NATIONAL SECURITY AGENCY DIRECTOR AND U.S. CYBER COMMAND COMMANDER ADM. MICHAEL ROGERS DELIVERS REMARKS AT THE BILLINGTON CYBERSECURITY SUMMIT

SEPTEMBER 16, 2014

SPEAKER: NATIONAL SECURITY AGENCY DIRECTOR AND U.S. CYBER COMMAND COMMANDER ADM. MICHAEL ROGERS

[*]

ROGERS: Thank you very much for taking time from your busy lives to focus on something I think is very important to us as a nation. This idea of how do we achieve true security in the cyber arena in the face of a constantly changing environment, and one in which the level of activity directed against our systems just continues to grow.

And I don't care if you're in the U.S. government, I don't care if you work in the corporate sector, I don't care if you work in the academic world, there is nothing but increased activity out there.

Now, one of the things you heard Darrell tell you is that -- and what really drives me being here today with all of you is the idea to me that partnerships and relationships are the key to our success here. That there is no one, single enabling technology that will overcome these challenges, nor is there one single all-knowing group that has access to all the insight, information, and technology necessary to achieve success in this mission domain. It's all about creating partnerships.

Now, how many of you who are associated with the court would associate yourself with the corporate sector out there? Give me a show of hands.

How many of you come from the academic environment?

How many of you work for government, whether it be federal or state. Up there.

How many of you work in the media?

How many of you work in the thinktank world, or academic thought, so to speak?

The reason I asked you to show your hands is one of the reasons that I wanted to be here today was I very much appreciate the diversity of the expertise that tends to be resident at gatherings like this. Because in the end, it's our ability to harness that expertise.

Now, the topic is cyber resiliency. So, what does that mean? Now, to me, as a uniform, in my culture, resiliency is the ability to sustain damage or degraded mission impact, and yet still achieve the desired mission outcome. That's what resiliency is to me as a uniform as a member of the Department of Defense.

I would argue, in the cyber arena, for purposes of this discussion, resiliency becomes how, in the midst of potential penetration and degradation, do I continue to achieve my desired outcome, whether that's corporate, academic, whatever, and at the same time have confidence in my systems, the information

they contain, and their ability to execute the mission or achieve their desired outcome.

That's an important vision of the future, to me, because as I look back and only speak for myself, as I look back on my journey in cyber and the kinds of things that I tended to focus on, my experience is that most organizations have tended to put their cyber-defensive resources, intellectual capital, and focus on the idea that "I should spend the majority of my time stopping people from penetrating my networks."

And my concern, increasingly, is when we watch in the world around us is, and particularly as a warfighter, resiliency is all about, "despite my best efforts, I'm going to sustain some level of damage or degradation of capability, so what am I going to do keep operating? What am I going to do to fight through that?"

And increasingly, I tell organizations, and that includes the uniformed segment in the department of defense, that we have got to not only focus on trying to ensure that no one gets into our systems, but quite frankly, you have to assume that someone will. And the question becomes, how are you going to operate and remediate at the same time? That's resiliency to me, the ability to do both simultaneously.

And so one of the things I always urge partners to think about is what does it mean to truly operate and remediate at the same time? Because I watch in my own culture at times where it's only -- where the answer is, "I'll just shut down. We'll just pull the plug, we'll go dark. We'll figure out what's happening, and then we'll bring the systems back up."

And I tell myself, and I tell the team, "so tell me how we're going to achieve the desired mission outcomes if we're just going to go dark?" We don't do that in any other mission set that I'm familiar with in the Department of Defense.

When I, as you heard in the introduction, I started as a surface warfare officer. A ship-driver in the United States Navy. And I can well remember as a junior officer, I not only spent a lot of time figuring out how do I employ the combat systems capability of those ships I was on, I spent a lot of time focused also on, even while I was doing that, what do you do when we have fires? What do you do when we have flooding?

What do you when you take damage? You don't pull out of the fight. You keep doing both, simultaneously. And we spent a lot of time, energy, we set up our systems, we set up our infrastructure. We set up the way we allocated people and their skillsets, all with the idea that despite our best efforts, the probability or possibility as a minimum existed that we were going to sustain damage. And that in doing that, we still had to keep fighting.

So, what do we do in the cyber arena to do the same kind of thing?

Because quite frankly, I watch organizations and you see this in some of the major compromises that we're all observing in the commercial sector right now, but I would argue they're much broader than just the commercial sector. And you watch organizations you know, literally taking months to try to remediate.

I've deal with that in my own experience within the Department of Defense, trying to deal with major degradations, major penetration, and keep working, keep the systems up, but at the same time, trying to fight through it. It was amazing, the cultural change the first time I had to deal with this in my professional life.

Just the mental gymnastics about trying to get a team to think about what does that really mean, and how do you truly make it work? The key in my mind are a couple things. Number one, leadership buy in. Whatever organization you're a part of, the first point I try to make to people is defensive capability and success in cyber is predicated in no small part as is any other segment, is leadership's buy-in.

A recognition and a buy-in from the leaders of the organization that number one, a recognition that this is likely to happen. Two, a sense that hey look, as a result of that, there's some things we need to do, whether that's investments in financial allocations, whether that's how do we create the right workforce.

And it's not just the cyber piece, it's not just your information technology individuals. The argument I try to make in the Department of Defense is this is so foundational in some ways to the future, it's about all of us. It's not just, hey this isn't my issue, that's what my tech guy does for me. I don't think that's going to get us where we need to be in the future.

At U.S. Cyber Command, in order to try to work our way through this, we're really focused on five different things, if you will. The first is, how do you build a truly defensible architecture in which redundancy, resiliency, and defensibility are core design characteristics?

If your networks are anything like ours, they reflect a very different historic view about what's the role of a network, what's the importance of the network to my operation, and what's the right level of investment?

And the idea that you can just bolt on, if you will, defensive capability, I think is a really losing strategy, particularly if you're trying to do it to scale.

So, in the department, we are focused at the moment on spending a good deal of time about how do we truly create something that is defensible, you know, in which redundancy, resiliency, and defensibility were built-in from the ground up.

The second thing that I'm focused on within the department is how do you create true situational awareness when it comes to the cyber arena? That as a decision-maker, you truly have a picture of what is going on in your networks.

My simple analogy to most of my teammates is look, tell me how you defend something you can't visualize?

As an operational guy, in my service, I am used to the idea of walking in to a nice, darkly-lit command center with some beautiful visual displays that very quickly enable me to use symbology, colors, geography, to very quickly assimilate a lot of data and start to make some decisions about so here's what's really going on out there, and this is what I need to do.

You can't do that if you don't have a level of awareness of just what is going on in your networks, and the ability to visualize that, and the ability to sense what are the implications for the activity that I'm observing, and quite frankly, sometimes the activity that I'm not observing can be almost as valuable to you.

The third thing I'm trying to work on is, so how do you create those partnerships, those relationships, and in our world, those operational concepts about how we're actually going to do this. This is not a pick-up game. it has largely been, to date, in many areas across, and that doesn't matter whether you're government, whether you're in the commercial sector. In some ways, particularly on the defensive side, I would argue that the defense -- the cyber defense has largely been a pickup game. I don't think that's going to get us where we need to go.

If you look at the scale of the challenges we're facing; if you look at the proliferation of threat we're facing; if you just look at the changes in malware and the tactics, techniques and procedures we're seeing, it is amazing to me. I mean, there shouldn't be a doubt in our minds, there are a lot of groups out there, individuals, nation-states who feel that this is an area worth investing in because it achieves positive outcomes for them if they can penetrate systems.

Whether that's because they want to steal intellectual capital, which we're certainly seeing some nation-states do; whether it's their view that by stealing intellectual data, as I said, whether it's they feel that by stealing credit card information, the particulars on business activity -- I mean, there is no doubt -- there shouldn't be any doubt in anybody's mind that this is generating billions of dollars in revenue for individuals, unfortunately, as well as costing companies, the government, you know, billions of dollars.

This is not a small problem. And it's not one that's going to go away. And those of us that would think, "Well, maybe this is just something temporary; technology is going to catch up." I just don't see it that way. I think this is very foundational to the future. And again, it's one of the reasons why when this first came up, I said, "Hey, look, I would be glad to sit down and talk." Because I, quite frankly, need your help. Those partnerships are critical.

The fourth thing that I said that we're really focused on is, you know, working the authorities piece. Because certainly as United States Cyber Command, element within the Department of Defense, as the director of the National Security Agency, an organization where it's foreign intelligence mission tends to get the majority of its attention, what really brings me here today as the director of NSA is our information assurance mission where NSA is tasked to provide its expertise in the cyber domain to assist on the defensive side.

We do that with entities within the U.S. government, within the Department of Defense, partnering with DHS and the FBI and others. We do that in the broader commercial sector to try to help generate knowledge and solutions about what activity is going out there. It doesn't get much publicity, but it's a great aspect of the NSA mission, because NSA really brings some amazing technical capability that we try to apply to support others achieve a better defensive posture.

And then lastly: How do you create the workforce that's going to help you achieve this vision of cyber resiliency? That's the fifth and final thing that

I spend a lot of time on. The Department of Defense right now is committed to the idea that we're going to build a dedicated workforce of about 6,200 cyber professionals. One segment of that workforce, if directed by the president and the secretary of defense, allocated to U.S. Cyber Command has been tasked with the mission of on-order, be prepared to provide defensive support in the defense of critical infrastructure in the United States, partnering with DHS, with FBI, with the corporate structure, with others in the federal government. That's a big mission set for us, and to do that, it's all about partnerships.

And we need to build on those partnerships. I'm not interested in just what I would consider to be fairly superficial relationships. My attitude is the culture that raised me as a uniform is you must train like you fight, and you don't wait until the first day of conflict to decide what do I do today. You build those relationships. You exercise those relationships. You work out how you're going to share information. You identify what information do you need; what information do others need from you.

You work through what are the paths we're going to use to share that information. How is that information going to flow? In what format? What are the critical centers of gravity in my network that -- within that critical infrastructure, for example? And if the federal government is going to apply capabilities to support the defense of that critical infrastructure, what's the best way for us to do it? What really matters within that network, within that architecture?

That is not a discussion that I want to wait until game day, as it were, to suddenly start to have. Hey, I'm here to help fill in the blank -- the financial sector, the power infrastructure. I'm just curious. Could you guys tell me how you're structured?

That's not really the discussion we want to have when it's hit the fan and the direction for us has been, as U.S. Cyber Command, to provide our capabilities to try to support that effort.

But bottom line in the end, it's all about partnerships and recognition. I always tell my team the first step in solving any problem is recognizing the problem. And I think we need to all recognize that there shouldn't be any doubt in our minds that our information systems are collectively under assault by a wide variety of actors who are interested in penetrating those systems for a variety of different reasons, but in the end, they are interested in penetrating our -- our systems.

And that's not a good thing for us. What happens to us when we lose confidence in our systems, when we don't believe the data that we're looking at? You know, we've seen a lot about denial of service kinds of things, others attempting to forestall the public linkages between our organizations and the public, for example, on the use of -- if you want to go look at your bank account, you want to log in on the website for your particular financial institution, you want to put in your password and your logger ID, and you want to go look at how much money do I have in my account, I want to move money around -- and you suddenly can't do that because that interface has been severed, is gone.

Think about the ability to do that on a massive scale and do it for a longer period of time and do it in ways much more than just that connection. That ought to concern all of us.

With that, what I thought I'd do is -- I'm much more interested in some ways what's on your mind. So, Tom, if you're ready, I'm ready to do some Q&As.

(CROSSTALK)

ROGERS: All right.

STAFF: If I could have questions, please, from the audience. And I would like to start with one.

You talked already about the cyber workforce at U.S. Cyber Command. And you're aiming to increase the cyber force to 6,000 strong. Could you describe -- give us an update on that and the importance of it to U.S. Cyber Command?

ROGERS: So, the Department of Defense committed to the idea of a dedicated cyber mission force of about 6,200 or so individuals that would really have three primary mission sets, if you will. The first one I mentioned, you know, if directed by the president and the secretary of defense, we would be prepared to provide defensive capability in the support of critical U.S. infrastructure. And some of you are aware the U.S. government has actually identified 16 different segments as, quote, "critical infrastructure."

The second mission set is use that workforce to defend the Department of Defense's information network or networks.

The third segment of that force is designed to provide operational commanders with a full range of cyber capabilities. Those operational commanders, primarily combatant commands -- Pacific Command, Central Command, Transportation Command -- there's nine -- as well as a measure of capability that the services will also be using.

So, 6,200 people designed to do those three primary mission sets. We are on a timeline between fiscal year '13 and fiscal year '16 to complete that build-out. So we're about halfway through. It's hard to believe, but we're less than two weeks away from the beginning of fiscal year '15. So we're working our way through that.

And there's not an insignificant amount of challenges about how do you build a truly dynamic force that's capable of changing as technology is changing; that's capable of staying abreast; that's well trained; that's got a sound basis of operational concepts about how we're going to work.

This is new for the Department of Defense, just like everybody else. So we're working our way through this journey just like our corporate and civilian teammates, as well as our teammates across the broader U.S. government. I feel pretty good that we've got a good vision. I'm very comfortable with the construct. I'm going to work our way through it.

QUESTION: Admiral Mike Brown...

(CROSSTALK)

ROGERS: This is a ringer. This is Admiral Mike Brown. Admiral? Admiral.

QUESTION: Admiral.

ROGERS: Your Admiralness. Yes, Your Admiralness.

(LAUGHTER)

QUESTION: Mike? Mike.

(LAUGHTER)

QUESTION: You mentioned and clearly articulated your priorities in how important partners across the environment -- the public sector, private sector. What's your vision for doing that training, (inaudible), to be able to understand what the capabilities and capacities of all the partners are?

ROGERS: The argument that I'm trying to make with my broader teammates out there -- DHS, Treasury, FBI -- is we ought to start with a series of exercises. Let's focus on a particular sector. Let's create a model that we can then use to bore down deeper into that sector and then apply it more broadly.

In fact, to be honest, I'm meeting later today with my counterparts in another hour or so after this, and that's exactly what we're going to be going over.

The three elements that we're going to talk about -- how do we create a true exercise framework? Again, we're all victims of our cultures. As a uniform, we use exercises as vehicles to replicate what we think are the most likely real-world scenarios, and then how we're going to have to deal with it. And we often try to put a notional opponent in who doesn't always go by the script we think they're going to go by to challenge us to think about how we're going to need to do this differently. That's one element.

The second element we're trying to do is working the specifics on information-sharing. You're all aware there's -- I'm -- and I have said this publicly before -- was in my confirmation hearing as U.S. Cyber Command -- I'm a big advocate that we need cyber-sharing legislation. Because as much as we have tried to do this on a voluntary basis, when I look at the level of activity that we're seeing out there versus what I'm seeing shared with us, I just scratch my head and go, "Wow, we got a huge delta between what I'm seeing out there and what people are telling me they're seeing out there." We need to change that. And I think in fairness to our partners out there, you know, clearly, there are some very legitimate liability concerns. So, my view is, look, we can use the law to try to help them do that. And that's the focus of the Hill. They're trying to work their way through that. And hopefully, we'll achieve something in the near-term.

And third and final area -- I apologize -- this is where I'm drawing a blank. The third area we're going to focus on -- oh, I know what it was. So, when we say we're going to defend critical infrastructure, exactly what does that mean? And what exactly should people expect from the U.S. government? I said, look, we got to be realistic. And we got to make sure our partners understand just what they should expect from us, just as we need to understand what to expect from our partners. Because -- and then it's not one of the three areas, but just for me personally, the other area that I'm trying to work is, how can we continue to refine how the federal government will provide support to the commercial sector in other areas. Because I say, look, if we're honest with ourselves -- if I'm outside the federal government and I'm watching us, we can be confusing as heck.

So, what's the difference between FBI and Secret Service on the law enforcement side? And do you want me to go to DHS? Hey, but I hear NSA and Cyber Command have some amazing capability. shouldn't I be going to them? You know, what I tell Secretary Johnson, Jack -- Secretary Lew and Director Comey is, imagine if you were on the outside watching us. This has got to be confusing as heck.

So, we -- one of the areas that I've -- I'm trying to work on as part of a broader team -- how do we truly make this simpler and well articulated so the outside world knows exactly who they go to to pass information?

(UNKNOWN): Thank you very much, Admiral Rogers.

Two points for those who want to ask questions. Please, if you could raise your hand, and we'll come to you. Also, there are note cards in the middle of your table. If you'd prefer that they use that -- and if you prefer to ask questions instead using the note cards, please do that.

QUESTION: Good morning. Admiral. Mike Orfini (ph).

ROGERS: Hey, Mike.

QUESTION: Another Mike. Another Navy guy -- with Northern Trust.

Your comments are all -- they tend to be U.S.-focused. And as you know, the cyber attacks -- they don't stop at the border.

ROGERS: Exactly.

QUESTION: So, can you just address some of the international cooperation that we have or that we're trying to achieve, either through our war gaming exercising, or just planning? Thank you. Jack (ph).

ROGERS: And that's a very good point. Thank you.

One question I forgot -- when I asked all of you to raise your hand initially, you know, one question I meant to do but I didn't do -- who is here from a foreign perspective -- non-U.S.?

Back there, good.

Thanks very much. Because one of the -- as you highlight -- cyber knows no geography. It doesn't really recognize the boundaries in many places that we put around the globe. And that's certainly true in the military, where we have tried to divide the world in some -- along geographic lines at times in terms of trying to identify and structure ourselves to best support our needs and executing our mission. And cyber doesn't always recognize that geography. In fact, often seldom does.

For me, it was -- as U.S. Cyber Command, my partnerships with foreign entities large -- there's probably 15 to 20 nations around the world right now that we're working pretty closely with in the cyber side, in the uniform world, if you will. And (ph) talking to DHS, Treasury and others, you know, the argument I have made is, so as we create this capability in the U.S., then one of the things we're going to need to think about is, how does it scale to

something larger that supports a broader set of people outside the U.S. potentially?

Because for those of you in the corporate world, particularly in the larger corporate segments, you don't necessarily recognize the purity of a U.S.-only challenge either. And I'm sure you are dealing with this in the financial sector.

So very clearly we're in the very early stages of that. The policy side is working very aggressively there, if you are at the White House, if you are State Department, we're part of a much broader international dialogue on the cyber side about how do we develop cyber-norms, rules of behavior, broad structures for how we're going to deal with the future in cyber.

You know my focus as U.S. Cyber Command is NSA tends to be a little bit more on the execution side about, OK, let's roll our sleeves up, let's get into the nitty-gritty about how we're really going to do this.

QUESTION: Admiral, Tom Goldberg (ph) with Lineage (ph).

ROGERS: Hey, Tom.

QUESTION: Thank you to you, to your service, for all you do for us.

In industry, one of the impediments to moving forward is knowing in which direction to go. You indicate that information-sharing is one, but when the C-suites tried to make their investments, oftentimes what they're really confronting is no good solution.

Is there an opportunity within the government to indicate, to endorse or in some other way to certify products that meet certain criterion that allow customers to decide that this will work for me in the interim as we go down this continual path meeting threat after threat after threat.

ROGERS: We have actually done that on the NSA side. We've created a program at the National Security Agency where we articulate a set of standards, if you will, and we have offered to corporate partners out there, we'll team with you if you are willing to adhere to these standards.

We're willing to do -- certification is the wrong word. But, you know, identify these as, hey, try to highlight that you have met a higher standard, if you will. We're certainly doing that on the NSA side.

I'm not particularly smart about have we done that more broadly. You can argue that the standards that we developed, partnering, NIST (ph) being the public interface, but NIST is the face of a much broader partnership designed to generate a set of standards for industry and others that we would suggest are kind of the fundamentals of a cyber-defensive strategy and structure.

We have done that collectively as a government. And those are all a matter of public record. It's one place I urge people. So if you're on the C-suite -- or in the C-suite, and you're trying to figure out, so, how do I prioritize? What kind of an investment should I make? Where am I going to get the best outcomes? What's the best return on investment for me?

I always urge people -- I would spend some time taking a look at some of the standards and structures that we have suggested, we have tried to develop to

say, hey, look, if you're trying to build a baseline, these are the kinds of things that we would suggest.

QUESTION: Admiral, Claire Sullivan (ph) from Georgetown University.

ROGERS: Hi, ma'am.

QUESTION: Hi. Given that there's a blurring between state and non-state actors, and the concern about protection of critical infrastructure, how do you distinguish between an act of war and a crime such as hacking?

ROGERS: Clearly, the short answer is, we're still trying to work our way through that. And there is -- if there was an easy answer, we would have addressed this and done the legal definition long ago.

And now you're starting to get into law and policy. And that's clearly not my particular focus in life. But I am part of the broad discussions we have about such as what does this mean.

You know, we're trying to work our way through it. I'm used to, from a military perspective, in almost every other domain I have ever worked, we have been able to develop over time a set of standards, a set of norms that through experience we have managed to reach abroad.

I won't say it's perfect. But a general broad consensus of just what's an act of war, what's an act of self-defense, what is an attack. I would be the first to admit one of the things I talked to the team at U.S. Cyber Command and our service teammates is, that you need to be very precise about terminology.

So, for example, telling me you've been attacked, that's not the way we need to work this, you guys. We need to get into more specifics. Tell me exactly what behavior you've observed.

So I don't have a short answer for you other than -- I don't have a real great answer other than it's one we're trying to work through. And it clearly is going to be much broader than the U.S. government. It's going to be much broader than just the U.S..

Tom, I lost you. There you go.

QUESTION: Hi Admiral.

Sean Lingus (ph) with Federal Computer Week.

ROGERS: Hey Sean.

QUESTION: Hi.

It's been reported, not entirely convincingly in my opinion that ISIS is intent on setting up a digital caliphate, and launching cyber attacks on U.S. infrastructure. How would you compare the sophistication of that threat with other threats from nation-states, and how confident are you in the ability of Cyber Command to detect and thwart the threat?

ROGERS: So, I have seen the media reporting that you're referring to. I'm not getting into the specifics in an unclassified, open forum. But my assessment is that -- of the technical capabilities of ISIL other than to say I

clearly assume, and always talk to the team about, we need to assume that there will be a cyber dimension, increasingly, to almost any scenario that we're dealing with.

Counter-terrorism is no different. One of the things we're working our way through is just -- so just what does that mean? Clearly, ISIL has been very aggresive in the use of media and the use of technology and the use of the Internet.

So, it's not something that I'm -- it's something I'm watching, but I apologize. I'm just not really going to get into a lot of specifics.

QUESTION: My name is Mike Weber (ph). I'm from the Institute of World Politics, and I just wanted to -- hi. I just wanted to hear you talk a little bit more about the asymmetric aspects of cyber war. You know, I understand it's a complex issue, how we define whether we're going to defend ourselves or go after who's trying to break into our systems, but there's gotta be some sort of red line or some sort of area where we say, you know, fiu you attack our banks, you know, this is not tolerable. If you attack our energy infrastructure, this is not tolerable.

And so, I just wanted to see if you could sort of talk a little bit more about, you know, where that red line broadly might be drawn, and so that, you know, our adversaries have some idea about what that is.

ROGERS: Right, I mean, clearly there doesn't seem to be much of a sense of red line right now.

I mean, one of my frustrations is -- there does not seem to be any sense of consequence for actions taken to penetrate, destroy, degrade systems information, theft of intellectual property.

There certainly doesn't seem to be much sense of consequence to that. Again, that's part of the discussion about we have got to create this idea of norms and behaviors. We need to come, although I'd listen to some who'd tell me, "hey Rogers, it's unachievable." I'm not there yet.

We have managed to create a sense of deterrence in the employment of some capabilities that call into our question our ability to -- if you look at nuclear weapons, over the course of the -- almost 70 years or so that we have had a nuclear capability on this planet, we have, over time, managed to come to a series of norms and behaviors, formal treaties that level, that govern numbers, amounts, types, concepts of deterrents, so that even though multiple nations around the world literally have the means through nuclear weapons to call into question the long-term existence of nation-states, I'd say as a whole, in broad terms, there's a general sense of comfort that while the capability is there, there's a good sense of control of that capability, and there's a good sense of under what circumstances would nation states envision using that capability.

And people understand there are red lines you just don't cross. We clearly are not there yet in the cyber domain. We need to get there. That's a combination of policy, that's a combination of the academic world. We're going to need to work our way through that.

I'm hoping that as we see increased levels of activity across every segment of our society in terms of penetration of systems, that this will help

spur -- because -- and we're going to need to do it on an international scale, a much broader dialog about hey, just what is acceptable and unacceptable behavior here, and what are those red lines?

Because if we're going to articulate a red line, then we have to be prepared to act when people violate it. And so, we have got to have a broad policy consensus, and that's just what that means.

I'm part of that process, but I'm not the driver of that process.

QUESTION: Great, thank you.

STAFF: Again, a reminder about the notecards in the middle of your table, if you have a question and would like to write one there, please do. And just hold it up and we'll grab it.

And we do encourage questions. Next one, from Mr. Dewalt (ph).

QUESTION: Admiral Rogers, Dave Dewalt (ph).

ROGERS: Hello, Dave.

QUESTION: I'm CEO of FireEye (ph).

I really resonate well with what you're saying about the partnerships. We see this in the private sector as a security company. You know, no silver bullet with a product. We know it takes people and process and product all coming together to make it happen.

Some of the recent breaches that we've been seeing, some of the large, critical infrastructure breaches, some of the best success we've seen coming out of those was these industry ISACs (ph) working together.

ROGERS: Right.

QUESTION: And the speed of information is a critical element: having the relationships, the partnerships in place, the ability to share from one company to another really makes a difference, because of the risk timeframe that they have.

Do you see, in your role, trying to expand those ISACs (ph) across all 16 critical infrastructures, kinda getting them ready, much like the FSISAC (ph) is today and some of the others? Is that a part of your strategy?

ROGERS: I mean, I think that's part of the solution. Now, we -- we, U.S. Cyber Command, or the National Security Agency, won't necessarily be the primary drivers in that, but I am certainly trying to make that argument, that I think part of the solution set here is can't we build sector-specific capability and harness the power of the sector?

Because it's -- commonality in systems, commanality in structures in many ways, commonality in mission. There's lots we can learn from each other.

It can be a challenge, at times, not always, but in many instances, I'll watch sectors who are fundamentally structured along very different lines. And we don't always get the same value about trying to bring them together, but I've seen great returns on working this from a sector segment. And the delineation

of the 16 sectors as critical infrastructure, from a U.S. government perspective, I think is a good starting point for us, so yes.

And anything you and others can do to help in that regard, excuse me, I think would be a real positive.

QUESTION: Admiral, good morning.

Charlie Krum, Lockheed Martin.

ROGERS: Charlie, how you doing?

QUESTION: Doing great sir.

When the good Admiral Mike Brown asked the question about partnerships, and you got involved with exercises, but you mentioned the FBI, DHS, Secret Service, all government partners. How are you going to involve industry in the partnerships and will you -- do you see them involved in the exercises?

ROGERS: That's what the -- the exercises are so key to me. Because I have argued it's great that internally within the U.S. government, that we are increasing the partnerships and we are increasing the flow of information, and we are working better as a team and responding.

To truly make this work, we have got to bring the commercial and private sector into this. They need to be integrated in those exercises. They need to talk to us about hey, here's my network structure, here's my network architecture, this is what I'm seeing, this is what I have seen. We are not going to solve this by, just hey it's all about getting the federal government together. That's an important part of this, but it ain't what's going to drive this in the end.

So, we have got to harness that capability. And yes, it is -- the argument I make is "let's bring them in." And the other point I try to make is, "and let's not do this at the CEO, you know, four star admiral level. We need to put this down to an execution level where the people who really roll up their sleeves and do the work are working. Because that's where it's really going to matter and generate more value.

Sir.

QUESTION: Admiral good morning.

ROGERS: Good morning.

QUESTION: I'm Steve Watkins with Federal Times.

ROGERS: Hey.

QUESTION: I've heard you and others talk about how the country, the government is still working on the fundamentals of basically creating a national cyber posture: everything from information sharing, defining what's to be expected from the U.S. government, operational concepts amongst the different agencies, building the work force that you discussed, the laws and policies relating to you know, a state of war versus a hacking incident and so forth.

How far away do you think we are in terms of months, years, what have you, from achieving that kind of 1.0 version of a -- a national cyber posture?

ROGERS: You could argue that we're at 1.0 now. If I -- you know, it's 2014. It's September of 2014. U.S. Cyber Command is a little over four years. We celebrate our fifth anniversary in January of 2015.

If I go back and look at where we are now versus where we were, we have made some amazing strides. We are -- I don't waste any time these days with discussions about who should be doing what, or who has control, or what the lanes in the road are. We're way past that discussion.

So, I would argue, we have a broad framework and a broad vision about what we need to do. Now, we're trying to get it to, that's great, broad framework positive. Good first step. But now we gotta take it down to hey, it's all about execution. You know, what do you need to really make this work, and that's the focus right now.

So, I would argue in many ways we built the broad foundation. Now we're trying to get down to the how do we get to execution level and make it smooth and agile and speedy?

Because I always tell people, look, in the cyber domain for -- in my experience, it's all about speed, agility, and accuracy. You have got to be able to respond in a timely way. That's speed. It's about agility. You have got to be able to shift to an unforseen threat quickly. In a world that's constantly changing, you have to be agile, you have to be capable of changing.

And then accuracy. I always remind the team, it's great to get 99.5 percent of it right, but the .5 we don't get right, that's exactly what they'll exploit.

That could be -- I've watched the work force. That can be frustrating as heck. I can remember one time we did a password reset on a huge scale within our department and three days later, I see activity associated with, in this case, a particular account where I'm going, I thought we changed that. And that one, I was going through the scheme, and said, "hey, we changed that." "Well, sir, we screwed up, and out of the total there was like 113 or so that we just screwed up through an admin error, and we didn't change."

And I'm thinking to myself, so we've got, in this case it was something like 99.7 percent of what we were trying to do right, but it was the .03 that sure enough, got exploited. So my comment to the team was, don't ever understimate the accuracy piece. Don't be so fast, so agile, that you become inaccurate. Because you get one digit off in a nine-digit sequence, and one data entry field, and suddenly you're in a total different I.P. address in a totally different location, or you fundamentally have not done what you thought you did.

That's not good for us.

QUESTION: Sir, Mark Jameson, CSFI.

ROGERS: Hey, Mark.

QUESTION: Can you talk to the convergence of cyber and electronic warfare?

ROGERS: So, I think that question goes to the fact that cyber increasingly is using the spectrum, the R.F. spectrum, which traditionally had been the world of electronic warfare within the Department of Defense. Use of the spectrum, we had traditionally identified as an electronic warfare kind of mission set, increasingly you see cyber with an R.F. component to it in many ways.

It's one reason why, in the Navy for example, we made a decision early on that we saw that trend. We said that this was the future, and we wanted to combine in many ways our electronic warfare and our cyber work force and expertise into one, integrated capability.

I think that's a broad trend. I don't see that going away. The interesting thing is, in electronic warfare, we have a very well-developed set of norms and structures that I don't think automatically translate on the cyber side. So, we're trying to work our way through that.

QUESTION: Just one.

ROGERS: All the way in the back.

QUESTION: Sir.

Yes, Admiral, great to hear ya. Buck Buchanan from Power Tech.

ROGERS: Hey, Buck.

QUESTION: Great to hear a SWO's (ph) perspective on this.

Two questions. One, and bringing you back down to the operational, how important is, in real time, detecting the behavioral changes in an I.T. environment?

And also, without going into too much detail, are we developing offensive capabilities? Because that's the best defense.

ROGERS: OK. So, let me answer the first question -- let me ask the second question first.

In broad terms, I am trying to ensure that in the cyber side, the Department of Defense has a full spectrum of capability.

(LAUGHTER)

OK, so that's what I'm trying to do, is ensure we have a full spectrum of capability for if the decision is made, to employ it. Now, that's a much broader policy decision. I'm trying to ensure we have at least the capability to enable decisionmakers to have the option. The first part of your -- will you repeat the first part of the question again? I want to make sure I get it right.

QUESTION: Detecting behavior.

ROGERS: Ah, on speed.

So, detecting behavioral change at speed. That's where that situational awareness piece gets to be so critical for us, because that's a -- the ability to visualize change to identify what is normal and what is not normal becomes really critical and to be able to do it on scale becomes really critical for us, and when you don't have the means to do it visually, you really lose a lot, in my experience, in the speed dynamic here.

Because it's all about, you know, the first step to solving a problem is recognizing a problem. You can't recognize a problem -- if you don't see it, you don't recognize it. So, we've got to work our way through that and how we're going to see it.

And Mr. Tom, I'll take one more.

STAFF: OK, great.

Further questions.

OK, yeah.

ROGERS: OK, you two guys will be the last.

QUESTION: Good morning Admiral.

ROGERS: Good morning.

QUESTION: I was a Navy radio man.

ROGERS: Thank you very much for your service.

QUESTION: Awhile back.

ROGERS: And I am -- I am old enough to have served when we had radio men or R.M.s in the United States Navy. We no longer have that rating. We have the function, but we don't have the rating.

QUESTION: My name is Mitch Backfield. I'm actually a student at George Mason University...

ROGERS: Hey, Mitch.

QUESTION: ... and also a federal government employee at DHS MPPD.

ROGERS: Great.

QUESTION: My question -- I'm actually getting ready to go into my PhD dissertation, and one of the -- one of the issues that I'm exploring is this notion of how every day, day in and day out, Americans feel relatively safe because of our Defense Department, and we have reasonable assurance that the money that our government is spending in the Defense Department is providing us with a very high level of security. With respect to cyber security, however, I feel that perhaps ordinary Americans or the average American may not feel that same sense of security, whether it's data breaches or whether it's our personal information that's out there in the public for bad actors, day in and day out, we hear another incident of a data breach or personal information out there.

So, for the American people who perhaps may not have that same sense of security and safety that we have with respect to defense issues with cyber issues, what do you tell those people today? Thank you.

ROGERS: Well, first, I wouldn't disagree with the premise that right now, I think broadly across our society, we're scratching our heads, looking at what's going on around us, and going, "wow, this is not a good thing."

It is impacting us on a very personal level. How many of you here, within the last 12 months, have had some form of compromise to your knowledge of your personal information or personal systems? Raise your hand.

My hand is up there with you.

Increasingly, this impacts us not just at work and in the functions of major corporate and private entities, but increasingly down to the personal level.

I'm hoping, personally, that personal level helps generate a broad consensus as a nation in us, that this is something that we collectively need to put a greater level of emphasis on.

But it is not, in the end, going to be something that the government is going to do wholly by itself. So, to me at least, the idea that well, I'm going to turn to the federal government and say "hey, well it's your job to make sure we have no cyber security issues across our society," I don't think that's particularly realistic. And I don't think that is necessarily the traditional model we have used as a nation in how we're going to solve problem sets: particularly something like this.

Don't get me wrong, the department and the government clearly will be a part of that. But I think it's going to be much broader than that, if that makes sense.

And sir, you, there was one standing out there, going to be the last one.

All right, take us home, young man.

QUESTION: OK, thanks. I...

ROGERS: And then they gave you a microphone that doesn't work.

QUESTION: That's right, I can project.

There it goes, it's fine. That's much better, thanks.

Patrick Tucker from Defense One.

ROGERS: Hi Patrick.

QUESTION: So, your other role is as head of NSA. And you're basically the person in charge of our nation's signals intelligence collection. So, you've talked a lot about the importance of partnerships international, and within the industry, in creating a meaningful cyber defense.

I think a lot of people would say that over the last 10 years, NSA signals intelligence collection has alienated a lot of government partners around the world, and a lot of people in the tech community.

So, how does your approach to signals intelligence differ from that of your predecessor, and what role does signals intelligence play int eh future of our country's cyber defense? Thanks.

ROGERS: An interesting cyber defense question.

(LAUGHTER)

You know, first and foremost, I say tell people, look, I'm not focused on the past. I have great respect for those who went before me. I have great respect for the roles they played and what the organization has done collectively.

I have to tell you, I fundamentally reject the premise that says "wow, NSA is in a position where it no longer has relationships with foreign counterparts, where the corporate sector, nation sates, foreign counterparts have fundamentally walked away from us. That's not what I have observed in my five months as the director.

Clearly, what I always try to remind the work force is the key for us is as you heard in the very opening. We always follow the rule of law. OK, we have yet, in any of the reviews of our organization, in the last year or so, following the revelations, you can clearly have a debate, and that's a good thing for us as a nation, about should we have these laws?

You can clearly have a debate about are those laws constitutional? You know, that's what lawyers do. That's not my particular role. What I try to remind people is, even as that debate is ongoing, the reviews to date have all come to the conclusion that the National Security Agency has been fully compliant with the law, and that secondly, in the execution of those lawful operations, there has been no finding that NSA has attempted to systematically undermine that law or failed in its duties to protect the information that it collects.

OK?

I remind the organization we follow the rule of law. We remind ourselves that we are accountable to the citizens of the nation we defend. When we make a mistake, we stand up and say we got it wrong. So, another point I would make. Much of the information, not all, but much of the information that has become public is in no small part because NSA and the execution of its responsibilities to notify the court system, to notify Congress, to notify the Department of Justice and the director of National Intelligence Organization, largely the four people that we -- organizations that we are required, that we consistently inform our oversight mechanisms when we make a mistake -- when we get it wrong.

And I have clearly articulated to the organization as the director, if you make a mistake because we failed to train you, because we made an error in the technical solution we have put in place, or some other reason, we will acknowledge that mistake. We will correct the mistake. And I will be there for you.

Because it is the nature of the human dynamic to make mistakes. I wish I could tell you I have been part of an organization for 33 years as a uniformed member of the Department of Defense that has never made mistakes. I have yet to run into that in my life, whether it be at work or whether it be in my own life and at home.

However, there's a difference between a mistake and a choice. And what I remind the work force is, if you make the choice to violate the laws and procedures that we have in place, if I catch you or we catch you violating the standards that we have put in place, and you made a conscious choice, I will hold you accountable for that choice. And there is no place in this work force for those of this ilk.

Now, we are blessed with a motivated and dedicated work force. It ain't perfect. But they go to work every day, and they say to themselves, what can I do to help defend this nation and those of our allies and teammates around the world?

They don't come to work and say to themselves, "Jeez, how can I indiscriminately violate the rights of my fellow citizens today?" That is not, not what drives their behavior and their focus at work every day.

It's all about executing the mission, defending the nation, and our key allies and friends around the world, ensuring we follow the rule of law, reminding our selves we are always accountable to the nation we defend, and then wehen we make a mistake, we are honest and forthright about it.

And I hope that answers your question, sir.

And with that, I thank you all very, very much.

(APPLAUSE)

Thank you for your time.

(APPLAUSE)

END