

National Security Agency

CyberMaryland 2014 conference

Speaker:

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

Location: Baltimore, Maryland

Time: 12:30 p.m. EDT

Date: Wednesday, October 29, 2014

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

(Applause.)

MR. : (Inaudible.) I did just want to mention, involving the admiral, that we're going to have an informal fireside chat today. It is unscripted, although we have a few notecards with some notes as backup. A fireside chat – we'll also engage the audience. You should see on your table some 3-by-5 note cards. Please use those notecards and the pen provided to ask questions that you might want to have presented to the admiral, and we'll be collecting those up. Card collectors, could you raise your hands? And if you have one, just kind of wave it in the air and someone will come and get it from you. And let's go ahead and get started.

(Cross talk, laughter.)

MR. : So, Admiral, thank you for being here and taking time in our fireside chat today. I just want to – thought you could start off by providing us a little context and background about the role you have and, like, what is the job? I don't know that we all know. There's multiple hats you wear and multiple things that you do.

ADMIRAL MICHAEL ROGERS: I get to – (inaudible) – jobs. First, as commander of United States Cyber Command, three primary functions: first, to defend the Department of Defense's networks; secondly, to create and operationally employ the cyber force – dedicated workforce, if you will, that the department is creating, work the range of cyber activities for the defensive to the offensive.

And then a third mission is, when directed by the president or the secretary of defense, provide our capabilities to support and defend critical U.S. infrastructure. The U.S. government has designated approximately 16 sectors in the private industry as being critical to the nation's security. So think of water, think of power, think of aviation, fuel, financial, et cetera.

As director of the National Security Agency, related but different, that first job, U.S. Cyber Command, is an operation of one of the – (inaudible) – operational commanders in the Department of Defense. As the director of NSA, I lead an intelligence organization, part of the 17 segments of the U.S. intelligence infrastructure and primary 17 segments.

NSA – two primary missions. One you have heard much of – although my characterization of it actually accurate – (inaudible) – what you've heard much of in the last 15 months – is foreign intelligence to use signals intelligence to generate – (inaudible) – nation states – (inaudible) – individuals are doing, particularly with respect to those who would attempt to gain an advantage or do harm to us or our citizens or to our allies or friends.

The second major mission for NSA, and one that I think is very important for our discussion today, NSA also has an information assurance mission, and in that mission we do several things. Number one, we help the Department of Defense develop – (inaudible) – and security standards. We help partner with the – for the Department of Defense we help partner with NIST and other elements in the U.S. government to generate the same standards for both the U.S. government and more broadly the U.S. as a nation.

And then lastly, we provide cyber expertise to help defend both infrastructure within the U.S. government and, when requested – and we do this through the Department of Homeland Security and the Federal Bureau of Investigation. When we are requested – and increasingly we find ourselves looking at trying to apply capabilities to support those agencies as they collaborate with the private sector to give them some of the major penetrations – (inaudible).

MR. : So you're not busy at all? (Laughter.)

DIR. ROGERS: I wanted to say please accept my apologies, if I could. Let me start off by apologizing by saying I was 15 minutes late. So please accept my apologies. Quite frankly, I was at a session down in the national capital region and had to get out of that and get in a vehicle and get up here, so please accept my apologies. It's very rude of me to start out by being 15 minutes late. Unfortunately it was just beyond my control. Thank you for your willingness to wait. I hope you were eating well in the interim.

MR. : We'll see if we can get you out five minutes early and give you – (inaudible) – five minutes. (Laughter.)

DIR. ROGERS: I'll tell you what's your most precious resource – (inaudible) – time. If we could just put about 30 hours in a day, life would be so much easier.

MR. : (Inaudible.) (Laughter.)

So you mentioned – I mean, you've got a lot going on, obviously. How can Maryland companies, companies in the region, even our friends on the West Coast, help you achieve your mission on a day-to-day basis or really in the coming months or years? In no particular order.

DIR. ROGERS: Help us generate the workforce we need, because I always remind people, look, the technology is incredible. It certainly gives us the capability to do some amazing things in the nation's defense. But what our real edge is isn't the technology; it is the men and women of the organization, both at U.S. Cyber Command and the National Security Agency. It is the men and women who apply the technology and their intellect and their passion and their commitment to mission, to doing the right thing in the right way. That's what our edge is.

And so the first thing I'd say is, I welcome your help in trying to identify how we're going to generate a workforce for us in the future. I also ask your help in – we, just like – (inaudible) – are constantly asking ourselves, so how might we address specific problems? And oftentimes we will turn to the corporate sector and ask, given your expertise, given your capabilities, can you give us some of your insights and help us work through how do we solve some of these problems? Those problems could range from very technical things. Those problems range that – how we're going to build the IT structure that we use to underpin our mission.

You know, in both hats, U.S. Cyber Command and NSA, we are global entities with a footprint that literally spans much of the world and certainly much of the United States. And so we have to tie that all together. So IT has done one area where we had particularly turned to counterparts on the outside and said, hey, can you help with – help us with this? What insights do you have? How can you help us do this in a more efficient and more secure way?

MR. : Just to follow up on that, do you spend much time as a team talking about how to operationalize cyber, because if I see – if we say that development is epicenter of cyber, how do you then take that out and instill the right operational aspects in a San Diego, in a San Antonio, in Silicon Valley and beyond?

DIR. ROGERS: So for U.S. Cyber Command, I gave you the three missions, but I'm always telling people, look, when you cut to the bottom line, it's about how do we operationalize cyber within the Department of Defense? That is where I spend my time now. Generally, I won't go into the outside world for that as much because I'll use kind of very traditional operational concepts within the military.

One of the arguments I may give is while cyber has many areas and aspects that are different than some of the more traditional domains, I believe that it has much more commonality than difference. And so we have tried within the department to start from the perspective that would argue, accentuate the commonalities – common terminology, command language, common tactics, techniques and procedures, the way we do business to the maximum extent we can with the broader, more traditional areas within the department – and then, as cyber is different, acknowledge the difference, but to the maximum extent we can, try to emphasize the commonality.

MR. : So which, in fact, ties in operationalizing the armed forces.

(Cross talk, laughter.)

MR. : What does that workforce that we were just talking about, certainly at Cyber Command, at NSA, CNC – (inaudible) – what does that look like tomorrow? We all understand how we got here to now.

DIR. ROGERS: Right.

MR. : We all – and I think a majority of us understand the current threat, but what do we need to do to develop – (inaudible)?

DIR. ROGERS: This is another area where I think you guys can really help. The traditional workforce of NSA – one of the things I'll always do when I'm walking the halls and eating lunch down in the cafeteria and just talking to people, and the workforce – (inaudible) – meet the director. I'm speaking on the NSA side – and I do this on the U.S. Cyber Command side – that you have to go to the director and ask, have I met you before? And if the answer is no, hey, tell us about you.

And among the questions I will ask is, tell me what brought you to us in the first place? How long have you been with us? And what is it about the future that you – (inaudible)? And one of the things that has struck me is we have a workforce – I will routinely talk to people who tell me, I've been with the team for 20 years, 25 years or 30 years, 35 years. We just – I was just talking to an employee. Six weeks ago she was retiring after 50 years at NSA. And I was thinking to myself, wow, 50 years. I'm at 33 years as a commissioned officer and I – and then when I think, 17 more? Who's going to do that? (Laughter.)

And so one of the things I talk to the leadership about is I think the model for the future for us needs to be different. While I want to build on the idea of longevity, I also want to create an idea where our workforce can leave us and can go out and work in the private sector for a period of time and then come back to us; where we can also go to the private sector and say, hey, would you be interested in coming to take – work with us for a couple of years, gain greater insights on what we do?

Because one of the challenges I find, quite frankly – and you see this playing out very publicly – we are talking past each other. Our culture doesn't understand the outside world as much as the outside world doesn't understand us. And it doesn't mean that either side is good or either side is bad. It just means they have a different set of experiences and a different culture. And the experience set in a culture isn't necessarily optimized for interactions with people of a different culture and different perspective. And I think personally that – (inaudible).

So one of the ways I've argued internally – and this is – (inaudible) – moment, is what do I need to do to make this a reality? How can I get a workforce that's able to go out and gain experience

and come back to us? And I think they will be that much better. And how do I gain the capability for the corporate sector to come with us for a little while and then go back?

MR. : So is part of that discussion, you know, looking at new ways we think about compartmentalized information? As we all know, there are folks out there who have incredible aptitude in this area that couldn't ever get a clearance because of things in their backgrounds – (inaudible) – adverse. But, you know, ways of saying, you know, perhaps we can bring people in without having them work on everything?

DIR. ROGERS: For right now what I say is you're going to have to get a clearance. I mean, one – (inaudible) – I put in when we started this – and we'll do this integrally over time – I said, to start we're going to need to be able to look at – (inaudible). Then, over time, if we find – (inaudible) – background, you know, we'll take a look at it. And I fully expect that it will change with time. But I would tell you, if you look at the workforce, particularly at NSA, U.S. Cyber Command – (inaudible) – military, you can't tell the difference between one of our people and an industry guy. We have one set of standards for all of them that we all have to comply with. And I have to meet the same – (inaudible) – standards as anybody else, you know, within my service. We don't differentiate by specialty.

In the NSA workforce you will find some amazing people, from that individual walking around with a ponytail and tie-dyed t-shirts and shorts, and in flip-flops no matter what the weather is. It's an amazing, eclectic group of – (inaudible). So it's not – lest you think, well, they must all be a bunch of, you know, people carved out of the same fundamental – (inaudible) – have the same background – (inaudible). I find that personally, as a leader, incredibly invigorating. I love the different men and women that I meet every day.

The one thing that unifies them – even though some of them are very different, the one thing that unifies them is an amazing sense of both mission and responsibility: Hey, we've got a mission that the nation counts on. We've got a mission that makes a difference, you know, a mission that's important, but also the responsibility piece: Hey, look, we've got to do this right. We don't cut corners. We comply with the law. We assure we work within the authorities granted to us, and we protect the information that we generate. We don't sell it. We don't give it to other people.

We have strict controls about what we do. We're all governed by law, which is a good thing for us as a nation. We would not want an organization that seemingly just does everything on its own. That's not what the National Security Agency is about, and clearly the same in the U.S. Cyber Command.

MR. : This makes me think of your predecessors. How do you see – any special shape that you put on the organizations that you're touching now versus how your predecessors have run the operations? Because when I think about mission and vision, I know that both of your predecessors had also very strong missions and visions. I'm curious to know if they're aligned, you know, all along the way, or do you decide that, oh, I'll sort of shape things – (inaudible)?

DIR. ROGERS: I'll be honest. I've never been driven as much by people going before me – (inaudible) – come out the wrong way. Let me tell you what that means. I was blessed to inherit an organization that was well-structured – (inaudible). It's amazing, even – (inaudible) – what you can be. But I never asked myself, well, gee, I need to do the same thing that the men and women that went before you did. I'm just not wired that way. I just think, hey, Rogers, they're paying you to decide. You know what the mission is. You know what the challenges are. So how are we going to get there? What are we going to do?

And when I do that, I don't consciously think to myself, boy, I – (inaudible) – the leaders who were before me. And that's no remark on anybody that went before me. I'm just never – I'm just not wired that way. I just don't spend, really, any time thinking about it.

(Cross talk.)

MR. : I want to give some – (inaudible) – the audience.

(Cross talk.)

MR. : Let's go to an audience question. Someone was asking about how your role divides into issues around offensive and defense cyber, because you have a special mission, just as U.S. government, as DOD has an offensive role that the commercial side doesn't get involved in.

DIR. ROGERS: So the first thing under both hats – it goes to Cyber Command and NSA – I do not – do not have the authority to conduct offensive operations. It does have to be granted to me. That is something that the president and secretary of defense would be responsible for.

Having said that, clearly under both hats I'm very upfront with people. I say, look, part of our job is to provide policymakers and operational commanders with a wide range of options – (inaudible). I do not have the authority to do that on my own. That's a very carefully controlled, very well-thought-out, very structured process.

MR. : (Inaudible.) I wanted to talk about workforce development. You know, especially the work inherent in the Washington beltway area, building the workforce. And again, I'm curious about the – (inaudible) – of that because, you know, of our distance in places like San Diego.

But how do you see that shaping up? Do you feel like the – (inaudible) – work is providing supportive structure to what you're doing? And are there any improvements or guidelines that you would provide on what you're seeing across the workforce?

DIR. ROGERS: Well, first, I really like – (inaudible) – work. Because we're a global organization, our recruiting and the way we bring people in is reflected in that. It's not just focused, if you will, here in greater Maryland, Baltimore area, not that a large segment of the workforce doesn't come – does come from here, and no small part of the largest segment of the workforce physically works here for – (inaudible).

Having said that, though, because we have a wide geographic dispersion we also try to make sure that our recruiting effort is reflected in that. So you will find NSA men and women on college campuses around the United States, high schools, technical organizations, cybersecurity, cyber – (inaudible) – organizations. You'll find us trying to interface with a wide range of people because we acknowledge that the workforce of the future needs to be fairly – (inaudible) – experience.

And it's more than just cyber. In an intelligence organization cyber is one tool we use, but we need more than that, so the workforce on the NSA side is a greater set of capabilities and requirements. On the U.S. Cyber Command side, largely – it's in the title so we're largely cyber-focused, so the workforce there is reflective of that. If you look at the U.S. Cyber Command workforce, it's about 80 percent military, about 20 percent civilian. If you look at the security agency, it's probably 60 percent civilian, 40 percent military, so inverse, different compositions in the two. The good thing is that no job gets – (inaudible).

The partnerships clearly are important for us, whether that be partnerships – (inaudible) – here in Maryland. If you just take a look at last week, I had been out – (inaudible) – and spoken in San Antonio, Texas; Orlando, Florida – (inaudible) – Georgia – (inaudible) – here, the District of Columbia just in the last seven days. Columbia, here those have included large conferences, cybersecurity sessions, business community, academic institutions.

One of the things I talked to the team about is, look, we have got to create partnerships with a wide range of entities out there. There's no one single source for this. It's all about creating partnerships and relationships across the breadth of insights that we need, because the days when the Department of Defense drove technology I just think are way past us. The days of the 1960s and, you know, the Apollo space program and how huge government structure and investment really had a fundamental role in shaping many of the cutting-edge technologies of the nation, most people forget, hey, the Internet itself started with a DOD defensive – what used to be – what is now DAPRA, what used to be ARPA, when DOD posed the technical question, could we create a system that will enable us to move information between individuals spread large

distances across the United States? That was the fundamental premise that DOD posed to its research arm in the late 1960s: Could we do that and not do it by RF, not do it by telegram and (not ?) do it by fax – (inaudible). Could we do this in an automated, highly efficient, high-speed manner? And from that simple technical question, (drived ?) through the hard work of many, many people and certainly far beyond anything at the Department of Defense. And people tend to forget: This started – (inaudible) – because of the government question, those days, to me, are far behind us. And so I look for technology to be driven in the private sector. And so one of the things I always tell our team about is, guys, we have got to create relationships with the private sector. If we're going to be technically focused organization – or organizations in this case – if we're going to be technically focused, you've got to go where the technology is. The technology isn't originating with us. It's out there. And we just – (inaudible). If you look at – if you're a business – many of you from the private sector – do you – your business slice – (inaudible) – largest company – your business slice with DOD is so small compared to the broader commercial sector which you're dealing with. You know, the days where will drive things from a perspective I think are long past over.

MR. : So staying with the innovation topic, one of the greatest challenges of bringing in external innovation, whether it's innovation of thought, innovation of technology, innovation of leadership within the organization for these partnerships is collaboration, which is essential really to overall success – (inaudible) – some other organization – (inaudible) – what's your challenge?

DIR. ROGERS: So the challenge isn't technology (for ?) me. The challenge is, how do you create an environment, an ethos on culture that embraces the idea that change is both continual and can be a real positive for our organization. Change for us as humans can be very difficult. It injects uncertainty. It brings differences. It tends to make us uncomfortable as people on a personal level. And yet, I'm telling the organization, look, if we pride ourselves on being a technically focused organization, we have got to be capable of changing ahead of the technology that we're dealing with. And look at how quickly that technology is changing. And to do that, it's all about what kind of structure you create, what kind of ethos, what kind of culture you create – one that values – not that we've done it; I don't mean to imply that – but to put it another way, one of the questions as the new guy I asked the organization was, at what point does our size start to work against us? You know, there's a lot of things to being big, a lot of positives, but there's some tradeoffs to being big. So what I'm trying to walk the team right now through, are we comfortable with the tradeoffs and have we really optimized ourselves and so not letting our size work against us? Because the nation and our allies are counting on us. We have got to be efficient and we've got to be effective.

MR. : I'd like to follow that up with an inquiry about the Internet of things. I remember when you were in San Diego a year and a half ago or so, then we were talking a lot about bring your

own device and some of the challenges that that presented to DOD and to your command at the time. And I'm just curious to know, you know, how – (inaudible) – started to look across your organizations at this Internet of things, you know, another 30 billion devices connecting up to the Internet, cars, automobiles, but presumably other things as well, right? So if you look at the classic Cisco definition, it's IP plus real-time analytics – (inaudible) – all those things. And I'm curious to, you know, what you see shaping up in that regard and how that will impact the work you do.

DIR. ROGERS: I mean, from a cybersecurity perspective I would argue that that is among the fundamental challenges of the future, for us as a society, not just us here at DOD but as a society.

I do not think yet we fully understand what the second- and third-order effects of both the connectivity and the proliferation. So we have both quantity and a quality aspect here – what the second- and third-order effects of this are going to be for us as a society, as a nation. It brings amazing opportunity, but it also brings potentially tremendous vulnerability. And we've got to work our way through to how we're going to deal with that, because none of us want to walk away from the convenience that these portable devices provide us. I mean, you don't run into anybody now – and I won't do this with this – (inaudible) – I'll often ask is, let's walk through how many devices that you've integrated into your life and then – (inaudible) – average for most people is somewhere on the order of three to five. When I go to tech audiences, hey, if you include everything – well, I've probably got 10, eight as a kind of baseline. If you look at the proliferation of them, this is so integrated for our everyday life now. The idea that we're going to do without it I think is a nonstarter for us. None of us would want to accept that.

So we've got to figure out how are we going to make this work, how are we going to secure it and how are we going to make sure that this doesn't present a potential – (inaudible)? I mean, I think about, well, what if we had an Ebola-like challenge in the Internet – (inaudible) – that wasn't an infectious gene, so to speak, or a disease that changed our internal – what if we had something equivalent to that in the digital age and it used this connectivity – not a disease, but in terms of something that was able to replicate on a global scale, to use this connectivity in terms of ability to potentially impact information flow, our ability to conduct the basic fundamentals of our everyday lives in some way? And that's pretty amazing to me, but you've got to think about so how are we going to deal with this? And we will work our way through it. We're not – we're nowhere near fully understanding this.

And if this is – now the other point I'd make – (inaudible) – but the other point I make is, we're dealing with this right now. I still run into people who will often tell me, well, again, that's an issue we can deal with in, like, two years.

MR. : It's not the emerging Internet of things.

DIR. ROGERS: Four years – (inaudible). Hey, we're there, folks. We're living this now.

MR. : Well, and I think this morning Peter Bloom (ph) was talking, you know, about two different things. It's the Internet of other people's things as well as that, you know, China has integrated this Internet of other people's things into their five-year plan, and so I think it poses a question and a challenge for us as a nation is how do we partner with our national security interests and our commercial interests to ensure that we're aligning and securing, ultimately, the bigger picture and having sort of a national strategy, much like we did in the past – not that everybody had – (inaudible) – devices in their home, but, you know, it's that we have a national strategy for, you know, securing our country, and I think – I think we're at that point now where we need to sort of think nationally or perhaps internationally about how are we going to address this Internet of other people's things and prevent them from being – (inaudible) – instead of just saying, well, doesn't NSA do that – (inaudible)?

(Cross talk.)

MR. : And I just have one more element to that. You're talking – (inaudible) – is think about rules of engagement, right? It's a notion that I know is sitting there inside of cyber. We think of it in terms of more of a nuclear thing where it's very clear that in nuclear terms, if you do this, then this is what you can expect in response. And I wonder if these same sort of discussions are at play in your work regarding cybersecurity and also how that might play towards the Internet of things.

DIR. ROGERS: OK, so lots of implications. Let me see if I can try to distill this down to a few things. So, in the U.S.'s structure, not just for cyber but generally, we have historically differentiated between what is a private function that the corporate world deals with, what is done outside the community. We've generally argued that there's a separate set of functions that tend to be very governmental and are really – the government tends to shape and drive. And then we have a set of issues that we generally apply – (inaudible). My argument is, cyber borders the line between all three of those things, that the days of looking at cyber where we're – for example, we can expect private companies to withstand the efforts of foreign nation-states to access information. I think that's putting a lot on the private sector to try to withstand that effort.

Likewise, I don't think it's realistic to expect, well – (inaudible) – that's what we want them to do. What I think we need to do is create a series of partnerships that enable us to work together in a way that we don't traditionally. And we need to view this in part through intelligence, but we need to view this in part through the prism of national security. If U.S. Cyber Command was

given that third and final mission I mentioned to you, about – (inaudible) – president or the secretary provide capability to defend critical U.S. infrastructure.

We did that because as a government we came to the conclusion – (inaudible). In one of these 16 critical sectors, if we can lose the ability to power large sectors of the nation, to sustain water, to sustain aviation travel – if we lose that because of some efforts on behalf of a foreign nation or a group or set individuals, that's a national security issue for us. Because of that, we asked ourselves: What can DOD do to help here?

Now, this is not solely a national security issue, which one reason why in the U.S. government the Department of Homeland Security has been designated as the lead, not DOD. Department of Homeland Security is the overall cyber lead in broad terms for the U.S. government. It's one reason why we partner as closely with DHS. We collaborate with DHS, as well as our FBI team, because there's a law enforcement aspect to this.

So as companies are dealing with theft of property, theft of – the criminal, whether it be the nation-state, that we've come to the conclusion there's a law enforcement piece of this. And so we, U.S. Cyber Command, actually – (inaudible) – partner with the law enforcement piece. But we have got to create a framework where we can bridge these and bring them together into – (inaudible).

In on the legislative piece right now, the U.S. Congress is looking at a couple different type of legislations. I have been very direct about saying I think that's critical for us as a nation because we have got to – (inaudible) – both in private sector and in government to share information both ways near real-time, at – (inaudible) – speed and elevated machine-to-machine – (inaudible).

I mean, people will say to me at times, hey, I'll send you an Excel spreadsheet with the kind of – (inaudible) – we're looking at. I go, are you kidding me? You think we can work this kind of complexity and the breadth of this problems at – (inaudible) – share information. That's not the problem for us.

We also need to ask ourselves, what is the information that we want to share? What makes sense? Because we can quickly drown ourselves with data. That's what it's going to be about. That's not – (inaudible). We also need to make sure we're not sharing private data. I don't want that. I – in specific – if I put on my NSA hat – for example, we have specific legal limitations about what we can and can't do and a series of protections that we have to put in place when it comes to U.S. person information. That really complicates my mission in the cyber defense. I don't want that. It will slow us down.

So I'm interested in can we get together and talk about, so, what kind information do we need. What do you in the private sector expect from us, and what do I in the government need from you? So for me, I would argue what I'm interested in the private sector is, here's what – well, first let me start out, here's what I think I would owe you.

Can you give us insights on the kinds of malware that we're going to see, what's going to be directed against us, when is it going to be directed against us, how is it going to be directed against us, when are we likely to see it? Are there any indications that you can share with us that would be indicative of, hey, that malware that we were telling you about, these are the kinds of attributes you're going to see in advance. This is the kind of activity that you're potentially going to see as a precursor. And here's where the threat factors are going to come from. That's what I think you would expect from me.

What I would ask of my private teammates is, I'm not in the networks, and you don't want me in your networks. So I don't know what you're seeing. I don't know if what you've tried has worked. So I am interested in, so, tell me what the malware looked like from your perspective. Tell me how you configure your systems.

What worked? What didn't work? What did you try that failed? And then give me the specifics of what you're seeing. Did it match what we told you we'd thought you'd saw? Is it something totally different we didn't anticipate? What were the characteristics that first told you you had a problem? That's the kind of insight that I'm interesting getting back because between those two I think each of us will get a better picture about what we're dealing with and what we need to be ready for in the future.

The other thing I think that's very powerful for us in this whole idea of partnerships is within those critical infrastructure segments, the U.S. government, partnering with industry, is trying to put together a kind of comprehensive approach about how we can address many of these issues within each of the segments. And so what I try to remind people within the segments is, remember the insights of one can lead to the defense of many.

So the value that we can get when we work along sector lines, for example, will really pay off much more than just one company and the U.S. government. I think this will be much more insightful. And I don't pretend for a billionaire and a government guy that we have the answers here. I want to learn and gain insights from you. I want to talk to your IT team. I want to get a sense for what worked, what didn't, what do you think you're seeing? What did you try? Because then I'll use that to shape the kind of advice we're giving you. So here's what we think. Here's how we would counter it. Here's what we would do for mediation and – (inaudible).

MR. : It sounds easy.

MR. : Oh, it certainly – (inaudible.)

MR. : (Inaudible) – I mean, the very critical infrastructure sectors that have been identified, it's simple to say that there are enterprises in there that have an interest and certainly understand – or at least an awareness that sharing information with you has value. But as we learned, certainly in the Target situation, you know, there – all these large enterprises are connected to very small companies. Many companies don't even understand cyber.

So if somebody uses a payroll system that manufacturers spices, you know, may be the vector for trouble. How can we engage with these non-cyber-aware community to, A, let them know that they are a vector, but also that they have something at risk, and to share information with them?

MR. : Right. So what we – you know, what I have said internally is, hey, start big and work our way down, because the greatest vulnerability in some ways, as you've said, it's not the largest. The ones that we often talk about from amongst ourselves – we're looking at these 16 different segments, for example. It's the mid to smaller ones. If you look at – (inaudible) – for example, they've been very public about talking about their annual computer network defense baseline budget is about \$250 million. How many companies can afford a baseline investment of \$250 million a year?

And they have just talked about doubling that. (Inaudible) – activity they've seen, they talked about doubling that. Half a billion dollar investment. How many segments – entities within the private – we'll ask all of you, the businesses that you're affiliated with. If somebody asked you, hey, come up with \$250 million as a baseline? That gets to be really, really difficult.

So what I'm hoping is if we start with the largest organizations have the greatest resources, and in many ways – (inaudible) – rather than trying to do it from the bottom up. Just concerned that working from the bottom up is probably not going to be, in terms of speed any –

MR. : But how do you – how, or – and I don't know the answer, and that's why I'm asking – is how we ask these large enterprises to collaborate with these small companies, to share that information? Because certainly we're in a competitive time. I think a lot of people think, oh, I need to hold onto this information. Also, you have stock prices are maybe coming into play sometimes. But you know, there is a value to sharing information, to collaborate with the smaller organizations and vice versa.

MR. : I think the second approach helps us there because there's commonality of structures, commonality of objectives, commonality of problem sets. I will say I was very – yesterday I spoke at the U.S. Chamber of Commerce in the District. And I was introduced by a leader at

American Express who – it was very hard to hear. In his remarks Mark (sp) said we have got to stop thinking about, hey, we don't want to share because of the competitive piece of it. In the end, our competition collectively is enhanced with a secure cyber infrastructure.

And that, in the long run, is a positive for all of us, not something to be viewed as, well, I have a competitive advantage in the cyber sphere. Now I'm more secure than the other guy. I – for that, I was very – (inaudible) –

MR. : So – (inaudible) – is starting. (Inaudible) – supply chain, you know, is the way I think – in terms of that, right? Is that large companies, agencies, they all have a supply chain, and it's sort of their responsibility to work up and down – (inaudible) – enhanced security. So I think there is a supply chain discussion that's been ongoing, and that – (inaudible) – provides –

DIR. ROGERS (?): And you certainly saw that highlighted – (inaudible) – the activities, the large-scale commercial penetrations you saw over the last six months, supply – (inaudible) – has played a very major role – (inaudible).

MR. : I wanted to take a little different direction and sort of move back to – (inaudible). And I'm asking a question in a moment about variables and see about applicability, but I wanted to mention to the audience, so embedded inside the cyber – (inaudible) – this year is a track or a set of presentations, keynotes and panels about the (Internet things ?) and securing – (inaudible), so I want to encourage you to look at your programs and try to attend the sessions if it's something of interest. But I want to ask you, you know, there is – one of the key elements of the (Internet thing ?) is sensors, and there may not be any organization on the planet that has as many kind of sensors as you have, not only devices but human beings as well and with things like (variables ?) coming in and – (inaudible) – one is, do you see that continue to expand, you see a time when we might even have – (inaudible). Then I just like to explore this idea of sensors in general, how you cope with all that data and create information on it.

DIR. ROGERS: I mean, I clearly see that as – (inaudible). If I put it on my intelligence hat and I look at what social media and social network phenomenon is doing, you know, I look and I say, wow, we are turning literally every individual on the planet into a sensor with a series of digital devices that enable them to gain situational awareness and to share that situational awareness with the greater around them, whether that'd be video you're doing, the audio work you're doing, whether that'd be the text or the vocals – I mean, it is just amazing. We are characterizing the world around us constantly in ways – (inaudible) – understand.

As an intelligence individual, there is a attractiveness in some ways that – to me because I'm always trying to generate – you know, within the law and the policy, how can we generate more – (inaudible) – provide better security for the nation.

The flipside, though, I think is – so if that's the case, you know, what does that mean to us as a society? What are we – (inaudible)? And have we – (inaudible) – thought about this? And what does privacy mean in the digital age, in the 21st century? And what is true – (inaudible) – for us as individuals in this digital environment?

The discussion that we have had to date from my perspective is so incredibly narrow. I would welcome a broader discussion and a broader debate within our society about, so what just – just what does privacy mean in the digital age? Whether that'd be government, private industry, the technologies that we have incorporated – (inaudible) – the technologies that as a nation we've embedded around us – I mean, if you walk out of this hall today, you know, ask yourself, so, how many cameras am I getting picked up on, walking from here to fill in the blank – (inaudible) – come to a conclusion from a society – (inaudible) – that video surveillance offers an increased measure of protection and defense, an ability to understand and hopefully identify problems. We did it because we thought, overall, you know, it was positive for the nation and for us as citizens. I think we need to have a broader discussion about, so what are we comfortable with? And is what the – (inaudible) – industry can do, is what the government can do, should they be the same, should it be different, should it be comfortable with one versus the other? I've just – I've found the discussions to date to be so simplistic in some ways to me – (inaudible) – to think much more broadly about this because if you think that government is the only aspect of this question, I would argue I think it's much broader than that.

MR. : Yeah, I wonder what the cultural implications might be. You know, I've wondered, you know, with so much monitoring and – in a way, it could – it could – in one direction – (inaudible) – what I call a culture of forgiveness, you know, we might actually change the way that we view certain fractions or certain things that people do, sort of we all know we do, you know, silly things sometimes, and maybe that will create sort of cultural nuances in our society where it's, like, hey, that's – that is one on you, and I may be the next person, that is one on me. And I wonder if from that we'll sort of bend our cultural norms over time.

DIR. ROGERS: Yeah, it would be interesting to see all that played out. I will – it will be interesting, and I'm sure there is many academics taking a look at it, but how is the technology that we're dealing with every day starting to change us as a society and on a personal basis, both in terms of norms, expectations – (inaudible) – you can see it in the way we interact in the world around us.

MR. : (Inaudible) – the discussion of what types of avatars do we have in the digital age and, you know, how do we begin, especially around consumer devices – you know, we're getting things for free, and what – you know, really, are we the consumer? I mean, not are we the consumer; we are the product – (inaudible) – and we are the product in this digital age. We

assume that we're buying something, but we – in most cases we're not. We're agreeing to give up something. But do we, you know, have a – do we need to have a broader discussion on what are our – (inaudible) – privacy? What avatars do we have – (inaudible) – this is family circle. This is my – this is a circle I'm OK to deal with when – you know, in – with health care, and this is what I'm – (inaudible) – government, or – you know, because I – (inaudible) – I think the conversation is very simplistic. It's – (inaudible) – currency that sort – (inaudible).

And then – (inaudible) – you know, there is no segue, but I think it does bring, since we're running out of time – (inaudible) – question I think – I've heard debated in this room and certainly over the last 18 months is, what's – what – you know, what is the difference or what are we doing to define the difference between a cyberbreach, a cyberattack, an accident and war? You know, so I think those – you know, those are all things that people look – is this war? I don't know. You know, and I think that the – right now the – (inaudible) – certainly with the number of things that have been happening, there is a lot of uncertainty, and I think a lot of people are very nervous that, are we on the brink of a cyberwar or is it just a breach, it's a mistake?

MR. : You made a great distinction yesterday – (inaudible) – you mentioned there is – you know, we – (inaudible) – seem an act of war from the cyber perspective; however, there is a Cold War taking place in the commercial side. And I thought that was an interesting distinction that you made. What are your thoughts on that?

DIR. ROGERS: I mean, clearly, as a government, we're trying to work – or certainly in the Department of Defense we're trying to work our way through those kinds of issues.

You know, one of the questions that we always ask is, so what's the intent of the action? Is the desire here – I mean, is the fact of (getting/giving ?) access, does that in and of itself trip some threshold? Is it because of what the purpose of that access is for? Is it – well, if it's a criminal act, want to steal our information – (inaudible) – criminal act or – (inaudible) – cell, do you have a different threshold if it's – (inaudible) – intellectual property and another threshold if it's – (inaudible) – steal government – (inaudible)? Is it another threshold – (inaudible) – and we want to change the data? Is it different threshold it's – (inaudible) – and conduct destructive activity – (inaudible) – want to change data – (inaudible) – potentially want to destroy it, we want to destroy infrastructure – (inaudible). So one of the things we're trying to look at is, how do you define it intent clearly here from a military purpose – (inaudible) – because remember, those are generally – (inaudible) – talking about what is offensive. From a military standpoint, those are some of the nuances in the traditional ways that we have looked at defining actions – (inaudible).

Attributions is getting a whole lot better – (inaudible) – I would tell you. And I guess it's just – it's everybody knowledge raises – I'm much more confident in the attribution piece than I was.

If you go back five, 10 years ago – I've been doing cyber on and off in the Department of Defense for, jeez, a little over 10 years now, and if I think back to the – my earliest days, you know, real concern about what kinds of offense – (inaudible) – can you get the decision-maker as to the attribution, what the source is or what the intent – (inaudible). I remember 10 years ago – (inaudible) – boy, are we going to be able to, within a military framework, retain or improve and train a cyberworkforce, that has been a pleasant surprise. We have been able to do that. I am really impressed with the uniformed cyberworkforce, both in our ability to get quality people, to train them to a level where they provide true value and our ability to retain because what I try to remind people is, look – (inaudible) – going to compete – (inaudible) – where the Department of Defense will compete – and this is true on both the U.S. Cyber Command and NSA – is because we have an ethos and a culture of service to something bigger than ourselves; because we have a mission that resonates with people; because we do something that matters; because we do something, quite frankly, and – (inaudible) – that you can't – (inaudible) – and because we're going to give you responsibility at a young age – at a younger age, in some sense. And for example, if you like travel, we're a global organization, so if you want to live – (inaudible) – you can do that. Now you can do that (for one ?) – (inaudible) – do that with a lot of the major transnational corporations (which – you can do that ?). It's those things that are going to enable us to compete in the workforce, because we're all – many of us – we're all here – we compete for the same talent.

It's not with the money. We are not (in the department ?) going to compete on pay. We could make the top dollar, and that's not us. We'll compete on the other things. That's what we're going to be doing to make a difference, and I see that every day from the men and women that I am so honored to (team with ?) at U.S. Cyber Command and the National Security Agency. I will tell you they come to work every day and ask themselves, what do I have to do to get the job done? But how do I do it in a way that fully complies with the laws and policies that I have? They do not – do not – think to themselves, you know, today I just want to indiscriminately use the capabilities that are afforded me to just go out and see what – fill in the blank – or to use the authorities and the capabilities that are granted to me, provided to me, to just indiscriminately – (inaudible). That is not – that is not – what the men and women at the National Security – (inaudible).

I'm proud to be a part of that team. I am proud to be the director of that. I think the work they do is critical for us as a nation. It's very important to the greater world around us.

And we need the dialogue we're having. (There's a reason for that ?). We need to ask ourselves, as a society, what's the right balance? What are the trade-offs – (inaudible) – and our privacy and our rights – (inaudible)? It is not either/or. It's got to be both. But we need to have a dialogue about that, and arguing that it's all about one or it's all about the other I just think is a losing proposition for us as a nation. A world with great security but no freedom is not (really

place ?) that interests me, and the flipside, a world with great freedom but (no ?) security would also – (inaudible). So it's how are we to find that middle ground where we can do both, and we do it in a conscious way. We have a well-informed discussion. We ask ourselves, as a society and a nation, what are we going to do about it? That's important for us as a nation, and as the director of NSA, that is something that I view as a positive, as something (real and alive ?).

But with that, I think we've run out of time. Let me just conclude by saying thank you very much for your willingness to spend time here today with CyberMaryland on how we collaborate and try to increase the level of cyberknowledge and capability here in Maryland area. (Selfishly, all I want to?) gain from that is the individual here in Maryland who's interested in partnering – (inaudible) – workforce and – (inaudible) – we have around here. I thank you for your willingness to give up your time and – (inaudible).

MR. : Sir, I say this a lot at a lot of our events, certainly, around the state – and I particularly wanted to remind people that it is an honorable profession, and thank you and the people that work with you on your team for your service. It's incredibly important to remind this – you know, our society that it is an honorable duty. Thank you very much.

MR. : Yeah, I just want to thank you for being here. I want to encourage the young people look for inspiration to Admiral Rogers, as older guys like us have. Thank you for your work, and (we greatly ?) appreciate you being here. Admiral, thank you for that.

DIR. ROGERS: Thank you.

MR. : And next time we'll see you again.

DIR. ROGERS: All right. Thanks, Jim.

MR. : Thank you very much. (Applause.)

(END)