks? First, internal or homeland security and national security in the case of cyber are intimately intertwined. It's very hard to separate those two. Equally important is that in Estonia's case and most probably in the case of future attacks, these are privately-owned institutions that are attacked. So, public-private partnership is strategically important. We have to build this trust and confidence into public-private relationships from the very beginning, from scratch, whenever we design something to secure our cyberspace.

Thirdly, these attacks will always be global or international in one way or the other. In the case of Estonia, we still don't have solid evidence of who was behind, although there is a saying that if somebody barks like a dog, bites like a dog, and looks like a dog it's most probably a dog. But I won't go further, because it's too sensitive.

The biggest number of computers involved in those attacks were not located, neither in Estonia nor in our big neighboring country. A big share of them were located in the United States, for instance. So, international dimension is always there.

Fourthly, for different reasons -- for conceptual but also, for I think, for real practical reasons -- our laws are not very effectively applicable in the case of cyber events. When we -- either it's a problem of assignment or responsibility, or any kind of question, I think people tend to mystify cyber, on one hand. And on the other hand, it is in a way virtual. I mean, all what happens is, you know, a fluctuating electrons, for a while, and then it's gone. So it is a problem, how to handle the cyber events altogether.

Some of that is in the mindset, we simply don't know. For instance, what is beyond reasonable evidence? I mean, very many people believe you can fake everything in virtual space. There is no solid evidence at all. At the same time, you can fake fingerprints and footprints, and you can fake everything. But there is an understanding what constitutes beyond reasonable doubt evidence in physical space.

But I mean, judges, prosecutors, lawyers, they disagree on very many occasions what constitutes beyond reasonable evidence in cyberspace. I think there is a lot of, I don't know, communication, dialogue needed, in addition to legislating into the area, in the case of this. But I personally, I don't think that we need a totally new kind of legislation in the case of cyber events. Including very sensitive questions like, what about Article 5 in the Washington Treaty? Or, how is one authorized to respond in physical space when attacked in cyberspace? I mean, questions of that kind are -- I don't think they are so different, so mystical.

I'm very much in favor of a pragmatic approach. If bad things happen, loss of human life and material damage, then it's not that important what were the means to carry out that offense. And as a conclusion thereof, appropriate, balanced response by kinetic force is a right thing to do.

There are certain sensitivities, but in principle we shouldn't exclude, otherwise we end up, I think, in lack of deterrence in real terms. So that is just one more thing.

And last but not least, it is -- and we just heard how important it is to cater for general awareness of cyber threats, cybersecurity, and cyber defenses from different perspectives. We have developed consumer protection in a number of cases. For instance, you can always read on a microwave that you can put your cat in that to dry him. But I mean, I have never read on a computer that -- a warning. This device can be dangerous to your health, property, and integrity, which actually is true. I mean, things like that -- so public education from the very early age, I think, because kids start using that device already at the age of two or three or four. So, school is too late already.

We haven't done definitely enough, we have to do more. And this has to be, I think, a balanced thing. On one hand, you have to build awareness of the potential threats. On the other hand, I think cyber is here to stay and to develop and we are interested as nations, as economies, and societies that we develop those technologies. But we have both built awareness concerning threats, but also trust and confidence by using that. So both industry as well as the government should do to increase that trust in those services delivered by these technological means.

Just one example and then I'll finish my introduction. We've been very enthusiastic in Estonia into all this ICT stuff. I mean, that's thanks to maybe our not most glorious past, but also thanks to our neighbors who are very technology-oriented, like Finland, Sweden, Northern Europe altogether. So, 10 years ago we started experimenting with e-elections, meaning you can cast your votes by Internet. Starting with local elections, we gradually built trust, starting with 2 percent of the electorate voting via Internet. Last parliamentary election there was 25 percent. And of course, there is criticism with being -- trying heavily to invest in security of this electoral system, but I've seen how gradually we've managed to build trust on one hand, but also in a balanced way criticizing and trying to solve all of the risks related to this very sensitive issue. Because I think if one fails in e-elections with the electorate fraud, I think that's a very, very bad thing and it threatens the democratic stability of a country. So, I think this is a very, very sensitive issue.

But we've seen progress, and I am personally confident that this is here to stay, that we see more and more countries joining in most probably in the next 5 to 10 years, there will be quite a number. So, thank you for your attention. That is what I wanted to say.

MR. FRIEDMAN: Well, thank you very much, Jaak. And we'll have to have you back when we have a discussion about Internet voting.

So Jim, I'd like to turn to you. You've spent a lot of time dealing with many areas of how the country has adapted to higher tech in the defense area, the importance of innovation but also management of that innovation. Can you talk a little about that?

MR. LONGLEY: Let me try to. And let me just qualify what I'm going to be saying by saying I'm focusing more on technology as a tool and I think that we tend to forget that it's not about the tool, it's how people use it.

And there was an interesting article in the *Post* about two weeks ago. South African cave yields paint from dawn of humanity. Now you may wonder what something that happened 100,000 years ago had to do, but it said that in a cave overlooking the Indian Ocean, there was a man or woman who crushed a soft, rusty red rock, mixed it inside a shell with charcoal and animal marrow, and daubed it on something. Before the person left, he or she stacked the shell and grindstones in a neat little pile, where they lay undisturbed for 100,000 years.

The archeologist who discovered this said they probably understood basic chemistry, traces of paint on the tools showed that the cave-dwellers mixed ochre, red or yellow minerals that contain metal oxides, with bone marrow, charcoal, flecks of quartz, and a liquid, probably water. It took paint experts at the Louvre in Paris to perform the analysis.

And the question I want to pose is I mean, I think we all tend to assume that we're so much smarter today than people have been historically. And I would submit that somebody living in these austere conditions 100,000 years ago displayed a considerable amount of ingenuity. And the human species has a remarkable ability to adapt, particularly to the use of technology and tools. And so it's not necessarily about the tools, it's how we use them.

Now, there's a great book -- and I've got a couple recommendations, because I frankly don't think we fully understand the depth of the problem. In fact, I'm not sure were close to understanding the depth of the problem. If you've gone to law school and taken basic tort law, you'll discover that the first half of the 19th century there's a whole string of exploding steam boiler cases where the law had to grapple with the consequences of the new steam technology that was literally wiping out some neighborhoods, based on how the technology was deployed. And again, another example I'm familiar with is the role of steam ships and the rules of navigation took 60 or 100 years to sort out.

And I hate to say this, but we don't have that amount of time with cyber. So, one of the books I want to recommend -- and it's still in print or at least in stock at

Amazon for about $5. It's by Tom Wheeler, *Mr. Lincoln's T-Mails*. And what the author does is highlights -- and I think it's a very useful case study -- the introduction of the telegraph and how it was used by the President as a means to manage the civil war. But he also focuses on how the telegraph may have contributed to the civil war because it was an unprecedented increase in the speed with which information went to the South following Lincoln's election. Then it was a strategic problem for the South, because they were more averse to technology than the North was. They're also more averse to railroads, and it tells the story of how the telegraph and the railroad came together.

And again, the point I want to make is, this was not pre-planned. In fact, if you ever have a chance to go out to First Manassas, there's a nice little placard on the wall about General Johnston who moves his troops, 10,000 troops, about 50 miles south using the railroad. And it points out this was the first strategic use of rail to move troops in North America. And having been an infantry officer, my perspective was a whole lot different than all the strategists who write about the strategic use of rail, because the general is standing there, he's got to move his troops 50 miles, do I want to walk? Or, do I want to figure out how to get on this train? And needless to say he made the right decision, but think of the hundreds of people who have made careers out of how that developed.

I want to wrap up some early points on the balance, if you will, between what I'll call the human factors and how we use technology and the legal construct within which our government operates. The Constitution is very clear. We the people do ordain and establish this Constitution for the United States of America. Our legal premise is that the people delegate to the government. We are not subjects. We retain individual rights, including the right of self-defense, and that can be interpreted broadly.

We're also a country that settled -- 80 percent if not more was settled by people who did not have the benefit of any established rules or benefits of civil society. They learned to improvise. The concepts of posse, by the way, and jury and militia are not unique to America. They go back 1,000 years in our Anglo-Saxon legal history. Those principles are going to, I think, become more operative than we appreciate.

There's another book that I think puts -- it just came out two weeks ago, I recommend it highly. It's *Worm* by Mark Bowden. Now, I'll summarize this very quickly. It covers -- it's a history, it reads like a novel, of Conficker, Alpha, Bravo, and Charlie. And it discusses how when -- and without getting into technical details -- the worm was able to enter through an un-patched hole that was the Alpha version. Microsoft immediately put out a patch, which was a red flag because 95 percent of the people on the Internet didn't understand that they needed to either use a patch or they were using a bootleg copy of Windows. So, the patch was a signal to those who create malware. It led to Conficker B. Conficker B was randomly generating 250 domain names a day, and this group of 6 or 10 individuals, volunteers, all unpaid were using personal credit cards -- they ran the clock ahead using personal credit cards to buy up domain names so that they could try to find the mother computer that would be sending the signals to the bot net that was being established.

The malware creators were actually watching what they were doing. And version Charlie came out, which now was pulsing 50,000 domain names a day. And not at SHA-2 encryption of 10-24 bit, but now jumping to 4,096 bit encryption using SHA-3 provisional, or the draft version of it, if you will. They were ahead of most of our civil society -- I won't try to comment on where elements of our government were.

They felt it was pretty much of a crisis. They had been trying to get the government involved, we're getting blown off. So the senior member, Rodney Joffe, shows up in Washington, contacts a friend at the Department of Commerce, briefs some of the staff at Commerce, turns their hair white, sets up a brief with another agency -- and my point here, I'm not trying to be critical of anybody. I'm only trying to make objective observations of factual situations. But the suggestion is that the agency responsible for monitoring the Net was 2 to 3 months behind what this group of 6 or 10 private sector volunteers were doing. And if you will, you know, where was the government?

And this was not a unique circumstance. If you know anybody who was involved with Aurora, it's a similar situation. And so the point I'm trying to make is, I'm not so sure the government is keeping up with the threat. I think we have a very serious problem in that respect, and I'll just quote one part of this, and then maybe wrap up and we can get to Mike.

But, the DHS reports documented in the aftermath of Conficker in an unprecedented act of coordination and collaboration the cybersecurity community, including Microsoft, I-CAN, registry operators, antivirus vendors, academic researchers all organized to block the infected computers from reaching the domains. Despite a few efforts, the effort was very successful. But then later in the report, it says one unnamed member of the cabal that was working this effort on a volunteer basis summed up the federal contribution during the actual conflict: zero involvement, zero activity, zero knowledge. And I would submit that the government has a real serious challenge on its hand. I look forward to talking more of what role I think the private sector needs to be, in terms of frankly helping the government.

MR. FRIEDMAN: Thank you, Jim. So, that sounds like an excellent segue to Mike Nelson, who spent a long time sort of promoting the use and deployment of technology inside the government, and also inside the private sector. Thoughts on that and perhaps how it touches on other aspects of technology policy?

MR. NELSON: I'm very glad to be here today. I think I'm here as the token skeptic and also the token futurist. (Laughter)

I have been working in technology policy for almost 25 years. You mentioned my work at the White House with Vice President Gore. I actually came to Washington in 1988, and I worked with Senator Gore. My very first assignment was working on the Earthquake Hazards Reduction Program. You might wonder why I bring that up. It's a great model for what we're facing today.

I got here, I had just gotten a PhD in geophysics and earthquakes, and they actually put me in charge of something I knew about. But I found very quickly it wasn't about the technology or the science, it was all about the politics.

At that time, there was this multi-agency program with FEMA, NIST -- the National Institute of Standards and Technology -- NSF, and the U.S. Geological Survey. And they were all trying to reduce the threat of earthquakes, but they were all trying to take different approaches. So, NSF was trying to fund research so we could better understand the threat. NIST was trying to help people build better, safer buildings, so to prevent damage. The U.S. Geological Survey was trying to assess the threat. And FEMA, which got the bulk of the money, was there to clean up the mess after the earthquake happened. And of course, they all thought their own piece of the puzzle was the most important.

I think you start to see why this is similar to what we're facing today. Some agencies think the most important thing to do is to punish the bad guys, go after them, throw them in jail. Other agencies are working on research, better cybersecurity solutions. Other agencies are trying to help companies and government agencies protect against them -- against threats.

I'm going to focus on that third part today which is, I believe, the most important because it's often the most cost-effective. If the damage isn't done because the systems are secure, we have a much better situation than if we're trying to chase the criminal after the database has been compromised or the intellectual property has been stolen.

The other problem, though, with this whole field besides the fact that many different agencies are working with different agendas and it's very hard to coordinate them, particularly on Capitol Hill where everybody has their own fiefdom -- the other problem is that everybody understands that there's a big threat here and a huge potential price tag, but they don't know what that price tag is. The do know what the price tag is for preparing for the problem. So, it's very much like the earthquake situation. People could figure out how much it cost to retrofit a building to make sure it doesn't fall down, but they had no idea when the earthquake would occur or if it would occur or where it would occur. So there was this asymmetry. You knew how much you had to spend now, but you didn't know what the benefit you were going to get would be in the future. And so, we have that dichotomy.

The other problem we have is that everybody wants to be involved in the decision making but nobody wants to be the person who puts their hands up and says I'm responsible for this whole mess. We saw that several times after major earthquakes in this country, where everybody who had been working on the problem was able to say we helped solve or prevent loss of life, but it wasn't our fault that people died. And so there's this, again, dichotomy there between who's responsible and who's involved. And so we have to find a better way to coordinate this process, and this is the biggest challenge the Hill will face as it tries to work through this legislation. Nobody wants to be the point person when the digital Pearl Harbor happens.

What I want to do today is go through a couple quick FAQs, frequently asked questions, about cybersecurity. And I'll start by talking a little bit about the technology, and particularly about new technologies that are changing the game, new approaches that I think we need to talk about. I hope these are new thoughts and new issues. We're in the middle of Cybersecurity Month and we've had lots of conferences and lots of panels. I am going to try to bring some new ideas into the discussion, and then I want to go and talk about policy and how to best approach this problem.

So first off, we've heard about -- the first FAQ is why do we need this legislation? And I guess the cynic and the skeptic would say, because Congress wants to be seen as doing something about this. When I was on the Hill, there were -- I knew of no more dangerous phrase than a Senator saying, we really must do something. You read my resume, but you didn't read the most important part of my resume. The most important part of my resume is the part I can never talk about. It's all the stupid things I prevented from happening, because I was in the room and was able to put my hand up and say, that sounds like a good idea but you're violating the third law of thermodynamics. (Laughter) Or, worse.

And I think we really need to focus on this question. You know, don't just do something, do the right thing. And I would argue we should start with the principle, do the minimal thing. Don't think about the grand comprehensive plan, don't talk about writing standards for every part of every company, don't think that way. Ask the question; what's preventing individual companies and agencies from doing the right thing today? There's a lot of barriers already that we can focus on, rather than trying to do the grand plan.

So, the things I wanted to bring up that -- so, the second question is what's new? Why is this a particularly important time to deal with cybersecurity? A couple words. The first word, cloud. I spend about half my time working on the evolution of the cloud. I just worked with TechAmerica on a very good report called, *Cloud First,* *Cloud Fast*, all about policies for facilitating the adoption of the cloud by government agencies and by the private sector. A very good section in there on how to do security for the cloud. And again, there was a stress on not trying to specify exactly how to do this but instead setting goals, measuring performance, not measuring technology.

One big opportunity is that we're moving to the cloud. We have the chance here as more and more companies start using Google data centers and Microsoft and IBM platforms, CSC cloud services. We have a chance here to get the security right and do it better. We're already making progress there, that's a great thing.

On the other side, the cloud is enabling the bad guys. I think you've probably heard of software as a service and infrastructure as a service? There's also CAAS, crime as a service. There's a great site called Future Crimes dot com, and he develops this idea that you can now go online and, just like you buy shoes on Zappos and knickknacks on eBay, you can buy hacker tools, you can buy criminal services. You know, crack credit card files, launch a DDoS attack. I mean, it used to be you had to have a little bit of coding talent. Now, you just have to be able to type in your credit card and type in the target you want to attack. So, CAAS, a phrase that we will see more of.

The other phrase I want to get out there, the other idea I want to share, is transparency. I'm finishing up a report for the Leading Edge Forum called, *Creating Your Transparency Policy in the Age of WikiLeaks*. And it takes the exact opposite approach to the question that many companies are asking themselves right now. Many companies are asking how do we lock more stuff down. How do we lock everything down? I would argue that's actually a wrong-headed question. Companies not only need to realize that they have very valuable data that they have to lock down, they also need to realize that they've got a lot of data that they should be sharing more. They should be making themselves more transparent and stop wasting a lot of time and effort trying to protect data that could and should be shared outside the company.

This is an hour-long lecture, I won't go into it. But I think we need to talk about security through transparency as well as the other techniques we're using. Sharing more information about what you're doing, making more people aware of the technologies and the tools you're using to protect your systems. Actually bringing in a larger community of collaborators who can help you understand how to protect yourself better.

And the last point here is the idea of networks to fight networks. John Arquilla is one of the leading theorists on cyber war, and he's made this point very well that we're losing in this area of cybersecurity because the bad guys are better networked and more collaborative than we are. We've talked a lot about information sharing, we need to do that more, but we need to use these tools better. And to do that better, we need to be more transparent and willing to share more information about what companies are doing. So, there's this balance that we're getting wrong right now. We're locking down too much; we're not being transparent about how we run our operations, about what threats are out there. And I think we can fix that.

Second question I'd like to address is what are the different legislative approaches that we're seeing? The one that we hear a lot about is a very prescriptive approach. It's about checklists of technology, it's about requiring that someone's password is a certain form, it's about all these different process and procedures that are going to be dictated to companies and agencies.

I would argue that's not going to keep up with the technology. And often, it's going to hold us back from adopting better cybersecurity technologies. So rather than a prescriptive approach, we might look at a performance-based approach. So, if we're trying to evaluate whether a company is secure or not, don't go in and see what they're doing, go and see what can be done to them. Hire a third party, ethical hackers, people who can go and attack their systems and see if they're vulnerable. Find the problems they've got and correct them. So again, it's about taking a close look at what's possible, about what a hacker can do to a company.

A third approach is a transparency-based approach to legislation. And I think we've made some good progress here, whereby requiring companies to reveal when there is a security breach. We're putting more pressure on them to invest more in security. The new SEC regulations, I think, are going to be very helpful, and we've already seen some changes in behavior because there is this increased transparency.

And then the fourth point is one that Representative mentioned that I think needs a lot more explanation and a lot more development. And that is, legislation that would foster an insurance-based approach to this. How to mobilize the insurance industry so that they will be there rewarding companies that are providing better cybersecurity; that they'll be motivated to do some of the audits that I've talked about. A lot of proposals on the Hill right now, but a lot of the ones I hear are much more prescriptive. They're telling people how to do things, not providing an environment that would push them to do the right thing. And so, I hope that we will see that instead of some of these prescriptive approaches.

Third FAQ, what models should we look to here? I think one particularly good model is the way we approached Y2K. When I was at the White House, I was involved in preparations for Y2K and then I moved to the Federal Communications Commission where I became the point person on that issue. At the time, there were some people that said, well we need to have checklists and we need to have every company reporting every quarter what they're doing to meet the Y2K challenge. Luckily, saner heads and a few of us who were arguing that's not going to work, that's going to distract people from the real problem. A few of us said, no. Let's just make sure that companies are talking to each other about their fixes, sharing information, let's make sure the U.S. government is asking the right questions of its contractors, providing a push that way. But don't think that we can anticipate all the things that have to be fixed to make sure we don't have a Y2K problem.

And instead of doing this sort of top-down approach, there really was a bottom-up approach. Lots of consultants out there who went in to work with companies to fix the Y2K problem. Luckily, everything was aligned, and luckily there was a deadline. We don't have that with cybersecurity, maybe we need to create an artificial one. But, we did very well with Y2K without the top-down prescriptive policy.

Another question I think would be helpful to address is what will not work? I think one thing that will not work is creating government-only networks and trying to have isolated networks that run a different protocol that don't use the Internet protocol. Trying to isolate those and make sure that nothing bad ever gets inside those networks is a very expensive, counter-productive idea. And I think this idea has been floated several times over the last 10 years, and again lots of people stood up and said, no, you can actually build sub-networks within the Internet. As Representative Langevin mentioned, you can build gated communities within the Internet where you have to have better authentication, where you don't have anonymity, where you have better monitoring. But to throw out 30 years of Internet technology and think that we can create better security in a brand-new network and keep that network isolated from any bad viruses or malware, I think is a fantasy.

Another really dangerous problem, I think, is thinking we can have security by obscurity. That we can somehow use tools and protect the code in a way that the bad guys won't ever be able to figure it out and ever be able to attack it. That's not working. I think security by transparency is a better approach.

Another really bad idea is going to be making cloud service providers and other IT service providers liable for any kind of breeches that might occur on their platform. This is a really tough issue. Right now, this is one place I really hope the Congress and the courts can clarify because we don't know where the liability really lies for a security breech. And it's getting more complicated when a little startup might create some software and run it on a cloud that's run by Amazon or Google, and then some other player, some other customer, comes in and uses that code and maybe doesn't secure it properly so their customer ends up having a problem because of a security breech. Now you've got four different layers there, four different players. How are you going to assign liability? Right now, we don't quite know. And I think there's a huge opportunity for cyber lawyers. There will always be money to be made in cyber law because we haven't clarified a lot of these important issues.

MR. FRIEDMAN: So, Mike, I hate to interrupt you but I feel --

MR. NELSON: That was my last, I think --

MR. FRIEDMAN: -- if we go through the fullest of bad ideas, we'll be here all day.

MR. NELSON: Well, that was sort of --

MR. FRIEDMAN: I just want to make sure of --

MR. NELSON: I'll just finish on an optimistic note. And that is to say what I really do hope the legislation will do. And that is that I hope we will see efforts to increase information sharing, improve the transparency both between government agencies and among corporations. I hope we'll see the government become a model customer for high security solutions, and share the lessons they've learned. And I really hope that we continue to create more economic incentives. Not tax breaks, but things like the security breech notification that push companies to do the right thing and to adopt new technologies, not to try to meet an old, outdated checklist of old technologies.

And the last point is that we do need to do this in an international way. Because the rest of the world is going to watch what the U.S. does. And if we do stupid things here, they'll replicate them very quickly. If we try to, for instance, decide that securing the cloud means that U.S. companies and U.S. agencies should only use U.S.-based clouds, that's going to invite the rest of the world to do the same thing. And they won't be hiring U.S. cloud providers to provide services, because they're not going to export their data if the U.S. doesn't export their data. So we need to work on a global basis to take advantage of the new technologies and new opportunities.

Hope that's helpful, hope it's provocative, and look forward to the Q and A.

MR. FRIEDMAN: Thank you. Point out, you come to Brookings, you get homework. So we can post links to the reading recommendations that Mike and Jim offered.

So before I go to audience questions, I wanted to ask the panel sort of a broad, overarching question. Which is, this tension between understanding the narrow policy questions we actually face and this sort of call for broad, comprehensive cybersecurity reform and legislation when we have, you know, very senior people talking about, well cybersecurity is important because we have, you know, Stuxnet and fishing, right? We have low-level banking fraud and high-level economic espionage, and long-term threats to the critical infrastructure. Is this the sort of thing we should be trying to put together because it allows efficiency and management? Or, should we be trying to tackle it more piecemeal approach because it allows a more targeted solution?

MR. AAVIKSOO: Well, I'm definitely in favor of a piecemeal approach. I even don't believe there's a possibility of having a comprehensive master plan, which makes everybody happy and solves all problems. It's -- first, there's no need for that. And secondly, it's too complicated and we don't have that much time. Simply the technology is developing so fast that until we finish our master plan, either good or bad, that's out of date already.

So, I think a piecemeal approach, and very pragmatic, rational thinking. We have a number of good things in place already. We shouldn't over-mystify sometimes cyber or virtual reality, or think like that. Bad things have been taking place. Let's address it as a bad thing, and try with existing tools to address that.

And in the case of real need, okay, let's pass an additional act but only in the case we really understand that there are exiting instruments that are insufficient.

MR. LONGLEY: I want to give voice to what I consider the unarticulated theme that Representative Langevin was volunteering. And that is the complete lack of action on the Hill. This has become a crisis, and very quickly to just get back to the overriding purpose here, there are two people here -- you saw Jim Lewis. Melissa Hathaway is also here, and I would direct you to an article that she published about two weeks ago. I think it's on *Computer Week* or *Federal Computer Digest*, but it's a very comprehensive survey of the status of the different legislative approaches on the Hill, including the issues involved.

I think the point I want to make is, emphatically, we need to take a piecemeal approach. There's a very high risk of taking a wrong step and making an enormous mistake. My favorite is the Canned Spam Act of 2003, okay? Every spammer, innocent and malicious, now includes the Congressional disclaimer at the bottom of their spam. And if you're naïve enough to click on it, it's probably the worst thing you've ever done. And from the standpoint of the well-intended, it's essentially a legal defense against sending you unsolicited e-mail. So, we've got to be careful.

I would come down very hard on the fact that -- and I think we're at a period historically -- and I don't mean to be too broad in my scope. But I think the process is being badly abused. We've let process get totally out of control. It's become an instrument of manipulation and authority and power games and politics. And I don't know -- you know, the Congressman made the point about the need for an executive authority. I would come down strongly on the need for a commission or a small group of three to five people with executive authority to act. And the action needs to encompass not only some of the more immediate issues, but they need to transcend all the politics, all the business development experts, all the lobbyists, everybody who has a vested interest in how this is organized in the bureaucracy. They need to address how to empower the private sector. We need to empower pilot projects and prototypes, and most importantly we need to give some flexibility and agility to the people who are charged with defending us.

By its very nature, you cannot structure a defense. You can posit a defense, but defense -- any adversary is going to go after the weaknesses in your structure. If you don't have the ability to respond to it, you're dead in the water.

And I guess a final point I might make is -- and I know this is an incredibly sensitive issue. But I think this three-member of five-member commission needs to have the authority to manage some of the issues relating to titles between intelligence, defense, national security, homeland security, and law enforcement and the Department of Justice. We are not going to quickly navigate through those wickets, but they have to be addressed.

Cyber doesn't care where it's going, and it doesn't care what kind of nice rules we've put together, and we need to find a way to structure action in a manner that is respectful -- is possible of the rights of the people.

MR. NELSON: I think we're in agreement here that a comprehensive approach is not going to be the answer here and it's not really viable. We need to find ways that different communities can understand the issue better, create the economic incentives to get different companies and organizations to take action.

I do think there's a need, though, for the Hill to clarify jurisdiction. And that's been clearly a big problem. A lot of overlapping agencies, different people thinking they have a lead, and I commend the Obama Administration and Melissa for really helping to try to sort that out. But at the end of the day it's not what the White House says the agency rules are, it's what the appropriators and the authorizing committees say on the Hill. So I do think some legislation that provided some more clear goals for the key agencies involved would be helpful.

But at the end of the day, this book *Worm* is a great example of where the de-centralized bottom-up approach is what really saved the day. It wasn't some grand plan or some imagined line. It was a bunch of very talented volunteers getting together with the best tools and sharing the information that allowed them to figure out where Conficker was coming from and what needed to be done about it.

MR. FRIEDMAN: Excellent. So I think we can open it up to questions from the audience. Just a brief reminder to identify yourself when you ask a question, and again a reminder that questions end in a question mark. (Laughter)

Yes, right here. Microphones are coming around.

MR. MARMON: Hi, Bill Marmon with the European Institute. I would like to go back to Minister Aaviksoo's comments about the need and the advisability of some sort of kinetic force response to nation-state-originated attacks, and the desirability of creating some sort of mutual feared destruction.

And also, if that's -- since you were instrumental in the implementation of the NATO base in Estonia -- what that is doing now and what role that may be playing?

MR. AAVIKSOO: Well, thank you. I'll start from the last question, concerning the Cooperative Cyber Defense Center of Excellence in Estonia. It's not an online executive military unit; it's rather a think-tank of policy development and advisory function. So it's not fighting back, it's rather thinking what might a cooperative cyber defense policy be? So this is just, I think, an important remark.

But as for response, I think it's fundamental that if we want to fight the bad guys, whoever they are on whatever level -- bad guys or governments or whomever. If we create a framework where there is a zero probability of retaliation, we fail in 100 percent of cases. There must be a credible deterrent present. Without credible deterrence, we can't fight any bad guys, whoever is providing that.

So in principle, if somebody makes bad things happen, he or she must know that somebody comes after them, ending the case of proportional response. In the ultimate case, may use kinetic force to eliminate the attack.

I mean, without that concept I can't imagine a credible deterrent scheme. Of course, it's psychologically and practically very, very complicated. But in principle, we shouldn't give up that option, even if we use it with a very, very, very, very low probability and when all the other responses are used up.

MR. LONGLEY: If I could add something to that --

MR. FRIEDMAN: Sure.

MR. LONGLEY: -- I think there's also an economic dimension to this. And I frankly think sometimes we have a U.S.-centric view of the world -- fail to recognize the number of Internet users that are now developing in India and China. As I understand, presently there are twice as many people in those two countries using the

Internet as we have people. And in three years, it will be four times as many.

And to the extent that we don't get our cyber policy straight, then I think it's going to really handicap American industry. I think, frankly, a good part of the world is waiting for us to act and is depending on us to act. And if we fail to move forward, it's going to have real consequences.

MR. FRIEDMAN: Further questions in the audience. Yes.

MR. HALLLORAN: Connor Halloran from SAIS. So, a follow-up on your comments, Minister Aaviksoo. You say that deterrence is sort of the basis from where you start. But deterrence requires attribution of the attacker, and you admitted earlier that you still are not entirely certain what happened in 2007. And so before we can have deterrence, we need attribution. So, what steps can be done to help bolster that? And lacking a credible method of attribution, how can we have a credible cyber defense?

MR. AAVIKSOO: Well, of course we need to attribute an attack. But we also need to attribute any other attack in real, physical space. Sometimes it's highly complicated. In the case of classical conflicts, we were able to do that. But we are fighting terrorism worldwide.

Are we fundamentally sure that we're attributing things right? Sometimes yes, sometimes no. So the very fact that attribution is complicated, I think is not enough to give up on the deterrence argument altogether. Of course, we have to develop practices, policies. What do we mean by solid evidence or evidence beyond reasonable doubt in the case of cyber events? Yes, there's a lot of work, a lot of conceptual work, legal work, practices, negotiations, developing concepts, all of that kind. But it doesn't mean that's not the way or we can give up not doing it at all because it's not attributable in the classical sense of fingerprints and footprints. Fingerprints can be faked, footprints can be faked, everything can be faked in this world -- in the physical world. It's not principally different from cyberspace.

MR. FRIEDMAN: So, there. Yes, on the aisle there. Blue shirt.

SPEAKER: My name is James; I'm with the Internet Bar Organization. I just wanted to follow up on Mr. Longley's sort of discussion on tort law and the steam boilers. Can you guys evaluate or asses what you think a possible judicial response would be to this? Like, through tort if the Capitol Hill fails to act or if you guys would like that, or?

MR. FRIEDMAN: So this is -- you'll notice there has been a lot of discussion for people saying, well we can use as one of the carrots for incentives liability protection. We don't have liability now. So, I think it's a huge question.

MR. LONGLEY: Well, and I have to caution, but I practiced law for 10 years but it's been 20 years since I did so.

Let me just suggest that if you go back and read the history of our legal system, first you understand that we're the first written constitution. English constitution goes back -- United Kingdom goes back to the 12th, 11th century, and it's unwritten. In fact, if you go back to the 11th century, it was considered a felony -- and again, I'm referring to the 11th century, please. But it was a felony for a free man to fail to raise the hue and cry when confronted with evidence of a crime. And crimes weren't defined, that's where a jury came in. And 12 men "good and true" would be convened to base -- to evaluate the conduct based on the standards of the community.

I'm not suggesting we go back that far. What I am suggesting is that basic property theory, i.e. I don't have a right to go into your house unannounced or without permission, nor do I think you have a right to come into my computer and make changes to it without my permission. We have to deal with the fact, candidly, that I think Congress has actually empowered practices that are inimical to the best interest of the public. I mean, when was the last time any of you read a privacy statement that came in the mail with your credit card or some other bill? You know, and when you read them carefully, they're worded in a manner that basically says we have the right to share this information any way we want to, and we're telling you. I mean, they're more cleverly-written than that.

But again, I want to come back to this whole idea of the responsibility of a free citizen, and I would extend that to people in the government. And I think what we're seeing -- and again, I don't mean to be so broad, but I think it's part of the problem. I think that we've seen a significant dumbing-down of the rights of individuals, either in the private sector or in government. And I didn't mention this earlier, but two examples that I've been using is 9/11. And if you read the 9/11 report -- and I happen to know one of the customer service representatives who gave one of the terrorists his boarding pass. And in this specific case, this individual knew he had a problem. He said, I said to myself, I said the hair went up on the back of my neck. He said, I said to myself, if this guy isn't a terrorist, nobody is. And then he said, then I mentally slapped myself. I could be sued, my airline could be sued.

And you go fast-forward to the Detroit bomber, and we have an analyst sitting there with credible evidence of vastly significant new threat and he doesn't pick up the phone. It would have taken two phone calls, TSA and the Visa department at the State Department.

And the sad part is that no one has thought about, okay -- you know -- and so my larger point here is, we really need to think through how do we structure decision making authority on these issues? Because this individual didn't feel empowered to make a phone call. And he didn't know the -- necessarily know the people at these two other agencies, and if he had made the phone call they probably wouldn’t have done anything because it didn't come through as an official report. And so I think it's time for, you know, really for us to hit the pause button and think clearly about how are we treating our people, both in and out of government? And where's the respect? And maybe we've lost some sight of that.

MR. NELSON: If I could just add to that, I think as we try to sort through these legal issues we should look beyond cybersecurity. I worry that if we focus just on that and we try to get the liability issues around cybersecurity right; we'll not take care of some other issues. Because there's concerns about whether my system is reliable enough. There's concerns about whether I'm ready for a natural disaster. What about operator error? And all these are beyond cybersecurity, but they all raise similar liability issues and we are seeing court cases now.

We're seeing people sued because their data magically disappeared. We have concerns about bankruptcies, web-hosting companies that don't have a failover plan in place so that they go out of business and dozens of startups go out of business, too, because all the data, all their websites, they were all there. So, we have a broader question here of, you know, who's responsible for what and what kind of compensation do I get if a service provider fails?

MR. AAVIKSOO: Just one more remark. When the attacks of April 2007 took place, we were preparing to start the Cooperative Cyber defense Center of Excellence in Estonia. And we invited the best specialists in the country. The country is luckily so small that we can have them all in one room, more or less.

And they were people from the banks, from other private sector institutions, including energy and the Ministry of Defense, other government agencies. And this informal group of people were working for almost two years, had been working to develop a concept for this NATO Center of Excellence.

When the attacks took place, they were immediately invited together and they reacted in an executive manner without formal of master plan or authorization. And we carried out a study -- luckily, nobody sued based on -- I mean, whether they were authorized duly or not. We carried out a study of all the decisions that were taken by them, or asked by them to be done, including outside Estonia, blocking some of the information flows, say, in Sweden.

We found tens of cases where formally taken, they didn't have the authority to behave as the behaved. So I think I very much subscribe to the arguments that, first, we have to build a network of defense if we really want to defend ourselves. The trust and confidence must be invested beyond the formal limits. How to do that in a right way? Here's a question mark. But, we need to do that. We need to invest trust into -- and common sense -- and again, building a hierarchical and structured defense, I very much agree that you'll always have weaknesses in such a system.

So, it's not a constructive approach to have a hierarchical structure authorized system in place. Instead of that, you should behave as the bad guys do in a flexible manner, and invested trust of the system.

MR. FRIEDMAN: Bill Woodcock is fond of saying the Internet works because 20 guys who do border routing go drinking together a couple times a year.

I think no panel on cybersecurity could be complete without a comment from Melissa Hathaway. So, the final question for you?

MS. HATHAWAY: Thanks very much. Thank you very much for the panel and your service to the world and cybersecurity.

My question is I'm going to build on each of you really amazing visuals. Jaak, you know, the warning banner on my computer. I'm going to use it in one of my next speeches. (Laughter) Mike, the price tag. And Jim, the commission.

And so I'm going to charge you now -- I'm going to be queen for the day, because I get to do that today. You're the three members of the bipartisan commission and you have to make one recommendation to the next President of the United States. Who and what is that action going to be? And that's your recommendation. So, one, two, three.

MR. NELSON: I'm going to start with transparency and go beyond the security breach notification laws that we have now. Clarify the different state laws so we have a single, clear rule on what companies have to report when there is a breech and go a little deeper so it's not just, you know, how many credit cards were stolen, but give us some information about how it was done and start this building of a trusted network between the good guys so that we can move forward.

I have a longer wish list, but if there's one theme I want to stress it's transparency and government, I think, has a very important role to play.

The other side of that is that government has also put in place rules that make it harder for companies to share information. There's a lot of places where we, for other good reasons, we have blocked information sharing. And that, I think, has to be -- that's at least as important. Sometimes we have to go back and look at the barriers as well as what needs to be done to push people.

MR. FRIEDMAN: Jim?

MR. LONGLEY: Lord help us if we have another joint deficit commission. (Laughter)

And I want to say something, and I don't mean to be this cynical. But we have some really serious problems in the way our executive authority and the way Congressional authority is being invoked, and I think you're seeing a public reaction that's premised on that mutual observation.

And I'm very aware of the pressures within the White House wherein decision making gets constrained based on this or that political constituency. And I almost think that we need some type of an independent commission that can make these decisions and figure out joint appointment authorities between the House and the Senate.

The other point -- and it's something that I think relates to this. I think right now the Congressional structure is seriously impeding the reforms we need. If you read the 9/11 report, DHS reports to something like 80 committees. If you read Richard Clarke, reports to 30 or 40. I want to add something, it's not just Congress. Operational -- and I wrote this out, and I want to be careful -- operational concerns in the government sector, Congress and Executive, nearly completely preclude any sharing that will compromise sources or methods from a defense or an operational or even a DHS perspective, not to mention privacy and title concerns.

We're stuck in a situation where every time an information door is opened, five more pop into view. I don't know that we're going to be able to act as quickly as we need to. But reading *Worm*, were dancing right along a precipice. And part of what motivated them in trying to take down Conficker -- and by the way, they couldn't take it down. They were able to manage it. Is that they felt we were one or two keystrokes away from the Internet completely shutting down. And, Jaak?

MR. FRIEDMAN: Jaak?

MR. AAVIKSOO: Well, I believe there are very many more good people than bad people.

MR. LONGLEY: Amen.

MR. AAVIKSOO: And that basically means that if the bad guys can organize themselves, so there are very many possibilities to organize good guys in a better way and vest trust in them.

So, building these networks based on win-win partnerships, I think is the way forward because it has to react immediately. One simple thing, hierarchical structure is unable to do that. So, we have to go a little bit beyond the classical thinking of common lines and think about a truly networked response. If we manage to do that, we'll be on the safe side.

MR. FRIEDMAN: All right. And on that note, our time is up. Thank you all for coming out this morning and spending your morning with us. Thanks to the Congressman and his staff. And of course, thank you to Mike, Jim, and Jaak.

(Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012