Center for Strategic and International Studies (CSIS)

Protecting the American Economy from Cyber Attacks

Introduction:
John Hamre,
President and CEO,
CSIS

Moderator:
Stephanie Sanok,
Deputy Director and Senior Fellow, International Security Program
CSIS

Speakers:
Representative Michael Rogers (R-MI);
Representative Charles Albert "Dutch" Ruppersberger III (D-MD)

Location:
CSIS B1 Conference Center,
Washington, D.C.

Time: 1:30 p.m. EST
Date: Wednesday, February 13, 2013

Transcript by
Federal News Service
Washington, D.C.

JOHN HAMRE: OK, while we're getting some last-minute direction, I just want to say welcome to all of you. Thank you very much for coming. And I would apologize for a slightly delayed start, but that's because they had a vote at 2:00, and both of them to – they came racing down here. And I'm delighted that they were able to make it, and want to say thank you, thank you to Chairman Rogers and to Ranking Member Ruppersberger for taking the time to be with us today.

I would like to say a public thank you to these gentlemen for leading on an issue that's complex and difficult. And they have been leading consistently. They've not always had the kind of support they've needed to do that, but they've persevered. They stood with the challenge because they knew this is probably one of the greatest things facing the United States, one of the great problems. Congressman, come out here. There's a seat in the front for you. (Chuckles.)

Would – want to say thank you – thank them for doing this and for the leadership that they've demonstrated. When others were worried about the turf or standing of their committee in the process, these men put the country's security at the front. And I think we all owe them a great deal of thanks for that. And I think – they've promised that they're going to continue this leadership going forward. I'm encouraged by that.

Last night, the president of course spoke to this. But you know, this has to be hammered out in the people's chamber, the Congress. You know, it's – the president may speak for the nation, but it is Congress that speaks for the people. And this has to be worked out in a way that people accept and understand, and it's this kind of leadership that's going to make this possible.

So could we – without any further delay, I would introduce to you Chairman Rogers. He's going to begin, and then Ranking Member Ruppersberger. Sir, thank you for coming. Please welcome him with your applause. (Applause.)

REPRESENTATIVE MICHAEL ROGERS (R-MI): Well, thank you for that, appreciate it. Thank you very much. Thank you. (Inaudible.)

Well, first of all, thank you very much. Thanks for hosting, John. I appreciate it very, very much. It's a great organization, and we always enjoy participating with you. Thank you.

I'll just be quick. When I first got on the committee some eight years ago, we had a briefing on something called cybersecurity that they said, this is something that we should pay attention to; this could be a problem. Exponentially year over end, this thing exploded into what is an epidemic. We are in a cyberwar. Most Americans don't know it. Most folks in the world probably don't know it. And at this point, we're losing. I have never seen anything so rampant as I have both on the espionage front, where nation-states like China are stealing intellectual property at a breathtaking pace, taking it back, repurposing and then using it to compete against those very same companies around the world, at a huge disadvantage to the company they just stole it from. You see this new capability in attack that's being developed, that's already part of military planning. We've watched the Russians use it as a part of their military operations. We certainly know the Chinese have the capability, other nations-states.

But the real difference here is this threat, which I'll talk about briefly. You have nation-states like Iran who are developing its capability, and they're not the rational actor when it comes to trying to disrupt or cause a catastrophic attack to our U.S. economy, like Russia would make that rational decision, when in wartime, all bets are off. Same with China only when it comes to the attack portion. Espionage, they're alive and well, and every single day, they literally have thousands of very highly-skilled cyberwarriors, or cyberspies in this case, working to steal you intellectual property. That happens every single day.

The last – on this Iran piece, seeing something interesting. Public reports show that they were behind the Aramco – the Saudi company Aramco attack. And if you look at that – and this is a good case to – I think, to analyze – very, very different. So they went into these systems; they manipulated data; they destroyed data; they destroyed 30,000 machines, destroyed them. That's new. That's a new level of capability we hadn't seen before.

MR. : Are you talking computers?

REP. ROGERS: Computers. So they have obviously aggressively stepped up their campaign. We saw recently – and this is publicly attributed to Iran, the – our financial services, that were – our banks, on a very less capable attack regiment than you saw against Aramco and another company that they hit called Rasgas.

So why? Most people believe that's a probing action. They're trying to find deficiencies in our systems to find a better way to come back and cause some catastrophic disruption. You can imagine how devastating it would be, not just getting into that system or not just causing a denial of service to that system but actually breaking the system, manipulation and changing data and destroying data – devastating. Could wipe out a company, could bankrupt a company. Some have argued that had the Aramco case, the system that they used for attack gotten a little further out than it did before it was caught, it could have even come back to impact parts of the United States, including some telecommunications companies.

MR. : How long did it take to catch it?

REP. ROGERS: How long did it take to catch it? About – well, after it started, it was there for a while, which they're still – and some of that is classified, but it is – was a matter of about days, not weeks. Think how much damage that was, just unbelievable.

So you think of that – now the world's changed, so it's a different place. So we can admire this problem, we can talk about this problem, we can say we have differences of opinion on how we ought to approach it, but the day has come where that kind of attack capability has reached the shores of the United States, and we better be ready for it. And if not, we're going to be picking up the pieces of what happens after an attack, and I don't think you want to see what Congress does then, all right? We don't do anything well after a significant emotional event.

So this is our chance, we believe, to prep ourselves to allow the private sector to defend itself. This is really very simple. So I want to thank the president for putting it in his State of the Union. That has been incredibly helpful for us. I want to thank the president's executive order.

Now, it's not perfect, but we are excited about the opportunity to have – to work with the president and fill in the gaps. That's kind of a down payment on where we get – half to go to legislation. We've had some great discussions with the White House. We've had great discussions with the Senate on our bill, not endorsing our bill by any means, but this year we've agreed we're all going to work together to come to a package on which we can agree on. I think that is a huge and significant difference from last year. So we've made that progress.

This bill is very, very simple. It says that we're going to share cyberthreat information with the private sector. Our senior intelligence folks who do this for a living tell us that with that – you know, the hardest part of these cyberthreats is the last 20 percent – they think that this can help stop 90 percent of that very difficult 20 percent. That makes sense. That is a huge impact. And it's not the government doing it; it's not a surveillance program; it's in real time at the light of speed (sic) exchanging zeros and ones when it comes to malicious software, to catch it and stop it from getting on your machine.

So we think we've got the answer. It's a bipartisan bill. Both Dutch and I have spent about two years trying to just get this thing up and running. We've interviewed privacy folks, business folks, all the government officials, and this is the bill we came up with that had the most bipartisan support. And we look forward to talking about that bill.

Dutch?

REPRESENTATIVE CHARLES ALBERT "DUTCH" RUPPERSBERGER III (D-MD): OK, Mike. First thing, thanks for having us here. I was late; I just had my knee replaced three weeks ago, and walking from the Capitol to here took a little bit longer, so – (laughter) – (who knew ?) what we're doing.

Also, I want to acknowledge my good friend John Tanner, a great member of Congress. John, is it true that life is so much better after you leave Congress? People don't beat up on you, you don't have to raise money, everybody gets along. Is that true? And you're making a lot of money, I understand, too, so that's a good thing. Good to see you here.

Well, first thing, I want to talk a little bit about how we got where we are, and – but before that, I want to acknowledge the leadership of Chairman Rogers. Mike and I were – have served on the Intelligence Committee for a long time. Before we took over the leadership of the committee, unfortunately, our committee was not working together. We didn't pass a bill for five or six years. I think Dave Ignatius from the Washington Post referred to our committee as a snake pit, and that members of Congress should look and see how Mike and I are running this committee in a bipartisan way.

And the reason I think – one of the reasons we do that is because we understand the stakes are so high in what we do. But a lot of it's about relationships and trust. And Mike's heard this before, but I like saying it: I was a former investigative prosecutor, and he was a former FBI agent. And I remind Mike all the time that good FBI agents always listen to their prosecutors, even if we're in the minority. (Scattered laughter.)

So – but with that – with that said, the issue of cyber really is something that most people in this country don't have a clue about where we are or what the threats are. I got involved when I was chairman of the Technical Tactical Committee. We were in the majority, by the way. It's a lot better being in the majority, unless you're working with Mike. (Laughter.)

And we had – I get a knock on the door and I had Admiral McConnell, who was the director of national intelligence; he was former director of the NSA. And he said, I'm going to tell you something that's very serious and we need to deal with it. He said, as we speak, we're getting cyberattacked right now by different countries, hackers, and it's very serious and it could affect our country. It could affect us economically through jobs and destructive attacks, and we've got to do something about it.

And when I realized how serious the threat was – I was also in the Appropriations Committee – I went to Jack Murtha, who's no longer with us, and I said, Jack, we have some real issues about cyberattacks. "What's cyber?" And I explained to him, and I said, we need to put some money in the budget and we need to deal with this issue. And so that's kind of how I first got involved.

And as the years evolved, we started to get more involved in cyber, but those of us who were involved in cyber were very frustrated. I know the White House hired a – what they called a cyber czar named Eric Schmidt. Eric was very competent and qualified but he had no authority. And when you don't have authority or a budget, you just become another consultant. That's all we – we need more consultants in this town.

So, what happened, we just didn't know where to go. Everybody's talking about the cyber threat and how the country doesn't know about it; the media aren't picking up what cyber is and what the threats are. So, in the end, Mike and I, when we got in the leadership, we said, we've got to deal with this issue. And we decided to do it the right way, in a bipartisan way. We called in the White House to work with us in working groups, we called in the business community to work with us, we called in ACLU and their privacy groups. And as a Democrat, I had to really focus on a lot of the privacy issues. And Mike and I have had a lot of heavy negotiations on the privacy issues to make sure that we had a balanced bill. And then that's where we got and how we really went forward.

Now, one of the things I do want to talk about, though, is how important and some of the threats, you know, why we have to deal with this. The bill, by the way, that we passed a year ago, passed in a bipartisan way. And by the way, it almost didn't pass. We were working with the White House for one year, and we thought everything was going fine. And the day before we go to committee, you go to the Rules Committee and then you go to the floor the next day. And 15 minutes before we go to the Rules Committee – I don't know when you received it – but Mike and I received a phone call that the president was going to veto our bill. And I said, what? You know, veto our bill? You've been working and you're telling this at the last minute? What's going on here?

And, you know, when you get a little upset and you've been working on something, I made a comment to a group like this the next morning before we went to the floor. And I said,

you know, I felt like the White House kicked me in the solar plexus. Well, that made national news, and of course the White House –

REP. ROGERS: What are you saying, what –

REP. RUPPERSBERGER: – and I said, look, I'm the one that should be mad, not you.

Well, we resolved all that; we're working with the White House. In fact, as of today, Mike and I talked with National Security Adviser Donilon, and the White House is now working with us to make sure somehow, some way that we get a bill. And we have to get a bill.

Now, again, these cyberattacks are everywhere, you know – our businesses; they're attacking the Cyber Command at NSA, who's really in charge of protecting the dot-mil and all of our NSA issues. Estimated just last year that our country lost over $300 billion of trade secrets even to the point where we have China – who is the most aggressive in this arena – they're taking our fertilizer companies. Who cares about fertilizer? Well, China, which is competing with the United States in fertilizer, so they hacked a fertilizer company.

We – now, as things evolve – and what's really important, and the difference between this year and last year now, too, is the fact that the dynamics have changed because we've had more serious attacks. Not only the $300 billion. Now we're having our Washington Post, our New York Times and Wall Street Journal attacked. And the incident of the attack of the New York Times is – the allegation is that China was hacking The New York Times to find out who their sources were so they could protect their country from any bad information or find someone that they thought was cooperating. I mean, this is – this is what we're talking.

And, you know, the thing that upsets, I think, Mike and I a lot is that we had the privacy groups at the time – we bent over backwards to make sure this law was constitutional, that this law was focused, that we were not invading anybody's privacy. The law says clearly we do not – we do not go into anybody's – read anybody's Internet, but still, the privacy groups have come out and said this is a SOPA. And that's not the case at all. It's an unfortunate – and it's our – maybe we need to do more work in educating not only privacy groups but America that we are not violating any constitutional rights but the threats are so serious that we have to deal with these threats.

And what worries us is a destructive a threat – destructive threat, destructive attack. And we know Iran, who I feel is a rogue nation and, you know, they're like the terrorist groups and they've attacked other countries. We talked about Aramco; attacked the United States. A destructive attack could occur tomorrow. You could take out the records of Bank of America, as an example. You know, most banking records are records anyhow. You could – you could – you could cut grid systems down. Anything having to do with technology could be attacked, and it could be a serious attack. Look at al-Qaida, who's always attacking us. What's to say they can't hire a major – a major hacker who's very good, pay him a couple million dollars and come and have one of those attacks? This is a serious issue and that we have – we have to deal with it.

The – we talked about – well, you've talked about Aramco, the banks – very serious. Let's see, I'm going to get to the questions.

The final thing I do want to say, too, as far as the president: The president – we had some issues with the White House the last time and we eventually have worked a – we don't still agree with everything in the bill. They don't agree with what we do and the vice versa. But where we do agree is that we're going to work together – our staff and their staff; our intelligence staff and their staff in the White House have been working together now. And we had a commitment again today from the White House. They will work with us because they know how serious. And the good news is the president really referenced our bill indirectly last night by saying that sharing of information, which is basically what our bill is – sharing of information is one of the most important things that we have to do, along with protecting privacy. And, clearly, we're going to be doing that.

Now, again, I want to say this over and over – and this is so important: that the bill does not authorize the government to monitor your computer, to read your email, tweets or Facebook posts. That is clear. There was an issue – a lot of negotiation about lawsuits. Well, we – the – we don't want the private sector every time they do something, they're subjected to a lawsuit. We don't want – we're not here to promote litigation. But what we are here to do is to make sure that if a company does not use good faith in doing what they need to do to protect us, then they could be subjected. And Mike and I had a long drawn-out negotiation on that issue. So, when you hear about the privacy issues, I would – I would really – we're going to keep listening, but I feel very strongly – and I'm an attorney and I was trained to follow the Constitution – that we have – we have protected ourselves in that regard.

So, what we need now – and this is my opinion, but I feel there's one thing stopping us from these cyberattacks, and where we need to have the intelligence community give the – attacks that are coming in every day that they see and they need – we need to pass a law to allow them to pass that classified information to the businesses, to the providers, so that they can protect us, and then they can come back and we can work them to protect us and our country.

The one thing standing in the way, in my opinion, right now is Congress. We need to pass our bill, our CISPA bill, and if we do that, we then will be able to protect our country. All the other issues out there that they're concerned about – what happened when our bill went to the Senate, they talked about the issue of infrastructure, critical infrastructure. Well, that's not in our jurisdiction. Let Homeland Security deal with that. There're going to be thousands of cyber pieces of legislation throughout the years. All we're trying to do is get the camel's nose in the tent, let us get the information to the providers. The providers, they control 80 percent of our systems with our network in this country. If we can do that, we feel we're on our way to protecting our country and stop having the cyberattacks losing as of last year over $300 billion of trade secrets.

STEPHANIE SANOK: All right. Please join us in – please join me in thanking our two panelists here for their opening remarks. Thank you, gentlemen. (Applause.)

REP. : Thanks very much.

MS. SANOK: Now, if you checked out your agenda, you'd have seen that Jim Lewis, our director of the Technology and Public Policy Program here at CSIS was supposed to moderate this panel. As you can probably note, I am not Jim Lewis –

MR. : (Off mic.)

MS. SANOK: Well, I appreciate that. (Chuckles.) But I won't tell him you said that.

What I would say is Jim is on his way back from Europe right now. He will be hosting Michael Daniel, who is the White House's cyber coordinator, in an event here on Friday morning at 9:00 a.m. So, if you want to see Jim or want to hear what Mr. Daniel has to say, please join us then.

Before I turn and use the moderator's prerogative to ask our first questions – my name is Stephanie Sanok – I have some administrative details to let you all know about. One, I would really appreciate it if you could turn your electronic devices to silent or stun. We are being filmed; we're also live-tweeting from this event. We're getting some people watching our webcast, and so if you wouldn't mind turning your devices down, that would be really – (audio interference). And – (laughter).

REP : (Off mic) – want attention.

MS. SANOK: (Chuckles.) So, as the acting director of homeland security and counterterrorism, I have a tremendous interest in what Congressman Ruppersberger was just talking about – infrastructure protection. But before we get to that question and the question about protection of privacy, which is a big issue for the homeland security world, I would like to ask Chairman Rogers a quick question about what the president said last night during his State of the Union address. He talked about the importance of information sharing, voluntary standards. He also said that Congress must act to pass legislation to enable the government to take these steps. Can you talk a little bit about your reaction to the State of the Union statement on this issue but also why is legislation necessary? Why is the executive order not enough?

REP. ROGERS: Yeah, well, first of all, it was great news that the president put it in the State of the Union – that's a good thing – and to acknowledge that we needed to pass a bill in Congress – another very good thing. That's a bit of a tone change. That's a – we are wildly accepting of that tone change and we think that now we're in a better place to work with the White House to try to find some common ground as this bill moves out of the House. We also think by just him elevating it to that level we'll get better attention in the Senate as well. And the executive order, we think, takes a little pressure off of the Senate's insistence of infrastructure rules, regulations and standards. So, we think that all of that combined, I think, increases our opportunity to actually get a cybersharing bill that we all believe – and I think the White House clearly now believes – is important for us to get enacted.

Now, the reason you have to have the law is, A, the – it's about liability protection. So if you want a voluntary system where you are sharing threat information – we're talking zeros and

ones configured in, sometimes, literally millions of lines of code in some cases – in real time, you have to have the protection to say that I'm going to engage in that sharing and I'm not going to get sued because I'm sharing threat information from the government to the private sector. And if the private sector chooses, by the way – and they do not have to – if they want to share some threat information that they've gotten that maybe the government wasn't aware of, they want to make sure that they're protected with some liability protection. So, that's why we have to do it.

You have to change the law because information that is collected in a classified way can't really be disclosed in something other than a classified way, in a broad sense. So, you – the president has the right to declassify, but you wouldn't be able to declassify all of it simply because if I – if you all – if the bad guy knows what I'm looking for, then they change what I'm looking for. Pretty easy to do in the cyberworld. So you have to have that construct; it takes legal change in order to do that.

MS. SANOK: And you think that this sign from the White House that they want to advance the dialogue and discussion and policy in this area is something that will help the Senate sort of overcome some of the objection. My understanding is that they didn't even consider your bill last time around.

REP. ROGERS: That's correct. They wanted to make sure that there was a standards piece attached to it. And some, including me, had some serious, you know, differences of opinion. They actually had a kill switch in their bill. I just was shocked by that. I'm still shocked by that, and I wouldn't support that. And so we work very hard to try to avoid all that to try to preserve the open fairness of the Internet. That was our goal here: How can we do this in a way that still protects that openness and freedom of the Internet? We think this does it. We think the government having that kill switch is an awful idea. Might work for Iran or China or Cuba; it doesn't work here.

MS. SANOK: Thank you for that.

My other question before we open it up to the floor, sir, is for you. You had mentioned meeting with the ACLU, with the White House. My understanding is the White House's veto threat last time around was mostly hinged on civil liberties and privacy concerns. Can you talk a little bit about – you know, the importance of living in a democracy, you have privacy concerns of the individual but also the collective security of the nation. Can you talk a little bit about how you approached the White House, how the White House approached you, how these negotiations went?

REP. RUPPERSBERGER: Well, in the beginning we brought in all – different groups – the business community, the White House, ACLU – everybody, because we wanted their point of view. We realized if we wanted a bipartisan bill that was going to pass the Senate, be signed by the president, that we had to do this. The first thing we had to do though is really define what the threat was. And the threat is severe. And just since last year, the threats have gotten a lot worse. And you know, I guarantee you that if we have a destructive attack, like a – like we had at 9/11 – we'll get all the bills passed we want. But we're trying to be proactive and deal with

this issue before that really happens. And with an Iran out there or other terrorist countries, you don't know what the exposure is going to be.

But forget about the destructive attack. It's just the actual stealing of trade secrets, losing thousands of jobs. And when you get all the information where certain countries are using that to compete against us, that's wrong. So we brought the group in for a year. Where we got off, I think, was a lack of communication where we – the White House never signaled to us or our staff that they were concerned about some of the things that we – when we put our bill together – that we thought they were OK with. So we had some issues and some strong debates, but now we're right back focused on the bill, working closely with the White House. And again, Mike and I thought it was important to go to the top to make sure that we had a commitment.

It's not about us. It's not about them. It's about the country getting it right. And we want to make sure – clearly make sure that we deal with the issue of civil liberties and privacy. And again, as a Democrat, my side demands that. And Mike and I had a lot of negotiations on this issue – on lawsuits and on privacy issues and that – and that type of thing. What we – and I'll read these three things. The bill has strong privacy protections. First, it narrowly defines what information can be shared with government. Not – it's not as broad. So it narrowly defines that. And that's extremely important.

Secondly –

REP. ROGERS: It's a cyberthreat – (inaudible) –

REP. RUPPERSBERGER: Yeah, cyberthreat.

REP. ROGERS: It can only be cyber.

REP. RUPPERSBERGER: Well, what it is, there are five categories. It's cyber – and this so something that we didn't have in the beginning. And really I believe it was the ACLU or one of the privacy groups that felt we needed to narrow the bill. And it dealt with cyberthreats, it dealt with national security threats. And that is a – still a negotiation point as far as the ACLU is concerned, that they feel that's – national security is still too broad. We don't. We feel that national security is national security.

And that's basically cyberattacks, what these attacks will do to our national security. We have it in there about any – we can use any information about children and children pornography and that type of thing, if there's an imminent threat for life or danger or someone willing to commit a murder. You know, there are very basic five elements and that was it. So we narrowed that down. We listened to the privacy groups. We put that in the bill.

Also, third – and this is important too – it's always important to have checks and balances. If you look at why we still have the best country in the world, it's because our forefathers created a government of checks and balances – the judiciary, the administration and Congress. Now, in this situation, we have the inspector general of the intelligence community

has to complete a report evaluating this whole program and our law and highlighting any privacy problems that arise and ensures they can be fixed.

This isn't a five-year sunset; we look at it in five years. This is the inspector general completing a report evaluating this program. That's another check and balance. And we want to make sure those checks and balances are there because sometimes reality and perceptions aren't always – come out the same way. And I think what concerned me with some of the privacy groups, we reached out and it seemed that there was nothing we could say to change it.

There was just an opinion that the intelligence community was listening to everybody. Believe me, they aren't. In this country, it's against the law for any of our intelligence committee – any of our intelligences committees or – like, NSA or NRO or any of these groups – it's against the law for them to spy on an American citizen or gain that information unless we have a court order from FISA court. So that's already in place. And if we don't do that, we can go to jail. It's against the law.

So we feel strongly that the bill clearly deals with the privacy issues. And again, I want to say this over and over, it does not authorize the government to monitor your computer, to read your email, tweets or Facebook posts. That's clear in what the law is.

MS. : Well, thank you for that clarity. I would like to open it up to the audience for questions at this time. If you wouldn't mind, when we call on you, if you could stand up, state your name or your affiliation. We will be having roving mics, right? All right, please wait for the microphone before you do that. And then keep your question to a question, if possible.

So this gentleman up here can go first. Thank you.

Q: Good afternoon, gentlemen. Ronald Marks, George Washington University, Homeland Security Policy Institute – (inaudible). Last year, the Silicon Valley and the U.S. Chamber of Commerce really rained on this parade very badly. And I'm curious as to how you are reaching out to them this time around. It seemed as though there was some conflict last time.

REP. ROGERS: This is – you have hit the nail on the head for one of the big myths about what happened last year. There were two separate pieces of legislation. One was called SOPA. They rained on that as hard – and by the way, I did not support SOPA. I thought it was the wrong approach to this – to what they were trying to get after is protecting intellectual property, having the government force others to report on others, that's a bad idea. I did not support it. That's where it got confused.

So – and Dutch and I realized that up front that that had just happened and we had this whole other thing we had to do, which was to try to share information on threats. The Silicon Valley – I said when I started out, if I could get the Silicon Valley, Hollywood and Wall Street on the same bill, we had done something pretty amazing, right? It's almost impossible to do. We did it. We did it because it's very narrow, it's not intrusive, it's all voluntary and we protect privacy of their users – by the way, which is not happening today. Your personal private information, I'll tell you what. The Chinese are all over it, the Russians are on it, the Iranians.

Your Google – you know, the list is pretty long of folks who are getting after your private information. This, we think, probably provides the best protection from people stealing it and taking it overseas – Russian organized crime. So that was the difference. They are enthusiastically for this bill. So we have some 72 supporters, some larger groups. I think we estimate it was almost 4 million people in this business who directly were employed by this business being through the Internet in some way, shape or form, support the issue. The Chamber supports it. Their (backup ?), the Business Roundtable supports it. So we – that's why we feel so comfortable. We've found, we think, that middle ground, and it was also why we were able to get a bipartisan bill through the House.

MS. SANOK: Thank you.

This gentleman in the back.

Q: Hi, I'm Bruce MacDonald with the U.S. Institute of Peace, and I'm an adjunct professor at Johns Hopkins SAIS. First, I want to thank both of you for your leadership on this issue. When I worked in the science advisers office in the Clinton administration in the White House, information sharing was a huge, tough issue, and the fact that you've cracked it and been able to win support is really great, so I salute you.

I was in Beijing a couple of weeks ago and talking with some of their people there on nuclear issues but also space and cyber, and I'll just throw out for your consideration that, you know, they're worried about us, too, and legitimately. But I share all the concerns that you – that you both have expressed. And I would throw out for your consideration maybe there ought to be – see if we could set up some kind of at least dialogue so we could maybe reach some kind of an understanding.

But my real pointed question – not too pointed, I hope – is that it's a great piece of legislation. And I – from what I hear, I really support it. But would you consider something in it that might call for every couple years or so a review or evaluation to sort of check how it's doing in reality versus what you both were hoping for, some kind of evaluation so that you can, you know, update it, change it, trash it if it doesn't work – but hopefully that won't be the case. But would you consider something like that in there so that we can see and try to track in that way how well it's doing in meeting the good needs that you both have identified?

REP. ROGERS: That's such a good idea. It should be an amendment, and it was. So congratulations.

REP. RUPPERSBERGER: And it's in – it's in the bill.

REP. ROGERS: It's in the bill.

REP. RUPPERSBERGER: One of the most important things was –

REP. ROGERS: It's the IG inspector.

REP. RUPPERSBERGER: Yeah, the inspector general, who's entirely separate. You have – most of your agencies, NSA, has an inspector general, and they have to evaluate what they're doing and then finding out if they're breaking any laws or anything of that nature. We

not only have – not have them oversee it, we have them writing a report. So that is something important.

And we had a little negotiation, but I think most – we can together that we needed that outside – that independent party, and that's what the inspector general's job is.

The other thing – let me talk about China. China and the United States need to continue dialogue. China is a very powerful, strong country. They have a lot of money, and they're investing a lot in a lot of different arenas. We need to have dialogue, but before that dialogue occurs, we need to tell China to stop cyberattacking us. We have had dialogue. We had dialogue – Mike and I investigated Huawai and ZTE, two major Chinese companies, and what our concern was, is they were trying to be more aggressive in the United States and put their infrastructure in the United States. I personally in Hong Kong met with the founder of Huawei, who doesn't meet with a lot of people. And I said to him, look, we know we're in a global economy, but you need to tell your country, China, to stop cyberattacking our businesses and stealing information if you want us to work with you, and we'll do that. And you can deny all you want. We have the evidence that you're doing this. And I'm sure there are many Chinese in this room today that will take the information back of what we're saying. And we want to work with China, because this is a global issue, and technology will keep evolving as we go forward. So I think we're doing that, and I – hopefully that with the evidence that we have, that we can come together at least on the issue of not stealing information. I can tell you the United States is not cyberattacking China's businesses to get – gain information and classified information or anything of that nature. And it's just not China. There are other countries. And what worries me probably more than any right now is probably Iran. Iran's a country out there that they're mad at everybody, they're concerned about the United States and the sanctions that we have and we've organized the world, and yet they have the capacity or the ability to hire some of the best hackers in the world to cyberattack us.

MS. SANOK: Thank you.

REP. RUPPERSBERGER: So you raise a good point, but I think we're kind of where you are. I hope we are.

MS. SANOK: This man in the middle, please.

Q: Thank you. Jeffrey Lin (sp) from George Washington University. I was wondering particularly how the –

REP. RUPPERSBERGER: What university?

MS. SANOK: George Washington.

Q: How this sort of information sharing would sort of have to evolve with new trends in technology such as an increasing use of robotics, which I assume would be naturally connected to the Internet in a very large way.

REP. ROGERS: Yeah. Again, the beauty of the simplicity of the way we're doing this is our government comes across malicious software that sometimes – in some cases has been engaged and used, in some cases is developed and not used. So any type of that malicious

software in a classified setting can be shared with as high upstream to users as you can get. Providers are the most optimal, so whoever's providing your services, so whoever would service that particular – if it's a robot in this case, you want to stop it before it ever gets to the operating system for that robot. That's the goal here, is to stop it as far upstream as you can. So that sharing that happens, again, in real time – this isn't content-driven; it's zeros and ones at light speed, hundreds of millions of times a second – and they're looking for anomalies in the packet that fits a signature that they know contains malicious software. And so, again, the – any time you're hooked up to the Internet, you are exposed. So if you are on the Internet, you are exposed, period. And that's what we hope to accomplish on this.

And I'll tell you a quick anecdote, as well. The other part of this is computer hygiene. We are so woefully behind on educating people about computer hygiene: what not – what not to do, how to respond to fishing attacks, introducing other media into your computer that you're not familiar with. And I tell you that because I was invited not all that long ago to give a speech on cybersecurity, so this was a group of individuals who were geared around it, educated on it, and their mission was to do cybersecurity for this particular industry.

And I showed up at the event, and on the little gift bags, guess what was in the gift bags? A thumb drive. I said, man, I have – if we can't quite understand from the folks who do this for a living that you should never take a thumb drive that you don't – that isn't yours or isn't brand new and put it in your machine, we got a long way to go. And it just tells you how long we have to go to get on computer – we can solve 80 percent of our problems through operator education, and I mean operator at the computer level. So some of us talked about we need a new Smokey the Bear campaign, only like Freddie the Firewall or something – (laughter) – to try to educate people across America: Hey, these are just some really simple things you can do to prevent this malware from getting on your computer and infecting other people's networks.

MS. SANOK: Thank you.

Question in the back right here.

Q: Bob English (sp), RT News. You had talked –

MR. : Who?

Q: Bob English (sp), RT News.

MR. : OK.

Q: You had talked about privacy concerns and checks and balances with respect to the way that you would be, I guess, deploying this new bill, and you were talking about the legal protection for companies as well. Are there checks and balances on the companies' immunity from prosecution now that you see in this, and would that come from the inspector general, or is there something statutory?

REP. ROGERS: Yeah, part of the inspector general's charge in this – and it's pretty specific in the bill – is to talk about all the information that was shared and how it was used, to make sure it comports with the law. And it provides the opportunity for those company (ph) to

anonymize that information or minimize the information. So all of those protections are already built in.

And again, at the end of the day, content – if this was about content, none of this would work. It can't be about content. It has to be about trying to find that malicious code that may in fact be embedded in an email or whatever, but that's not the content. So that's not what we're worried about.

But to make sure – to doubly make sure that they're following the law – and again, this is hundreds of millions of times a second – you had the IG must every year go through, do an audit and then come back and report to us on what they found and how they've used the information, what kind of information came in; if they got it wrong, how did they rectify it to make sure that that information was appropriately destroyed and is not collected on government servers, which we thought was important.

Q: Thank you.

MS. SANOK: This man right in front of him.

Q: Mike Armstead (sp). I'm a privacy contractor specialist for policy. My question is to your point, Congressman, on computer hygiene being kind of the central focus of really helping solve these problems, one of the things I worry about is, how do you ensure that people who don't necessarily have proper computer hygiene, that become in some ways the tip of the spear of these types of cyberattacks by their computers being turned into weapons for these aggressions – how do you keep them from being caught up in the dragnet, so to speak, by the intelligence community when an intrusion is detected and their machines essentially are the front line?

REP. ROGERS: Yeah, well, again, here's the benefit of this, is that could happen. Even under this arrangement, there could be – you know, something could get through. This is – nothing's fool-proof. And again, this – we don't lay claim that this will solve all of our problems, by the way. We don't. We just think it's that – the one thing we can all agree on that would have a tremendous impact that we could implement pretty quickly.

So what would happen in that case – if that computer's turned into a botnet, I presume you're talking about – that if they find the anomaly, they won't find it probably here. But if, say, a McAfee or a Norton or somebody else who is constantly also hundreds of millions of times a second checking their system, right, for signatures that they know are bad, and if somebody – you see an anomaly that, say, happens in Switzerland that – and they've used the botnet of a thousand machines, some here, some over there, some all over the – Europe, Eastern Europe, then that's when they catch it. So they'll catch that anomaly. They either pass it off to a Norton or a MacAfee, right, and then they just stop it. So there's no – nobody's going to go through your system and go through your files. That's not what's going to happen.

And if they wanted to do that, they would have to get a court order, just like they would today. That would not change. And so that's the beauty – the beautiful thing of it. And if you're on that computer, you probably would have no idea that that malicious software just got killed. You'd be doing your thing and – that – in theory, that's the way you want it work, and it would work that way now.

REP. RUPPERSBERGER: You know, as cybereducation goes forward, you're going to see a lot of issues and problems that we have to deal with just through administrative issues – who sets the standards. Who is allowed to come in and help an individual owner in a residence with their computer? You know, what's – do you call a certain company? Do they have to be certified? There's the volume of information, the volume of people that are using technology today.

So – and one of the things – and I agree with the administration on this – they were concerned about having our military intelligence community involved in working on the domestic area, and I think they're right, because you have to deal with perceptions. We talk about perceptions and reality, and I don't think we want our government to be – to be involved in that arena.

Now the White House, I think, is leaning towards Homeland Security. My only concern with Homeland Security is they have over 21 missions already. I think this cyberissue is so important that we probably should have a sub-Cabinet or a special area just to deal with how we implement, you know, our cybersecurity issues to every individual in this country. But again, we're not dealing with that. That's not our mission on this committee, it's not our jurisdiction. We're just trying to get the information that we have, that we – our intelligence community gets every day and pass that information – we call it secret sauce – to the providers so they can then work with us to protect it.

And another thing, too. When the businesses are involved, this is all voluntary, and that's important, too. Because you know, we – this will not work, this – our bill will not work, and the process that hopefully we will create by passing the bill – if business doesn't work with government in partnership, working together. But business is not required. They don't have to get involved. Now they will want to because they'll want to protect themselves from cyberattacks. And if they sell computers or they deal with technology, they're going to be in a position where they're going to have to protect their customers. So that's a – it's an issue that we've got a long way to go. This is just the beginning of our bill, and all we're trying to do is to get it passed. It will start protecting you and you and us and all the companies that are out there that do not have that protection now until our bill passes.

MS. SANOK: Well, thank you very much. That's actually all the time we have for questions today. One thing I would like to say is, a common theme that resonated both last night and in today's conversation is this concept of the government and the private sector working together to address this threat and reduce vulnerabilities, and I think that's something that I will take away from this session as being very reassured that this is what you all are aiming for. So thank – gentlemen, thank you so much for joining us.

REP. : OK.

REP. : Thank you so much. Appreciate it. (Applause.)

(END)