

CRYPTOME

31 October 2014

https://www.nsa.gov/public_info/speeches_testimonies/28oct14_dirnsa.shtml

National Security Agency

"Sharing Cyber Threat Information to Protect Business and America"

Speakers:

**Admiral Michael Rogers,
Commander, U.S. Cyber Command, and
Director, National Security Agency**

**Marc Gordon,
CIO, American Express**

Moderator:

**Ann Beauchesne,
Vice President, National Security & Emergency Preparedness Department,
U.S. Chamber of Commerce**

Location: U.S. Chamber of Commerce, Washington, D.C.

Time: 12:29 p.m. EDT

Date: Tuesday, October 28, 2014

*Transcript by
Federal News Service
Washington, D.C.*

MARC GORDON: Thank you, Ed (sp), very much.

I want to just start by thanking you and the chamber. Your proactive leadership on this topic, I think, is second to none, and I think you're doing a great service for the global community in what you're doing.

What I want to do is very briefly provide a private sector view on the environment – the importance of information sharing in particular, and the obstacles that we face and a little bit of a call to action before introducing Admiral Rogers. So let me start with something that everyone here obviously well understands – the range of attacks that we experience in the private sector is really unprecedented, and getting worse by the day. The volume and sophistication of attacks is only showing signs of acceleration, and every published success simply encourages new entrants and bolder moves.

Threat actors from social activists, cyber criminals, nation states – tier one and tier two – with a range of objectives from disruption, intellectual property theft, financial crime, and the one that I'm the most concerned about over time – destructive intent. And cyber criminal activities in particular have simply exploded, and while one-at-a-time, they impact individuals, they impact companies, collectively, they represent, I feel, a potential threat to the country if they continue to build the way they're building, and in particular, if they become more orchestrated. Imagine the top 10 retailers attacked at the same moment – the top 10 financial services companies attacked at the same moment, and the impact on the confidence in our economy.

And especially if the capabilities that today are pointed towards financial criminal activity start to turn towards destructive intent. It's a very sobering concern for us. Now, we each, in the private sector, have a range of controls and capabilities in terms of cyber protection and continue to invest. I estimate we probably spend more than \$2 billion in the U.S. across the financial sector in cyber defenses, from protecting the perimeter to protecting data loss to insider threats, and we'll

continue to invest in our capabilities, but I like to use the fort analogy when I think about information sharing.

So you think of a company as a fort. Of course, we have to know when we're under attack, but at the same time, it is incredibly valuable to know when a neighbor's fort is under attack, or when the adversaries are marshaling their forces in the forest, getting ready to attack, or when they're back in the home country building weaponry to attack the fort.

And in my view, probably the single best control that any company could have is transparency around what's happening around us with our sector – across sectors and with the government. Said another way, I believe that the lowest-cost, highest-value control is information sharing, that information sharing has the best ROI of any investment any of us could make in the system of cyber protection.

One company's detected moment can become an entire sector's defense, or a cross-sector defense. And further, no one entity can stand alone. Not a single business, not a sector, not law enforcement, not the intelligence community. Each of us brings different and additive insights. I really believe that the whole is greater than the sum of the parts, and that to protect individuals, businesses, the country, we've got to work together. Customers, businesses, privacy advocates, law enforcement, intelligence, homeland security working together to protect our customers' interests, our business interests, critical national infrastructure and the country.

And further, while I do actually believe that information sharing is in the best interests for each of us in our businesses, I also believe that we have a moral obligation as socially responsible enterprises to try to share and not to consider our cyber insights as a source of competitive advantage that, unfortunately, some companies do look at it that way.

But effectively sharing cyber information actually is not easy at all. Now, there is a fair amount of information that does get shared. There is information sharing, but it's slow. It's relationship and trust-based. It's very variable within and across industries and with the government, and there are a range of obstacles.

The first obstacle, for the private sector, is that we are simply, in many cases, unable to share cyber information due to the potential legal liabilities that may occur from that. So you think about, what if someone acts on information that we've shared? We've shared it in good faith, but by acting, they've caused some harm, or, on the flip side of that, if we share information, but in good faith, a company decides not to act on that information, because they've got a basis for not acting, the liability in both instances is so substantial from a risk perspective that it completely stands in the way of material information sharing.

Second, there are just too many vehicles for information sharing. It's very variable, it's well-intended. It's frankly, a bit chaotic, and it's hardly complete. So, to throw out some acronyms – the ISACS, NCFTA, ECTF, CISCP, ECS, the (physics ?), fusion centers, NCIC, NCIJTF, company to company, FBI, Treasury, Homeland Security, Secret Service to company – all of those occur in some moment or another. They're well-intended; they're very appreciated, from the private sector, but sometimes they're conflicting. Sometimes very inconsistent, and almost no information sharing happens real-time.

The third obstacle, I would say, from the private sector perspective is, the government overclassifies. So what's shared at the secret level is very rarely actionable, and not enough private sector employers have clearances above the secret level, where more of the actionable information tends to reside. So there's an issue with government classification.

Now, I'd compare and contrast what we get in open source intelligence. I just think about the last two days. Yesterday, you would have seen some information

about a new watering hole attack that's been out there called Scanbox. It's open-source data. We get what are called indicators of compromise. We can act on those. Last night, overnight, detail was released in, again, an open-source context about the new purported Chinese APT attack called Axiom. But what comes with the open source is actionable intelligence, things we can actually do something about, and that really is an obstacle relative to what we hear and see from the government sector.

So I'll close with a bit of a call to action. On the private sector, support – for those of you from the private sector, as I am, support for legislation that's out there on information sharing – there are two bills out there. I would support either of them. They are really important to opening up the volume and speed and capability of sharing that can go on. And it is the highest ROI opportunity in the system of cyber defense.

I would call out two things. One is there should be liability protection both for acting and for not acting. I think that's important, two sides of the coin. And the second thing I would say is, very clearly, information can and will be anonymized. There's no reason not to anonymize. We can really address those privacy concerns, I believe, very effectively.

Also for the private sector, if you're not in one of the ISACs – and I can – I think you all know what those are, but if you're not in an ISAC, you should join one. If you're in an ISAC, you should be very active. There's a very uneven level of contribution across the ISACs in terms of information sharing. We need your insights. We contribute very actively. I would call on you to do the same.

For the public sector, a call to action from my perspective is, again, pass the information-sharing legislation. Also, we need a better process to get private-sector clearances either above secret or to make shared intelligence more actionable at the secret level. More importantly, what we really need is a systematized construct for how information is shared: frequency, format,

actionable substance and as close to real time as we can make it, coordinated across homeland security, law enforcement, intelligence agencies and the private sector. So that's a view from the private sector. I thought I would share that. It's now my privilege to introduce Admiral Rogers.

In April of this year, Admiral Rogers assumed the post of commander, U.S. Cyber Command, director of the National Security Agency and chief of the Central Security Service. You have his bio in your package, but to summarize, prior to his current post he served as the commander of the U.S. Fleet Cyber Command and the Navy's U.S. 10th Fleet. Since becoming a flag officer in 2007, he's also served as the director for intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, with over 30 years of service, both ashore and afloat. He has extensive experience in intelligence gathering, computer network defense and information warfare.

Now, on a personal note – and I shared this with the admiral as he was coming in – I actually met him in 2012 very briefly at a cybersecurity conference at West Point. And the theme of the conference was actually public-private collaboration and the role of each sector in defense of the nation. And my impression of the then-vice admiral was formed and we actually sat next to each other for maybe 30, 45 minutes the morning of that event.

And I thought back on the experience to try to convey the sense that I took away from that short moment, and what I would tell you is this: Having not had at that time a lot of private-sector experience, he was very inquisitive about the private sector. He asked a lot of questions. He was a very active listener. He seemed to have, to me, an appetite to learn about the challenges faced in the private sector and to contemplate the opportunities for collaboration. He also conveyed, as you would expect, a purpose – sense of purpose, a belief in his mission, and a very – what I would think of as a very calm sense of command.

What was interesting, though, as I reflected, was – what came away for me in that moment, which I think will be reinforced by what you have heard and what you will hear today, is the admiral is actually very committed to public/private partnerships and is a very strong advocate of information sharing and partnering with the private sector.

So with that, please join me in welcoming Admiral Mike Rogers. (Applause.)

ADMIRAL MICHAEL ROGERS: Well, good afternoon. How is everybody today? Doing all right? And I apologize; I'm going to speak while you're eating, but please keep eating. We've got about 50 minutes or so. What I'll do is I'll speak for 15 minutes or so, give you a few thoughts from my perspective, but I'm really interested in an interchange and an exchange with all of you, because I am curious as to the perspective that you bring to this issue.

So why is Admiral Rogers, some admiral in the Department of Defense, why is he talking to the Chamber of Commerce and to the private sector about the idea of cybersecurity? Because as you heard from Marc, one of my takeaways in the 10 years or so that I have been involved in cyber within the department is that cyber is the ultimate team sport, and that if we're going to make this work, it's about creating a true integrated team and a set of partnerships that are going to make this a reality, that there's no one single technology that will enable us to guarantee 100 percent security of our systems, there's no one single group or entity that has all the answers, nor is there one single group or entity capable of executing the solutions that we need to do. It takes all of us working together.

Now before I get into so what do I think we need to do to work together, let me first start off by thanking the chamber very much, both for your kind invitation today but more importantly for the dialogue that over time you have been a part in helping to facilitate, because this is all about trying to talk to each other about how we're going to figure the way ahead here. To Marc, thank you very much for your kind words, but more importantly, to me, as a senior business leader, I want

to thank you for your openness to consider partnership, for your sense that cybersecurity is of direct impact and concern to the leadership of corporations. I will tell you, I can always run – it doesn't matter if it's a military command within the Department of Defense, whether it's a private company that I'm talking to. I can tell which organizations have leadership buy-in and those which do not. And when you don't have leadership buy-in, you are fighting with one hand tied behind your back.

So all of you here today with us who play a role of leadership within the business community or in the government, I thank you for your willingness to spend some time in your busy lives on an important topic, because as leaders, it's up to us to help drive the change that I think we need. This is much less about technology, to me, and much more about changing our culture.

Traditionally in our nation we have tended to view the private sector in one arena, the government in another, and the whole question of national security as something that is apart from that in some way. My argument would be cyber blurs the line between those three groups, between those viewpoints. I view the cybersecurity challenges we are facing as a nation, I view them as a national security issue for us, and how are we as a nation going to address a challenge that is not going to go away? If we think that this is a short-term phenomena, either of short duration or of relatively minor impact over time, I would argue we have missed the boat. I see this both extending for a significant period of time, and it will have greater and greater impact on us, both within the corporate sector, within the public sector. You know, as U.S. Cyber Command, one of our jobs is to defend the department's networks, DOD. And I will tell you, we are dealing with the same challenges with – every one of you are. Every day, there are groups, individuals and nation-states attempting to penetrate our DOD networks, and it's the same thing we're seeing in the corporate world.

Now you might ask yourself, so what is an admiral doing talking to us? I come here today really wearing two different hats, two different jobs, both related and both applicable to this idea of cybersecurity. The first, as commander of United States Cyber Command, we have three missions, one of which is particularly applicable here. First mission is to defend the department's networks. Second mission is to generate the cyber mission force, it's been called, the cyber team, if you will, that the department is going to use to execute its missions over time. The third one, and the one that really brings me here today, is if directed by the president or the secretary, U.S. Cyber Command is tasked with providing protection and support to attacks against critical U.S. infrastructure.

So I have to be ready, if I get an order, so how are we going to partner with our teammates? Because if there's one thing you learn in the military, you do not wait until the day of the crisis to suddenly say to yourself, boy, I guess we better do some training with each other or I guess we better understand what our partners need and what they don't need and what's effective for them and what is not effective. So we're in the midst of working collaboratively: the Department of Homeland Security, our FBI teammates, ourselves, other elements of the government, depending on the sector. We're in the process of partnering on how are we going to work through the details about how we're going to exercise and train with each other, so that when we're in the middle of that crisis, we really can make this work in real-time way.

The second hat that I wear, the National Security Agency, the one that quite frankly has gotten the most attention over the last 18 months or so, has two primary missions.

We have talked much about one of those missions, the foreign intelligence mission. Now in the cyberarena, NSA uses its foreign intelligence capabilities to attempt to understand what nation-states, groups and individuals are doing in the cyberarena against the United States.

The other mission set that NSA has that is also critical here is information assurance. NSA is tasked, under its information assurance mission, with not only defending Department of Defense systems as well as helping to develop the standards for systems; we do it with the federal government, and increasingly we find ourselves called on by our DHS and our FBI teammates to provide capability from our cyberexpertise to support the private sector. That is not going to slow down. That is going to increase.

You can pick up a newspaper, you can get on your favorite website, you can blog on whatever particularly interests you, you can go to whatever media outlet that you find is the best source of your news, and every day you will find something about a major cyberincident. This is not a short-term phenomenon.

Later today you're going to hear from Senators Feinstein and Chambliss, and I think the role that they are playing in attempting to generate legislation to help the private sector deal with the very real and very legitimate concerns about legal liability – that's critical for us, because if we don't help address that very legitimate concern, then I think for many of you – then I think that many of you in the private sector – that's a real challenge for you, for timely information sharing.

As Director Jim Comey, director of the FBI – in a private life, he was the general counsel for the largest brokerage firm in the United States and the general counsel for the largest defense contractor in the United States. And I will often ask Jim, so, Jim, when you were a lawyer working up with the board and with the C-suite, what was your recommendation? Generally, what kind of advice were you giving the leadership?

And he doesn't hide the fact that, hey, look, I would always tell them, be very mindful about the liabilities here, that you have to be very careful and that if you're not careful, potentially we, the corporation, are going to be setting ourselves up for major financial liability and potentially impact on market share and our business and our image. We have got to help remove those very

legitimate concerns and address them, because, in the end, what we have got to get to, I believe, is real-time automated machine-to-machine interface.

Now we need to clearly define in advance just what information are we going to share. Putting on my NSA hat, I do not want privacy information in this, because, quite frankly, it creates challenges for me, because under the law, any time I start dealing with privacy information for U.S. citizens, I had very specific restrictions on what I can do and cannot do with it, and very tight controls. And so my input to this has been we do not want privacy information here. That will slow us down. That is not what the focus of cybersecurity is.

What we need to share with each other is I need to be able to provide – from the government standpoint, putting on my hat as the National Security Agency, what I ought to be able to provide is actionable information that you can use, that gives you insights as to what's the malware you're going to see, how is it going to come at you, what are the indicators that you should be looking for in advance that would suggest to you that activity of concern is coming, and I ought to help you identify. So who's coming after you?

What I need from all of you is – I am not in your systems and nor do you want us in. So I need to understand what's the malware you're seeing, what have you done with your system configurations that worked, what didn't work, what did you anticipate, what did you not anticipate. And then collectively, between us, we need to share this, and we need to share it both across the entire sector, because, as you heard Marc say, which I really agree with, the insights of one can translate to the defense of many. That's a great value for us as a nation, and we need to come up with a system that enables us to do this in a real-time way. And the only way to do that, in my mind, is the legislation that you'll be talking about later today, as well as sitting down in a partnership and walking through exactly what elements of information are you comfortable with sharing; what do you feel you need from us, the government, and likewise I'd like to have the

same conversation with you. Here's the elements of information that would help us, and here's what we're comfortable with sharing. And I have got to do this – and I say this as an intelligence individual – I have got to do this in a way that you can actually use it, and not, well, I'm going to classify this at a level that really makes it unworkable for you. That's not going to help anybody.

So we'll be working our way through that process, but the key to it is going to be dialogue. The sector construct, if you will, that has been developed over time, I think, is very powerful. If you are not engaged in the sector construct in whatever area of business you are in, I would urge you to consider doing that. That helps us from a governmental standpoint because now we've got a framework within a particular sector that we can deal with.

We have tried at times trying to simultaneously work across sectors. I would tell you that has proven to be complicated. And what is applicable and important in one area, quite frankly, a different sector will look at us and say, hey, that's interesting but it really doesn't apply to me, or I'm not particularly interested in that, or that's not really how we are constructed. So the sector piece has been very powerful.

I think one of the things we need to do on the government is we have got to simplify this. I am constantly, as a part of that, telling my peers at the senior levels we have created a structure that is in part so complex that if you are outside of government, it is incredibly cumbersome and difficult to understand it, if we're honest with ourselves. That's not because people aren't working hard, and it's not because they're not motivated to do the right thing. It's because we have tended to do this incrementally over time.

What I think we need to do is a fundamental look at how do we structure the government side in a comprehensive way that makes your – from the private sector, makes it easier for you, and at the same time makes it easier for us. Because as you heard Marc say, many times right now this information is based

on – information sharing is based on personal relationships, personal knowledge, limited awareness; hey, I know this but I don't know what else is out there. That's true for all of us. We have got to try to simplify that. So that's one of the areas that we'll be working on.

With that, what I'd really like to do is – I tend to use questions as a way to try to make some broader points, and I'm much more interested in what's on your mind. So Ms. Ann, if you're ready, we'll do the questions.

ANN BEAUCHESNE: (Off mic) – have a moderated discussion. We have collected some questions earlier.

ADM. ROGERS: Can I steal one of the waters, or would that –

MS. BEAUCHESNE: Absolutely.

ADM. ROGERS: – will that screw the whole thing up?

MS. BEAUCHESNE: There you go, sir.

We collected some questions earlier from the audience, and I'll take a few of those and then we'll go to the audience as well. So get your questions ready. We have mics that will come to you, and if you could just identify yourselves and what company you're with before you ask your question, that would be great.

So one of the things we've been talking a lot about is how do we punish those bad actors that are stealing companies' IT and committing crimes? Some private companies are really becoming more vocal about the need to actively defend themselves against cyberattacks in the absence of state support. Is this something that the private sector should do or is this exclusively the responsibility of the government, do you think?

ADM. ROGERS: Well, first, we have a legal framework, and you've seen that. We have seen five individuals from a nation state indicted. So we have a legal framework for how we as a nation address criminal activity.

You know, I often get asked this question about, put another way, cyber-mercenaries. Well, should we go out – as a private sector, should we go out and hire individuals to conduct what we in the military call offensive operations, to try to stop, through the use of tools, nation states, groups or individuals from conducting these attacks against us? Again, that's something that's a broader policy issue, so we'll work our way through it. My input to all of you would be, be very careful about going down that road. It really potentially opens you up for a whole range of complications. And if you think you have legal liability concerns from a sharing (import ?), as a nonlawyer, I would only tell you, wow, think about the legal implication to this. But again, I'm not a lawyer, so I'd be the first to admit I'm not the smartest one about it. But in general I would just urge to be very careful about going down that road.

MS. BEAUCHESNE: And how do we give attribution to the so-called bad actor, as well? We talked about that earlier.

ADM. ROGERS: Again, that's where, to me, where this partnership becomes very powerful because that information sharing between us about, so, what is the attribution, and based on our confidence and our knowledge of that, what are the options that are available to us? That just – information sharing and increased knowledge gives us a whole greater range of options to consider.

Ms. Beauchesne: Another question was talking about definitions. We have the different domains – air, space, water. One of the questions was does the Defense Department have a definition for what constitutes use of force in cyberspace? And will that definition be the same for our activities in cyberspace and those for other nations as well?

ADM. ROGERS: So we have a legal definition under the law of armed conflict and the rules of law of warfare as to what is a military act, if you will. We are working our way through a broader policy debate about so what is the extension of those rules to the cyber arena. We have done – we have definitions for what is offensive versus what is – we call it a defensive responsive action and we have definitions for all of that.

The broader issue, I think, as a society we're trying to come to grips with is so we see all this activity directed against corporate networks, governmental networks, us as private individuals. What's the right response? I think the broader issue behind the question really is so what's the right response to this?

What I hope we can develop over time is a set of norm and rules that get us into an area where we have a much better definition of what is acceptable and what is not acceptable, and even into the idea of deterrence because right now, if you're a nation-state, if you are a group, if you are an individual, my assessment is that most come to the conclusion that this is incredibly low-risk, that there is little price to pay for the actions that they are taking.

I'm not saying I necessarily agree with that, but I believe that most look at it, and in light of that, feel that they can be pretty aggressive. That's not in our best interest in the long term as a nation for others to have that perception. We need to try to change that over time.

MS. BEAUCHESNE: I have one more. Folks, get your – if you have a question, please raise your hand, and we'll bring a microphone to you. For – we have one right up here. Tom Kuhn from EEI, can someone bring him a microphone?

Q: (Off mic.)

MS. BEAUCHESNE: All right. I'll ask mine first then. One of the things we were talking about this morning was the Chinese issue and Russia as well, and I think

it was McAfee that conducted a survey of cyber experts around the globe a few years ago, actually, when Cyber Command was first stood up. And they asked Americans who do you fear most, and Americans said the Chinese. And they asked everyone around the globe, and every other country said Americans. I was just wondering what your – what your thoughts are on that? (Laughs.)

ADM. ROGERS: Well, what we have clearly articulated as a nation is like every nation in the world, we use a broad range of tools to attempt to better understand the world around us. The biggest issue really we have raised is hey, in the cyber arena, we do not use the power of the nation-state to use cyber as a tool to gain insights into foreign private competition to then share with the private sector in the U.S. to gain a competitive advantage. We do not do that in the United States.

Now, many other nations in the world do. Some publicly acknowledge it and many do not. And you can see we have been very vocal with our Chinese counterparts that this is of concern to us, that we view this as behavior that is fundamentally incompatible with the relationship we want with the Chinese.

And so we continue to work from a policy perspective; you've seen the legal action we've taken. We work our way through it. You know, my only argument would be wow, I certainly understand it. As an intelligence individual, I would only tell you we are subject to more oversight, and rightfully so, because it is the way we are structured. We are more – we have more oversight congressionally and legally than most of my counterparts around the world.

That's not a complaint, that has served us as a nation incredibly well because as a nation, we want to be comfortable with what we are doing and why we are doing it. So I view that as a strength for us.

MS. BEAUCHESNE: Thank you. Tom?

Q: Admiral, Tom Kuhn, from –

ADM. ROGERS: Hi Tom.

Q: – the electric power sector and former Navy lieutenant. So it's great to see the Navy in charge here.

ADM. ROGERS: I knew that you were a good man.

Q: Absolutely. (Laughter.)

ADM. ROGERS: I knew you were a good man.

Q: In the electric sector, I think we do have a very, very CEO-led effort going on with the Department of Energy and Homeland Security with an ISAC, with the Electric Sector Coordinating Council, and we're focusing on tools and technologies, and you're providing us some very good detection technologies. I think we've got a lot of good information-sharing going on. Hopefully, the technologies will help us get more of the machine-to-machine stuff going and on response and recovery.

But I – on the latter one, since you are from the military and I think the one thing that we don't do all that well, maybe, in the private sector is, you know, the actual drilling of – and exercising of response and recovery plans. And I wonder if you might give your thoughts about, you know, how we might be able to do that more often. And obviously with the participation of our sister agencies in the government is a very important part of that equation.

ADM. ROGERS: Right. So if I could, I'm going to do that in two parts. First, Tom, it's not one you asked but it just reminded me. You know, one of the things I hear in the power sector – and in fact I was just down in San Antonio talking to NERC last week as a matter of fact. You know, one of the challenges I think in the power segment, and what I often hear from corporate leaders is: Hey, Admiral, you need to understand some of the constraints we work under.

We're a regulated industry. In order for us to generate income to make some of the changes we feel we need to do, we have to go to a regulatory body and we have to make an argument. And few of our citizens are interested in increased power rates, you know, as a vehicle to generate more money to address cybersecurity. And our regulatory bodies share this concern. So, first, my thanks to the power sector for, within those constraints, trying to push this as hard as we can, because I have some real concerns in this area.

In terms of the kind of idea about how do we train and practice with each other, one of the things – I have said this both internally within the Department of Defense as well as the private sector individuals and organizations I deal with – we have got to move from a focus where almost all our resources are focused on stopping from someone penetrating our networks to an acknowledgement that there is a likelihood that despite our best efforts we are going to fail. And therefore, remediation and mitigation starts to become really critical.

And I have had to – I mean, I have had to defend networks against a determined opponent who got inside the network. That's one of the best fights I ever had in my 33 years as a commissioned officer. I mean, it really was – each of us, you know, trying to anticipate what we were going to do to drive – how they thought we were going to respond, and us trying to drive them out.

And so, one of the takeaways I told our team in the department was, we have got to learn, how do you continue to operate a network even as you're fighting to defend it with an intruder? Because oftentimes, what I'll hear is, well, the answer is just shut down. And I'm like, you have got to be kidding me. Do you know what functions this network executes day-to-day? Do you know what this does on our ability to execute our mission? You know, I'm not going to take mission failure – I'm not going to do a self-imposed mission failure just by shutting them down. That is not the answer in most cases.

So I think we need to shift to a focus on remediation and mitigation. How do you fight through a network that's been compromised, and one of the things that we're trying to do, as I said in my comments, is, on a sector-by-sector basis, how can we look at doing that? Now, one of the things I have said is – and these tabletop exercises – this coordination, this coordination should not be done at my level.

Where we really generate value is at the level of the men and women who are actually doing the work. That's what we've got to get to. It's not myself, cabinet heads, agency heads meeting with CEOs – not that that's not a part of it, but that's not the level we've really got to bore down into. We've got to get to an actionable level, and so I'm always looking to the private sector. How can we help with that, and what's the right level for you? If I say "actionable level," what does that mean in your construct? I know what that means in the Department of Defense; I know what that means in the government, but I don't know, necessarily, what that means in your structures.

I'd be curious what you think, Tom.

Q: Follow-up here. What it means is really at all levels, because, you know, on hurricane response, for example, we're pretty good at the response recovery, and also have a pretty good mutual assistance program, so – where companies come to help each other. And Hurricane Sandy, we got together an army of 67,000 people from all around the country with the help of the military to get that done.

So that level – it is very important to have those (trills ?) and tabletops, and we've done one of them pretty well. The other part of it, though, is, during a cyberattack, there's going to be a lot of things happening at the upper level in terms of coordination at the highest levels of government, in terms of media and Congressional interest, or governors and other folks. So there's got to be a lot of coordination. So there's really a couple of different tabletops that have to be done

– one at the operating level, I think, and also, one that would maybe practice coordinating some of those kinds of activities as well.

ADM. ROGERS: No, I would agree with you, and I apologize if I came across as not embracing that idea. I mean, clearly, this is such a multifaceted problem set. There are so many different levels and complexities to this. We've really got to step back and look at this holistically. It's not just the technical piece. And I see so many people who just want to focus on the technical piece of this. And I'm thinking, we've got to think much bigger than this.

What else for me?

MS. BEAUCHESNE: Yep, so following up on that, more of the human component. And we were talking about, even back in 1994, Time magazine wrote a story about the Internet, and it was brand new. No one had heard about the Internet. They put it on their cover, and they wanted to actually describe what it was. And if you think about it, all of the terms that have come into our vernacular now – Twitter and YouTube and blogging and tweeting, I'm just – you know, the question is, what will be the next generation of cyber threats that we will face, do you think?

ADM. ROGERS: Well, I think, clearly, the next big arena is going to be – you know, the digital hand-held device really becomes the next major frontier, both because it's exploding in its application and use – (I mean ?) increasingly, look at – (inaudible) – whether it's from business, whether it's in the military, whether it's us as individuals, look at the series of actions and steps that you're taking in your everyday life, corporate, government or individual, with the mobile hand-held digital device. That increasingly is just becoming the norm. And that, to me, is the area that I look to, you know, as I look out five, 10 years. That's where – that's what concerns me. We've tended to focus on fixed networks, large, you know, corporate-based, governmental-based. Those aren't going to go away, but the hand-held digital is the next area of concern to me.

MS. BEAUCHESNE: And the Internet of things, and the wearable apps and that kind of thing.

ADM. ROGERS: Right. And I consider the Internet of things all part of that digital beast.

MS. BEAUCHESNE: Other – question right over here. Just wait; they'll bring you a microphone.

ADM. ROGERS: And I apologize, with the lights I can't see you so well.

Q: Yeah, I hear the lights are pretty bright in your eyes. I'm Susan Morrow (sp) with Pepco Holdings, the power company here in Washington, D.C.

ADM. ROGERS: Hey, Susan.

Q: And I guess my question – you know, in the energy sector, we don't differentiate between physical threats and cyberthreats, and we actually drill with the assumption that they'll probably do both at the same time if it's a sophisticated attack. And to be quite frank, the military's response in its own protection seems to be focused on isolation as the tactic for dealing with the idea of the grid going down. And I wonder if you could talk to that a little bit, because I think – you know, as tempting as isolation is as a strategy for response, it also, you know, potentially makes security a lot more difficult if you have little webs and individual grids all over the place. So I don't know if you could talk maybe a little bit about isolation versus integration.

ADM. ROGERS: So isolation works at a very tactical level for a very immediate, short-term period. It's not, in the long run, a comprehensive, sustainable strategy. It's just like this idea of, well, I'll just shut down. That's how I'm going to make it go away. I'll just shut the network down.

It's not that it's a bad thing at the tactical level, so to speak. You know, if you're looking at a base, you're looking at an installation as opposed to an entire grid or sector – geographic sector construct. But in the long run, I think the right answer for us is going to be, again, rather than isolation, how do we do something in a more integrated way?

Isolation to me is also very difficult to sustain over time as a strategy, particularly if you have high power requirements. As the director of NSA, we have huge power requirements, so this is something I – for me, pay a lot of attention to because power is a big concern for us because we're a huge consumer of electrical power.

But I agree with your fundamental premise. I think the challenge then becomes how can we, starting from that sector perspective, have a conversation about what's the right response strategy here, and are we really comfortable with this idea that we want to go to this isolation kind of way to do business as a broader strategy? I don't think that's the best response in the long run.

Thank you, Ms. Susan (sp). Thank you.

MS. BEAUCHESNE: Matthew (sp)?

Q: Ann, thank you.

Admiral, I've got a question about kind of the baton hand-off, as I've heard some members kind of ask. So likewise with the response and Tom's question about tabletop exercises, you know, say a business is sharing information. They're using a framework tool or a risk-management tool, like the framework. And they're dealing with an adversary that outstrips their abilities to keep pace. We know that there are partnerships with DHS, other agencies and departments. When would NSA step in? And what's the policy thinking there? What would that look like?

ADM. ROGERS: Well, first, I would argue the most likely scenario in that regard is probably U.S. Cyber Command and the DOD, vice the National Security Agency. As I said, one of our three missions at U.S. Cyber Command is, when directed by the president and the secretary to provide capability to defend critical U.S. infrastructure. Now, our role to do that will, quite frankly – our mission will be to attempt to interdict the ability before it ever gets to that U.S. network, before it ever gets to that U.S. company. That's our primary strategy and that's what DOD brings to this.

A subset of our strategy on the U.S. Cyber Command side is, if we should fail in that regard we have also developed some defensive response capability that we can deploy to partner with DHS, the FBI and the private sector about – so it goes to Tom's question – about, so, how do you remediate, how do you mitigate? If you failed in a breach, so to speak, how do you remediate and how do you mitigate? That's really the U.S. Cyber Command side. Now, that's a legal call – because, again, have to be tasked. And that's what the president, you know, requests the secretary of defense to do.

So there's a policy debate there. There's a legal debate there. It's one of the reasons why, in my initial comments to you, I talked about, this is a national security issue to me. When viewed as a national security issue, then the capabilities of DOD and their application, you know, are very much in keeping with our broad policy and legal structure as a nation. If we're going to view this as purely a private sector issue, you know, then traditionally we have, well, hey, do you really want DOD, or by extension the broader government, involving themselves in this? That's where I think looking at this from a national security perspective is very important.

And there will be a discussion about, do we focus on critical sectors? Is it any private entity? For the federal government we have defined approximately 16 segments as being critical infrastructure whose loss would have significant – or

degradation would have a significant national security impact. So my training, what we are developing at U.S. Cyber Command is so be prepared to apply capability in those 16 segments if directed by the president and the secretary.

Q: OK, thank you.

MS. BEAUCHESNE: So, Admiral, October is Cybersecurity Awareness Month.

ADM. ROGERS: It is?

MS. BEAUCHESNE: Yes, according to the Department of Homeland Security it is. And as you may know, the chamber has embarked on a cybersecurity outreach and education campaign and over the past few months have been going around the country. And as you can imagine, very different audiences. I think a lot of the folks here in Washington are well-versed in the cyber framework. When we were in Phoenix and Chicago, some of them hadn't yet heard of it. So we're spreading the word with that –

ADM. ROGERS: Thank you.

MS. BEAUCHESNE: – and working with the White House and DHS and NIST. I guess the question to you is, so that's great; that's a campaign. You know, we've got a month designated in the fall for – what else do we need to do? I mean, you look at the ALS ice bucket challenge and how quickly that went viral and everyone was donating money. What can we do to jumpstart people paying attention to cybersecurity more?

ADM. ROGERS: I think one of the issues often – I'm sure it's not unique to us. I'm sure many of you have the same discussion. So what's the tipping point? What does it take when it gets so bad that we finally say, OK, enough; we've got to get the legislation piece out here, we've got to put those partnerships in place? Hey, look, the status quo is not working for us.

For whatever reason, it doesn't appear yet that we perhaps have reached that point broadly across society, in no small part, I think, because for many of our citizens it hasn't reached a true pain threshold. So someone steals your account information, steals your credit card data, charges on that card. Right now as citizens, if you report this to your bank, you know, we're not paying a price. The corporate sector is assuming the liability; they're covering it. The point I'm – I often think about is, so once this becomes something that really impacts a broad swath of our citizens in a very real manner, that impacts their daily life and their ability to do what they want when they want, you know, then, watch for a whole shift in the way we're talking about this.

Now, my frustration is, look, it shouldn't take a disaster, so to speak, to tell us that you can see this coming. Every one of us intellectually knows that this is a significant national security issue that is not going away and that is likely only to get worse. So we can either deal with this now in a collaborative, professional way or we can wait until we get hit with a two by four right across the forehead. I don't like to get hit by two by fours, I found that to be a very painful experience. I would much rather we have a dialogue with each other about so – and then move from the dialogue to the concrete steps as to how we're really going to make this real and how we can work comfortably between the private sector, government – and a broad swath of government because one of the comments I make is right now, we are asking the private sector to withstand the efforts of nation-states against them. And that is acting – asking a lot of the private sector.

And I think you've seen this reflected in what we're trying to do as a government, that we've come to the conclusion that this is about partnerships and that we have got to be able to provide government capability and capacity to support the private sector and that, likewise, we need the private sector to provide capacity and capability to make this work. It's not either/or, so for those who would argue, well, that's a private sector function, they ought to deal with this or those in the private sector who would argue, this is governmental function, they ought to go

deal with this, I think the reality is between the two viewpoints. We have got to work this collaboratively because again, there is no single technology, there is no single source of intelligence or insight that will clearly tell us in and of itself exactly what we're seeing. It takes a partnership to make this work. And you have information that I need and I think I have information that can be of value to you.

MS. BEAUCHESNE: Good. Well, you have not just one of the toughest jobs in D.C., I think you have two of the toughest jobs, as the cyber commander and the head of the NSA.

Just a question. You know, what do you think your biggest challenge is and what are your – where do you go from here with the Cyber Command and working with the private sector? And how can the chamber be helpful to you.

ADM. ROGERS: So for U.S. Cyber Command, my biggest challenge is creating a culture and building the framework for the future. So as a matter of act on Friday, the 31st of October, United States Cyber Command celebrates its fourth anniversary. So we are four years old as an organization.

In the scheme of things within the Department of Defense, four years is not necessarily a long time, so there's a lot of organizations that have a much longer history than we do. But my challenge at U.S. Cyber Command is create that work force, build the operational concepts and the command and control as to how we're going to employ it and then exercise it with our partners both within the department and outside the department as to how we're going to make this work down in the execution level of detail.

What you need from us, what we need from you. How we're going to share it, in what format, what are the elements of information that generate value? Because the answer to this problem isn't well, I'm just going to give you everything we

have. I don't want that from you and I don't think you'd want that from us, because we can bury each other with data.

I'm always looking at putting on my intel hat. Data is interesting, but what I really care about is insight and knowledge, and I use data as a tool to get there, but data in and of itself is not the end-all, be-all. What we've really got to share with each other is knowledge and insight.

MS. BEAUCHESNE: Great. We've got a question right here. Wait for the mic to get to you, please.

Q: Hi. I'm Nick Ahrens with the Retail Industry Leaders Association.

ADM. ROGERS: (Inaudible) – I apologize.

Q: Hi. I'll stand, I guess. Sorry.

ADM. ROGERS: Thanks. It's only because I can't see through the lights so well.

Q: Sure. So my question for you is actually – you've talked about the importance of cyber-information sharing, and we're going to hear a little bit later about sharing legislation. And one of the big criticisms by some, by privacy advocates, particularly, is that, you know, these bills allow, frankly, you to get the information, and they would like to have some use limitations. How do you see – how do you get around that or how do you –

ADM. ROGERS: Well, my first comment is let's have a very clear definition of exactly what you're providing us. I don't want privacy information. It creates challenges for me. It slows me down. For this mission set, not a good thing for us. That's not what I'm interested in. What I'd like to have is a discussion about so just what is the information we want to share with each other, and what is the value that that information generates? But this idea that inherently you can't trust, fill in the blank, that is a recipe for disaster for us, if we don't trust each other.

So among the things we need to address is, so what are the controls and the oversight mechanisms we're going to put in place? What's the role of civil liberties and privacy? What's the role of inspector generals? We have lots of mechanisms, both in the private sector and in the public and governmental sectors. We have lots of mechanisms about oversight and control of information, and we need to make that a part of this.

I'm not interested in anybody writing a blank check for either U.S. Cyber Command or the National Security Agency. And I bet you my FBI and DHS partners would tell you the exact same thing. And remember, DHS is the leader here. In military jargon, they are the supported commander and we are supporting them under either hat, U.S. Cyber Command or NSA. We work through Department of Homeland Security. We partner with others in the federal government in addition to DHS: FBI, depending on the segment, Treasury and Energy, if we're working the energy segment. I mean, we partners (ph) with others but U.S. Cyber Command, we're not the lead here. The National Security Agency, we are not the lead here. We partner with others.

MS. Beauchesne: Thank you, sir. We have time for one last question.

MR. ROGERS: Well, there's one – (inaudible).

MS. Beauchesne: Can you wait for the mic to get to you and introduce yourself.

MR. ROGERS: You are in the far reaches, here, so it'll take a moment.

Q: There's a – sorry, Tal Kopan, with POLITICO Pro Cybersecurity. There have been some reports recently about employees of the NSA working part time –

MR. ROGERS: I'm sorry, could you say the first part, ma'am?

Q: Yes. There have been some reports recently about employees of the NSA working part time in the private sector, some former employees going on to the

private sector. How is that affecting morale within the NSA and is there any concern about, you know, that particular relationship with the private sector and classified information sort of jumping from within the borders of the NSA?

MR. ROGERS: First, we have a formal set of processes that must be applied when individuals are going to do something in addition to their NSA duties. We review that consistently over time and when circumstances change. What was acceptable at one point, we'll say, hey, that -- that's not acceptable anymore, the circumstances have changed the nature of the relationship between the outside entity and us is different. So we do that on a recurring basis.

For some, it's as simple, for example, as someone with a language background says, hey, look, I want to use my language outside NSA in a contractor basis because I think it'll increase my skills. And so sometimes we'll say, yes, that makes sense. Sometimes we won't. In terms of, you know, the flow of partnerships and information back and forth, I have been very public about saying, for the National Security Agency, I would like us to create a model where members of our workforce don't necessarily spend 30 or 35 years working directly for us, which right now is -- has been a historic norm. It is amazing the employees that I will talk to, when I say tell me how long you've been with NSA, 30, 35 years, 38 years. I just said goodbye to an employee after 50 years.

What I've talked about is, particularly given the state of technology, we have got to create a world where people from NSA can leave us for a while and go work in the private sector. And I would also like to create a world where the private sector can come spend a little time with us, because one of the challenges, I think, as a nation that we're dealing with -- and you've seen this play out over the last, you know, year or so in particular -- we talk past each other a lot because we don't understand each other.

The NSA culture and experience is necessarily optimized to understand, you know, concerns that -- many of which are very valid -- from our IT corporate

partners. Likewise, are many of the individuals we'll work with in the corporate world don't really have an understanding of us. And I'd like to see what we can do to try to change that because I think it'll produce better outcomes for both of us and it'll serve us better as a nation.

So thank you very much, ma'am.

MS. : Thank you, sir. Thank you for time. Thank you for all that you. The U.S. Chamber of Commerce look forward to working with you and your team in the future. And we hope you'll come back and hope it won't be next October.

ADM. ROGERS: Thank you. If I could, let me conclude by where I started. I thank you for taking time from very busy personal and professional lives to be part of a dialogue – won't be just today, won't be just tomorrow, next week, next month – but being part of a dialogue about what have we got to do to address a really foundational challenge for us as a nation and, I would argue, for our friends and partners all over the world.

Cyber does not recognize geographic boundaries very well. So the idea that we're just going to deal with this in America, for example – I don't think that's a winning strategy for us. We can learn great insights both internally with each other, but also from our partners overseas as well. But it all starts with a willingness to have a dialogue with each other and a willingness to be open with each other, and not starting from a position of, well, gee, you know, you're in the private sector, and you're all about money. So I don't know that I can trust you as a military. I'm like, what?

Or, the private sector saying, hey, you work for the government, and I don't know that we can really trust you. That is not going to get us where we need to be as a nation. That is not going to provide the protection that our society – whether you do it in the private sector, government, or for us as private individuals – that is not going to generate the outcomes that collectively we need. This is a team sport

that will take all of us, and it starts with a collaborative, open relationship, and a willing to be – a willingness to be transparent and open with each other.

So I thank you very much for that, and you have a great day.

MS. BEAUCHESNE: Thank you. (Applause.)

(END)