National Security Agency

Stanford University Address

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

Moderator:
Amy Zegart,
Co-Director, Center for International Security and Cooperation,
Stanford University

Location: Freeman Spogli Institute for International Studies,
Stanford University, Stanford, California

Time: 4:00 p.m. PST
Date: Monday, November 3, 2014

Transcript by
Federal News Service
Washington, D.C.

AMY ZEGART: Good afternoon, everyone. My name's Amy Zegart. I'm the co-director of CISAC, the Center for International Security and Cooperation. I'm also a senior fellow and associate director of

academic affairs at the Hoover Institution. On behalf of both institutions, I'd like to welcome you to today's discussion with Admiral Mike Rogers, commander of United States Cyber Command and director of the National Security Agency.

I just want to remind everyone that we are live-streaming this event. Members of the press are here. And all of the remarks and Q-and-A today will be on the record. Admiral Rogers will provide a few opening remarks and then we're going to devote the bulk of our time together with questions and answers and discussion.

Now, Admiral Rogers' visit today is part of a growing cybersecurity program run jointly by Hoover CISAC here at FSI that included our first cyber boot camp for senior congressional staff, both Democrats and Republicans, in August here at Stanford, and that is expanding quickly into a growing campus-wide cybersecurity initiative. So stay tuned.

Now it's my great pleasure to introduce our speaker this afternoon. In March of 2014, Admiral Rogers assumed his current position as director of NSA and commander of U.S. Cyber Command. Prior to this appointment, he was commander of U.S. fleet Cyber Command and U.S. 10th fleet, which were created and recommissioned in 2010 to assume responsibility for the Navy's cyberwarfare programs, including information operations, electronic warfare, signals intelligence and space missions. As Admiral Rogers described it when he took command: If we've given you access to a keyboard, you're operating in our domain.

He also served as director for intelligence for both the Joint Staff and U.S. Pacific Command, as special assistant to the chairman of the Joint Chiefs of Staff, as director of the chairman's action group, one of the most important advisory bodies in the U.S. military. He's had a distinguished career of over 30 years in the Navy, both ashore and afloat, with extensive experience in cryptology, intelligence collection, computer network defense and information warfare.

He graduated from Auburn University, receiving his commission from Naval ROTC. He is a distinguished graduate of the National War College, a graduate of highest distinction from the Naval War College and an MIT Seminar 21 fellow. Now, when he was offered the current job that he now holds, Sara Sorcher from the National Journal wrote that if President Obama has posted a classified ad for the job it might look like this – and I just want to read it to you briefly.

Wanted: Military officer to lead National Security Agency and Cyber Command. You will be the target of intense criticism from civil liberties advocates to members of Congress. A majority of the public opposes the once-secret phone and Internet surveillance you will do. Your future workforce is already demoralized after massive leaks. Your boss, who happens to be the president of the United States, wants you to reform a massive spying bureaucracy. You will inherit some enemies – not just the alleged terrorists you're trying to hunt, but a rogue former contract employee who won't stop telling all your secrets. You will be in the media spotlight, trying to get the public and irritated allies to trust you, but all the details of your work will be the shadows.

Whatever you think of NSA's programs, it's clear that running Cyber Command the National Security Agency are no easy jobs. We are so pleased that Admiral Rogers has come here today to share his thoughts and answer what I fully expect and hope will be thoughtful and tough questions from our Stanford community. It is an honor to have him here. Please join me in giving Admiral Rogers a warm, Stanford welcome. (Applause.)

DIRECTOR MICHAEL ROGERS: Thank you, Ms. Amy. Thank you. So, can you hear me in the back? We're good? So what I thought I'd do is make a couple comments and then open it up to questions, because I'm really interested in a dialogue. So, first, you heard these job titles. What do those really mean? So as the commander of United States Cyber Command, the organization has three primary missions. First is to defend the department's networks. The second is to create the cyber workforce and oversee its operational deployment in the department. We are building a dedicated cyber mission force, if you will, within the department of about 6,200 people.

That'll be broken down into a series of teams and apply both to support commanders within the department but also the third mission set for us. When directed by the president or the secretary of defense, we will apply our capability to defend critical U.S. infrastructure. The United States government has designated approximately 16 different segments within the private arena has having critical national security implications. So think about power, fuel, aviation, the financial infrastructure – there's 16 of them. Those are the three primary mission sets in U.S. Cyber Command, largely a very traditional military kind of organization.

The National Security Agency has two primary missions. One of them has gotten a lot of attention, the foreign intelligence mission, in which we use our capabilities to generate insights as to what nation-states, groups and individuals are doing in the world around us – particularly those who might want to do harm to us and our allies and friends around the world. The second NSA mission that doesn't get much attention, but I think is really critical in the future, is we also have an information assurance mission.

We are tasked with helping to define the security standards for classified systems in the Department of Defense, partnering with NIST and other elements within the U.S. government to do the same more broadly across the U.S. government and, increasingly in the world we're living in, applying our mediation and mitigation capabilities in terms in cyber defense to support other elements within the U.S. and, when requested by the Department of Homeland Security or the Federal Bureau of Investigation, we also are now starting to provide that capability to support others outside the government on a case-by-case basis, normally associated with one of those 16 critical segments.

I am generally out in the valley at least every six months. In the seven months I have been in command, this is the second time I have been here. I generally come out for three reasons: First and foremost, I am interested in a dialogue between the men and women, students, the corporate sector in this area about what NSA is and is not. And I want to understand the perspective of others. To do that, we got to

have a dialogue with each other. The second reason that I try to come out here twice a year is because, quite frankly, the days when the Department of Defense drove technical innovation for the U.S. are way behind us.

You know, the Apollo Program and the days that – if you're old enough. I mean, I was a NASA-obsessed kid. I could still rattle off everything you want to know about the Apollo Saturn V rocket. Couldn't get enough of it when I was a kid. The days when the U.S. government is going to be the driver for technology, those are fundamentally behind us, I believe. And this area in the valley is a primary driver for technical change within the nation and the broader world around us. And so I want to try to make sure I understand that change.

The third thing is, we're competing for much of the same workforce. So one of the things I'm interesting in talking to the corporate sector out here is, so, tell me, how do you recruit? How do you retain? How do you train and educate? How do you build a workforce that remains aligned with the technical requirements of the technical focus that both the private sector and NSA in this area have? And how do you keep your workforce relevant? So I'm always trying to pick the private sector's brain about, so, tell me what works for you, what doesn't work for you?

We have fundamentally different models in that regard. For you out here and in the private sector, particularly in the IT arena, turnover's a constant. You know, the average person's in a job out here about two and a half years, three years if you're lucky. Very different from our model. Most of our workforce, once they come in the door, tends to stay with us for decades because they really love the mission, they love what they do. We're very fortunate. They have a set of skills where, quite frankly, they could be making a whole lot more money on the outside than they do working for us. But we're very blessed with the workforce that really feels strongly about the mission and what we're doing to try to help defend the nation.

So that's what the primary aspects of the jobs are. That's why I try to get out here about every six months or so, as I've said, this is the second time in seven months I've been out here, and what I try to do when I'm out here. And with that, I'm very interested in what's on your mind because I'm mindful we got less than an hour. So, please, I'll be glad to answer any questions on any topics.

MS. ZEGART: So I'm going to do some calling on folks. And I want to encourage our students who are here to make sure you ask questions because, you know from class, we can also call on you. (Laughter.)

DIR. ROGERS: So we got that going for you.

MS. ZEGART: Yes, in the back.

DIR. ROGERS: And I'll repeat the question if you can't hear it. Go ahead, sir.

Q: (Off mic) – extraordinarily – oh, thank you – extraordinarily close – (off mic) – Australia, New Zealand and – (off mic) – which – (off mic) – better term, the predominately white former British – (off mic).

DIR. ROGERS: I would argue, because it's a reflection of our history and the close historic nature of our relationship with those five. Every one of those five, we have fought major conflicts with. We have bled together. Not that those are the only five nations, but we've got a long history with all five of them. We're united by a common language, for example – there's part of it that make it a little easier, in some ways. But largely, it's because of that history. This is not a construct that was just created in the last five or 10 years. This is something we have literally been doing for over half a century. That's really the reason – much less nefarious. (Inaudible.) Sorry, it's just not the nature of it.

MS. ZEGART: So let me ask that you please identify yourselves so we all know who you are when you ask your question, OK?

Patrick.

Q: Hi. My name is Patrick Sorenza (ph); I'm an honors student here. I'm writing an honors thesis evaluating the analogy between the development of early nuclear deterrents and the development of cyber deterrents now. So my question to you is – in charge of Cyber Command and the NSA – I'm really interested – what do you think are the biggest challenges to the development of cyber deterrents today?

DIR. ROGERS: Well, remember, if you go back to the history of – we often have this discussion internally about what's a good analogy for deterrents? Is it the nuclear model? The challenges I see with the nuclear model are a couple of things. Remember, when we generated most of those foundational concepts of deterrence, the nuclear world was controlled totally by the nation-state. No individuals, no groups. Totally by the nation-state, and there were two. When we first started this initial dialogue, there were two nations – us and the Soviet Union – that had a nuclear capability.

I switched to cyber, and I go, hmm, cyber is pretty foundational in that almost every nation-state has some form of capability, and cyber has moved beyond the nation-state in the – (audio interference) – so the idea of using an exact template from the nuclear world, I think, is tough. Now, the flipside is, I do not yet know, in my own mind, what the right answer is.

The concern I have is, look: Right now, if you look at most nation-states – groups and individuals and the activity they are engaging in in cyber, very broadly, most of them seem to have come to the conclusion that there is little risk of having to pay a price for this in real terms. My concern is that perception that there's limited risk has the potential both to encourage nation-states, groups and individuals to be more aggressive in this area, but also, potentially escalatory, and that's not a good thing for us – I would argue, for the world writ large, that's not a good thing.

So I'm still trying to come to grips with the, how you do it, but I'm trying to ask myself, how do we get to a sense of rules, norms and expected behaviors in this environment, just as we have every other environment I've ever worked in as a military guy. You knew exactly how far you could push, and you knew exactly, in broad terms, what was going to trigger a response on the other guys' part.

And I was always struck by, if you look at the Soviets again and you talk about nuclear deterrence – even in the midst of two fundamentally different visions – even at the times we both had the means to literally incinerate each other, we still were able to create a series of norms and behaviors over time that you knew just how far you could push each other. We knew that tactically – you know, as a naval guy out at the individual unit level on ships, as we were aggressive with each other, you knew exactly how far you could push, and when you were stepping over the line and what was escalatory. We haven't been able to do that yet in cyber, and I just think we have got to get there. Otherwise, the trajectory we're on – just look at the activity that you're seeing. Pick up a paper, go to your favorite site. You get news the way you like – and every day we're dealing with this, and it's only going to get worse.

MS. ZEGART: Yeah, right here. Yep.

Q: Admiral, Danny Yadron. I cover cyber for the Wall Street Journal –

DIR. ROGERS: I'm sorry, did you say Danny or –

Q: Danny.

DIR. ROGERS: I apologize.

Q: I cover cyber for the Wall Street Journal. Your counterpart today at GCHQ and previously, Director Comey at FBI have said U.S. tech companies can get in the way of law enforcement, or will, with some of the steps they're taking with encryption. And I was wondering if you had any thoughts on that.

DIR. ROGERS: So I think, fundamentally, we're trying to come to grips with the following issue, in some ways. How do we try to strike that balance where there is a means to employ a lawful mechanism to gain insights about the commissioning of what FBI Director Comey is talking about? And I apologize; I haven't heard from GCHQ today, so I'm just not (smart ?) on that particular aspect of it.

MS. ZEGART: That's because we've been keeping you busy.

DIR. ROGERS: That's right. (Chuckles.) Although I spend a lot of time with my GCHQ counterpart. What we're trying to come up with is, so, how do we deal with providing insights in criminal behavior in a legal framework as opposed to just saying, hey, look, we're just no longer going to allow somebody to access that? We're just going to put an encryption level in, for example, that's going to preclude the ability to do that. And I think what Director Comey is trying to come at is, hey, look, is there some mechanism in the technical side that we can create that using a legal, lawful framework, where, under specific

conditions, as granted by a court, we could still gain access? And what he keeps talking about is the criminal piece. And you'll often hear him talk about child pornography, exploitation of minors, et cetera. That, I think, is what we're trying to come to grips with.

This is a good example of where we just have a fundamental mismatch, in some ways, between the state of technology and the legal and the policy frameworks we're still trying to deal with and we're trying to collectively work our way through, how are we going to make this work? How do you try to address those two competing and valid viewpoints? And, you know, I'm not who jumps up and down and says either side is fundamentally wrong. I understand what drives each side to their viewpoint on this.

MS. ZEGART: If I could, I'm going to take the moderators' prerogative to ask a follow-up question to that.

DIR. ROGERS: Yes, ma'am.

MS. ZEGART: I know I'm in trouble when you say "yes, ma'am." (Laughter.)

DIR. ROGERS: Yes, Ms. Amy.

MS. ZEGART: One of the things that I've been hearing a lot in the valley is that industry is very concerned about NSA – or evidence that NSA has been undermining encryption standards, not just because it's NSA, but if NSA can do it, China can do it. Other nefarious actors can do it. And so the question is that, as you look in the future – if NSA were to find a way through encryption standards, how do you weigh what the right thing to do is when it comes to communicating that with Americans?

DIR. ROGERS: So I'd make two points. The first – what I tell the team as the new guy is, let there be no doubt that a fundamentally strong Internet is in the best interests of us as a nation and the world around us. Secondly, in terms of, how do we strike this balance? The president has been very specific to us – hey, look, the balance I want you to strike will be largely focused on, when you find vulnerabilities, that we are going to share them, and the greater – I mean, by orders of magnitude, the greatest numbers of vulnerabilities we find, we share.

But he also talked about, hey, look, there are some instances in which we are not going to do that. And the thought process, as we go through this from a policy side as we make this deliberate decision – the kinds of things we tend to look at are, how foundational and widespread is this potential vulnerability? Who tends to use it? Is it something that, you know, you'll generally find in one particular nation-state or a particular segment, or is this pretty wide across a large swathe for the U.S. and for others? How likely do we think others are able to likely find it? Is this the only way to potentially – for us to generate the insights? Is there another alternative here that we could use?

Those answers then generally shape, so what did we decide, hey, look, we're going to share this, or do we decide not to? Again, by orders of magnitude, the default mechanism for us is, we share the vulnerabilities we find, and much of it you will never even hear about. You look at, in the immediate aftermath of Heartbleed, for example – the first media reporting I saw said, hey, NSA knew about this vulnerability and has been exploiting it against the U.S. for an extended period of time, wrong.

This first was outed, if my memory is right, on the 7th of April – first that we were aware of it. On the 8th of April, within 24 hours, using our information assurance mission, we developed a patch – a counter to the malware, and we shared that with the private sector. And what we said was, you don't have to tell anybody this came from NSA, just do it, because it's part of our mission. It's that information assurance mission. You know, it's just something we generally don't talk about all that much, but it's an interesting internal issue for us. Do we need to talk about – (inaudible) – that information assurance mission?

MS. ZEGART: Whit.

Q: Whitfield Diffie of – (inaudible) –

DIR. ROGERS: It's been too long, Whit, since I saw you. (Chuckles.) We were just in a session and Whit was there and asking a question.

Q: The only thing among the Snowden revelations that I can say really bothered me – thank you – was the charge that NSA had tampered with missed security guidance on key production, particularly something called dual elliptic curve randomizing. And I'm very concerned just what you – you know, I doubt you're going to say, yeah, we'll do things like that in the future, but what is being done to guarantee that IAD is not slave to the much larger budget of (SIGNIT ?)?

DIR. ROGERS: Well, first of all – no, for those of you not inside the organization, IAD is an acronym that goes to our information assurance directorate. So it's one of those two mission areas. And at times, you can see some people would argue, well, do you have a conflict between your foreign intelligence mission and your information assurance mission, and are there different perceptions here that drive you to different conclusions at times? In fact, there was a discussion at some point about, hey, maybe we need to separate those two. I strongly disagree with separating them because I made the following argument, for me anyway: When you're trying to work penetrations of networks and you're trying to defend networks, the techniques and the insights you gain in both roles help reinforce the other. And you want them aligned because the insights we gain in the information assurance mission, because of some of the other things we do, are very important. And I've argued, hey, look, if you split these two, you're going to hurt the information assurance mission.

With respect to this, in the end, hey, look, they've got one boss, and I'm the accountable guy. That's the way in broad terms we try to strike this balance between the two. As I've told you, what I have told the team as the new director is, let there be no doubt a strong Internet is fundamentally in our best interest

as a nation. If we've got to work harder, then we've got to work harder sometimes, guys. That's what they pay us to do.

MS. ZEGART: Scott.

Scott Sagan, senior fellow here at CISAC and FSI, professor of political science.

DIR. ROGERS: Hi, Scott.

Q: The Snowden – back on the Snowden issue, Snowden was widely considered to be the greatest insider threat that we've had in recent years. Could you share with us your views on his motives and how he got away with it and what you've done to try to, in terms of background checks, security assurances, personnel reliability programs – (inaudible).

DIR. ROGERS: So I'm not going to talk about his motives. That's his business and he will articulate those over time, I assume. I certainly hope he (does/doesn't ?).

The second part of the question really was, so, tell me what you've done to preclude that happening again? So a series of technical challenge – it is – there's an interesting challenge there in terms of I wondered at times as the new guy, were we in no small part the victim of our own cultural ethos, where we tended to trust each other. The – one of the biggest challenges, but as the new guy that I see a workforce that feels almost violated as a result of all this, you know, that one of their own did this, you know, so watching them.

Now, trying to strike a balance, because there are some who would argue – because at times I'll hear the workforce tell me, hey, look, one individual engaged in a criminal act and you're making the rest of us pay for this, because I get that at times from some elements of the workforce – which you could understand if the roles were reversed and you were in those shoes. And the workforce says, wow, you know, if you're going to start to consider very intrusive security measures, why am I paying a price for that? Hey, I didn't do anything wrong.

So what we have tried to do is a couple things. I tried to make sure we have a conversation with the workforce in which we walk through what we're doing and why – why we're trying to strike this balance. I remind the workforce, look, we all raised our hand and we all signed – to include he – we all signed a formal agreement that says, hey, look, we acknowledge the significance of the information we are (granted ?), we acknowledge and recognize that the compromising of this information potentially would do significant damage to the nation and we all agree that not only while we're an employee but forever we will agree not to divulge this information. And we have a – hey, if you decide you want to write a book, fill in the blank. We've got processes for how you do that.

So I remind the workforce, hey, we all signed up to a higher level of scrutiny and a higher level of security. We all know that that's part of the job. We all agreed to that, whether it's polygraphs, whole

lots of other things that we do. I mean, I can't stand them. I'd be the first to admit I hate them, but it is as – but I acknowledge that it's a good tool for us and if I'm going to do this, I go into it with my eyes open, even though part of me goes, oh, man, you know, I've got to sit down and get wired to a machine. Because we have one standard for all of us. It doesn't matter if you are the four-star running the organization or you're a junior individual. I've got one standard for all of us when it comes to our security framework.

We've sat down and taken a look, analyzed it from a technical standpoint. I also remind the workforce, look, this isn't just about technology, you guys. Again, it's interesting to look at cultures. Technically focused organizations generally tended to default to technical solutions and the technical prism to look through when you're trying to assess a situation. We're no different in some ways. So I'm trying to remind the workforce this is more than just technology. This is also a part about us being professional. And when you see unprofessional behavior in the workforce that doesn't make sense, hey, we ought to ask, does this make sense? Those are the biggest things. There's a few other odds and ends. I'd rather not get into the specifics, but in broad terms.

Now, people often say to me, so, when it's all said and done, are you going to guarantee there's not going to be another compromise. Ad I say, wait a second. Now you tell me how you guarantee that we're not going to have a compromise.

At times, I have some people telling me, hey, what this should show you is, you can't trust contractors. And I'm like, what? I don't draw that analogy from this. If you look historically over time, the biggest compromise – I'm a naval officer – the biggest compromise in the history of the United States Navy from an intelligence perspective was a uniformed warrant officer. He sold their cryptographic standards to the Russians.

Biggest arguably in DOD history, PFC Manning, WikiLeaks issue, a uniformed member. You go to the FBI, biggest compromise they ever had was an FBI agent. You go to the CIA, biggest compromise they ever had was a member of the CIA. So this idea that you can't trust contractors, I just don't think I'm concerned about the long-term implications of that.

MS. ZEGART: Over here, in the plaid shirt.

Q: Hi, my name's Varun (ph). I'm an undergraduate here.

DIR. ROGERS: Hello, Varun (ph), how are you today?

Q: Good. How about you?

DIR. ROGERS: I am in California. I am not in Washington, D.C. And you look out that window – man, is this a typical weather day out here for this time of year?

Q: (Inaudible.)

DIR. ROGERS: It's cold. (Laughter.) Man, I'm like – you know, you could live out here.

Q: Yeah, so, if you had to convince a Stanford computer science student – which I am not – but if you had to convince –

DIR. ROGERS: But would you like to be? Would you like to be?

Q: No. You're the director of the NSA. (Laughter.) If you had to convince a Stanford computer science student to work for the NSA, like, how would you convince him or her – him or her, even if that student was, say, disillusioned by the U.S. government and politics, the NSA, interested in capturing large quantities of wealth, interested in affecting, like, visible social change? Just curious.

DIR. ROGERS: (Check, check ?). So I generally say there's five things, because I'm the first to admit, look, if we're going to make this about money, we don't stand a chance. It has nothing to do with the current situation we're in. I'd have said the same thing to you three years ago. If it's just going to be about money, it's a losing proposition for us.

There are five things that I try to point out to people. Number one, we have an ethos and a culture that I think you want to be a part of. Number two, we're going to give you the opportunity to dedicate yourself to something that's bigger than you are, to serve the nation. Number three, we are going to give you an amazing mission: something that I think is an important mission for the nation and for allies and friends around the world. Number four, we are going to give you the (opportunity ?) to do some neat stuff that you can't legally do anywhere else. (Laughter.) Number four – or I apologize; I'm probably off on my number sequence – we are going to give you a lot of responsibility early. That's part of our culture. We generally – when we start you, we try to get you responsibility early. Those are the things that I would argue really make us different and why I would argue, hey, NSA is a place that you want to work.

As I said, our model is – the biggest challenge for us is not necessarily retaining people – not that there aren't some areas – I don't mean to imply there are some areas where, just like everybody else, we've got some challenges that we're working through – but as I said, our norm is, most of our work staff, workforce tends to stay with us for decades. The biggest challenge for us, in some ways, is more getting people in the door in this environment. So, again, it's another reason why I'm standing before you today, because many – how many of you are computer science backgrounds? All right. Many of you are potential future employees that I want to compete for. Again, you've got to decide what's right for you, but I'm not going to shrink from the idea that I think NSA is an amazing place to work with an important mission that matters to this country.

The four things I always tell the NSA workforce are: Remember, when all else fails, use the following four touchstones: We obey the rule of law. Two: We are accountable to the citizens we defend. Three:

When we make mistakes, we stand up and say we made a mistake because I wish I told you that I worked for an organization that's perfect but, for example, when you're entering a, you know, nine digit IP address and you get one digit wrong, it's amazing where you can potentially wind up. And lastly: We don't cut corners. We've got one way to do things and we do things the right way. We stay within law, we use the authority and the policy that's been granted to us and we don't cut corners. You do that, we're going to be fine. I will take the heat from the outside world; that's what they pay me to do. I need the organization focused on mission and I need you with your head up and focused on what we're doing because the country and our allies around the world are counting on us. That's important to me, to never, ever forget we're there for a reason.

MS. ZEGART: We'll go to this side of the room. Yes.

This is a big pocket question in here. You guys got –

Q: Dunkert Madison (sp).

DIR. ROGERS: Hey, Dunkert (sp).

Q: Admiral, you've got a great reputation, by the way. From what you do –

DIR. ROGERS: Don't say that to my wife.

Q: – and the way – and the way you're doing it but the thing that concerns me is, in reality, what kind of real cooperation are you getting from the heads of the other agencies that failed us so badly at 9/11?

DIR. ROGERS: I don't – well, I'll let others agree or disagree with the characterization that – Dunkert (sp), I'm not sure I agree with the characterization, but I have no complaints with the support I am getting. There's approximately – I think now we're using the number 17 – there's approximately 17 elements within the U.S. intelligence community. I have no complaints with the support of my 16 teammates. If anything, quite the opposite. In fact, I often tell the Director of National Intelligence, Jim Clapper, man, I can go back five, 10 years and – not as a director but as a guy who was at the table in a different job at the time, a little lower level – I look at the cooperation, I look at the partnerships that we had then and I look at the way we have it now, I have great respect for the men and women I partner with, from John Brennan at the CIA to Director Comey at the FBI, David Shedd at DIA, Robert Cardillo at NGA – you fill in the blank – Betty Sapp – you can fill in the blank, the 16 others. We all work very well as a team. I'm very proud to be a teammate with them and I have no complaints about what they're doing in terms of a support to us.

MS. ZEGART: Jennifer?

Q: I'm Jennifer Granick, the director –

DIR. ROGERS: Hi, Jennifer.

Q: - – hi – the director of civil liberties at Stanford Law School's Center for Internet and Society, and my question is about the information collection and the relationship with Five Eyes. And what we've seen in the news is that, in conjunction with the United Kingdom's spy agency, GCHQ, in particular, there are collection activities going on. For example, hacking the internal data centers of Google and Yahoo because there's no encryption there or GCHQ's collection of unencrypted Yahoo video camera chats and capturing stills from that. And then just a couple days ago, we learned from a Privacy International lawsuit that GCHQ has been receiving raw communications data from NSA –

DIR. ROGERS: Since it's a lawsuit, I assume it's actually an allegation as opposed to a fact.

Q: It's a – it's documents that they received from GCHQ as part of the litigation – ongoing litigation. And so the – and that, then, GCHQ's procedures for treating that data don't accord with what they say their procedures are for curating other data that protects the rights of their citizens. So when we see this kind of relationship and this closeness and the history and this data sharing, what can you say to Americans who are concerned that countries which don't have rules about targeting Americans or about minimizing Americans' data are then giving that information to our government and then our government is not having to follow the rules that are so often pointed to as being there to protect our privacy. We don't protect their privacy, they don't protect our privacy and then we just trade. How can you – what's your response to that concern?

DIR. ROGERS: Check. So I'd make a couple of points. First, we do not use any foreign partners as a vehicle to overcome or bypass U.S. law, OK, number one. Number two, when we partner with others, pick anyone in the – in the Five Eyes, for example – Five Eyes was the framework that you provided – when we partner with our Five Eyes teammates, we remind each other that we have specific requirements that we have to meet. So for example, when I share – we, NSA – share information with our GCHQ counterparts, I make them go through a very rigorous regime in control of the data we give them and particularly when it comes to U.S. persons. I require them to go through training, I control the systems that have access to it, I mean there's very specific things that we do when I sit down with my teammates in the United Kingdom about the kinds of things we do together. And we do not use the partnerships as a vehicle to bypass the legal frameworks that we have to work under. I'm comfortable what we do with our foreign partners – the examples you've cited, the Five Eyes – I'm comfortable what we do with our Five Eyes. And I always remind them, hey look, neither one of us – any of us in this arrangement, guys, we're not going to compromise ourselves in the name of a relationship, we're just not doing that. And there's specific restrictions on what we can and can't do and I always tell them, look, I expect us to abide by that.

Q: (Off mic.)

DIR. ROGERS: No, we don't, as a matter of general policy, provide specifics because part of the concern in doing so – so, if you're an opponent out there and you're trying to figure out so how do GCHQ, how

do NSA – pick one of the Five Eyes – how do they do what they do or how do they partner? How do they do the work they do? I'm a little leery about getting into the specifics of that because my concern is – not that it isn't a valid question, but my concern is that there are individuals and groups out there – and even some nation-states – that I watch them change their tactics and the ways they do things as a result of discussions. I'm watching that every day right now as a result of the media leaks over the last 15 months and I'm watching the impact it has on mission and our ability to meet those security requirements for the nation.

MS. ZEGART: Phil?

Q: Admiral, Phil Taubman, consulting professor at CISAC.

DIR. ROGERS: Hey, Phil.

Q: I'd like to ask you to put yourself in the position I know that you're partly responsible for as NSA director, which is assessing the threats to the nation. When you go to bed at night, what do you worry about?

DIR. ROGERS: Well, that's good – that's a better way – normally, I get the question, you know, when you go to bed, what keeps you awake? And the first thing I say is, look, with the hours I'm working, I've got no problem sleeping. (Laughter.) In terms of what my concerns are?

Q: What is the greatest threat to the United States?

DIR. ROGERS: I'm really – oh, I'm really concerned about two things: one I would characterize as a near term and the other, hey, longer term.

Near term, you know, you just want to knock wood because I'm thinking to myself, it has been 13 years since we have had a major transnational threat be successful in the United States and it ain't from a lack of effort on the part of many groups around the world today. So I'm always mindful about, man, how much longer can we keep this string going? You know, when do we make a mistake, when do we fail to see something, when do we fail to make a connection that leads to a successful attack on U.S. soil from a transnational perspective? Because I'm not – NSA – I'm not an internal security guy; the lone wolf kind of scenario we look at, that's not what you've optimized us to do. We're a foreign intelligence organization.

Longer term, the cyber piece really concerns me because I'm watching activity levels really ramp up. We have yet to be able to come – not because people aren't trying and because they're not thoughtful, but we have yet to be able to come to a broad policy and legal consensus about how we deal with some of the issues in the cyber arena. And, you know, part of me is going, look, we know we've got these issues, can't we get that consensus to deal with this? Is it going to take a crisis to wake us up to say, man, how did we get here? You know, I don't want to be at the end of another 9/11 commission going, so how did

we get here? We know the challenges out there that we've got to deal with. But let's face it, it is incredibly challenging in the nation that we are all living in right now to achieve political consensus and the will to deal with hard problems. We are just not having luck as a nation in doing so. That's not a criticism. I'm not trying to throw stones at anybody else, I'm trying to say look, hey, we've got to be realistic and up front with each other. That is the environment we find ourselves in now. It's an interesting dilemma for us, in some ways somewhat tangentially related, for NSA – again, big fan of history.

So you go back and you look at the framework that we use today for compliance and oversight – really comes out of issues from the late '60s and the 1970s. And so in the late '70s and the '80s we create a legal court infrastructure, the FISA Court, to address legalities in the generation of permissions to conduct some of the things we do under the law.

The second thing we came up with, coming out of some of those activities in the '60s and the '70s, was, hey, look, we want to use Congress as the elected representatives of our citizens, as the vehicle to conduct oversight for the intelligence infrastructure.

Fast-forward 40 years later, and collectively, as a nation, we question government broadly, we question government institutions, we have much – fairly limited faith in Washington – and that's where I live – but we have limited faith in Washington, incredible frustration over the mechanisms of our governance, whether it be the legal frameworks, the courts, the Congress.

So one of the things that I talk to the team about is, so what do you do when the very structure you created to provide oversight of what we do is no longer trusted in the same way that it was when we came up with this idea 40 years ago? You know, what are we going to do as a nation to try to engender that kind of confidence, so that U.S. citizens feel that you have a level of knowledge about what's going on and you have a level of comfort about what's going on?

That is an interesting challenge for us in the current framework, when it's hard to achieve a political consensus, when we question institutions, when we're losing faith in many of the mechanisms of government – governance that we've traditionally counted on. We got to work our way through this as a nation and figure out so how are we going to deal with this, how do we engender that confidence, you know, that goes to that number two tenet of the four I gave you. We are accountable to the citizens we defend. A way we're accountable right now is through that oversight framework and that legal framework. You know, to collect against a U.S. person in broad terms, we got to go to a court of law, got to get a warrant to let us do that. So what do you if people don't trust that framework as the vehicle anymore? We're going to have to work our way through this.

Could I ask one favor? Could we ask questions for people who – not that I dislike your questions, but all of you were in the previous session, so you had a chance to talk to me before. Could we try to talk to people who haven't necessarily had the chance to interact?

AMY ZEGART: Sure.

Tom (sp). Tom (sp).

Q: Do I need a mic?

MS. ZEGART: Yep. Mic's coming right up.

Q: My question relates to how we more effectively address the various cyberthreats that are permeating throughout our society today. You mentioned that DARPA is no longer the great innovator – technology innovator that it once was. Many of us have a sense that companies – the defense contractors within the Beltway aren't the leaders in this effort, that so much of the technology is being developed out here today. I've had the opportunity over the 12 to 18 months to visit with several of the heads of the – of the individual military heads of cyber, and I certainly didn't get a feeling that they're spending an enormous amount of time out here.

You mentioned that you're out here every six months. My question would be, why aren't you out here every six weeks?

ADM. ROGERS: Because I got a set of responsibilities that span the globe – (chuckles) – and I got more demands on my time than I got hours in the day.

Q: But do you – do you have people that are out here? Are we –

ADM. ROGERS: I'm not the only one, necessarily.

Q: We just don't – I don't have the sense from the interactions I've had that we are as focused on taking advantage of the technology development that's going on in this valley and elsewhere out here today as we should.

ADM. ROGERS: Oh, yeah. I mean, we have a – we have a presence out here on a regular basis. Much of my team, particularly on the technical side, tends to be out here. This is just important enough that I tell the team, look, I personally am the leader of the organization. I'm going out there about every six months, even though the rest of the team is out here much more frequently than I am.

I think the broader – tell me your first name again.

Q: Tom (sp).

ADM. ROGERS: Tom (sp). I apologize, Tom (sp). I – no, no, Tom's (sp) fine. I think the broader challenge in some ways in the cyberarena is we traditionally in our governmental structure have put very strong boundaries between the private sector, the public sector, (in terms of the?) government

and often what we've tended to view as national security issues. Cyber, to me, spans all three of those segments. I think it is unrealistic to expect the private sector to withstand the actions of nation-states all by themselves. I equally think it is unrealistic to expect the government to deal with this all by itself. The challenge to me is how do we create the partnerships and the relationships that enable us to work together as a team.

Now that's not the norm for us, historically, as a nation. We have tended not to go down that road.

The argument I make is, look, I look at this activity, and I go, there are national security implications here for us that we ought to be able to harness the power and capacity of the government, partnering with the private sector, as well as the academic world. It's one reason why I'm at Stanford today. I think this is the third major academic institution, by chance, for example, that I have been to in the last week, the last two weeks. Part of this is I'm trying –wherever I'm going, I'm always trying to do outreach on the academic side as well.

We have got to create those partnerships in a way that enable us to actually share information and insight in a real-time machine-to-machine basis. We need to sit down and think about what kinds of information do we want to share.

Look, putting on my NSA hat, I don't want privacy data in the name of cybersecurity. Given the legal restrictions it then places on me, that really slows us down and complicates things. I don't want it in the name of cybersecurity.

So I want us to sit down and say, hey, can we define what's the data we need to share with each other? I mean, I occasionally will get people telling me things like, well, hey, look, we'll just do all this via email, and I'll send you the characteristics of the malware in an Excel spreadsheet. And I'm going, what? We can't make this work that – (chuckles) – that way. We got to do this machine-to-machine in near real time, and we need to sit down and talk about so what are the – what do you expect from me, what do I need from the private sector.

That relationship with the private sector also enables us to get into the technical piece. In many ways, though, I would tell you this is much less about technology, to me, not that technology's not a part of it, but it is much more about the cultural challenges, about getting organizations to change. That has little to do with technology and much to do about culture and ethos. And hey, my organization is every bit as challenged by that as anybody else. We're a big, big team that spans the world, and trying to get us to make changes along these lines is every bit as challenging as it is for everybody else.

So we're trying to pass cyberlegislation right now, haven't been able to get a consensus to do that. I sure hope we do. I think it's pretty critical for us. We've got to provide a measure of protection for legal liability for corporations. Otherwise there's – they're just not going to share as much, for very valid reasons, from their perspective.

So I think it's all about the partnerships we got to create. And if we don't do this, my concern is, cyber becomes a huge cost sum for us as a nation. The amount of money, the amount of time, the amount of focus that we will be – that we're going to be forced – if we don't change the trajectory to plow into this, this will have some major economic implications for us as a nation. We have got to change the trajectory.

MS. ZEGART: Yes, sir.

Q: Good afternoon, Admiral.

ADM. ROGERS: Good afternoon.

Q: Tom Hart (sp), Hoover Council member and retired Navy intel guy.

ADM. ROGERS: Hey, Tom (sp). How are you doing? When did you retire?

Q: '96.

ADM. ROGERS: All right. Thank you for your service.

Q: You talk about money. How much money are you spending or the ratio of money you're spending on offense versus defense on what you consider to be your long-term problem?

ADM. ROGERS: (Jack ?), I'm not going get into the specifics of – that concerns me a little bit.

Q: Not even a ratio?

ADM. ROGERS: (I go ?) – that even the ratio concerns me a little bit. Let me phrase it this way. We clearly have focused the preponderance of our efforts on the defensive side, but I remind the organization, look, our task, our challenge – putting on the U.S. Cyber Command hat in particular – is to provide policymakers and operational commanders with a spectrum of options for them to consider. And to do that, we've got to generate the spectrum of spy – of cybercapabilities, and it can't just be about the defensive piece.

So don't get me wrong. By far the clear majority of our focus is on the defensive side, but I'm always reminding the workforce that ain't the only thing we got to work about in the mission set. And I apologize. I'm just not comfortable –

MS. ZEGART: Can I follow up and just ask you to drill down a little bit more?

ADM. ROGERS: Yes, ma'am.

MS. ZEGART: And it's a follow-up to Phil's question as well. You talked about – you're worried about terrorism, you're worried about the cyberspace sort of threat landscape. Can you drill down a little bit and tell us how you perceive the cyberthreat landscape? We heard last week from a senior DOD – a former DOD official that he's really worried about critical infrastructure, particularly power grids, and the ability of our government to restore power after combined cyber-small arms attack. Admiral McConnell, in Texas a couple weeks ago, talked about he's most concerned about critical infrastructure, specifically the financial sector and vulnerability to cyberattack there.

DIR. ROGERS: Right.

MS. ZEGART: Former COCOM commander said he's most worried about the theft of intellectual property.

How do you stack up these and other cyberthreats when you think about your tiers of cyberthreats?

DIR. ROGERS: So, first for me, particularly as U.S. Cyber Command, I've got a mission that's directly tied to the 16 defined segments, so that tends to shape my immediate prioritization because I've got a mission that defines it, in some regard. When I look at the segments, I probably put the financial sector in the top position in the sense of strong corporate buy-in from the senior-most leaders in that sector that, hey, look, we got a cyber-issue we got to deal with; the ability to apply resources on a scale that hardly any other sector can come close to. If you look at JPMorgan Chase, you heard their CEO come out and talk about their baseline computer network defense budget, their baseline budget, is $250 million a year. How many corporate entities out there, how many academic institutions, how many private entities could afford a baseline budget of $250 million? The financial segment, though, strong recognition and willingness to invest resources.

The concern I have really on the opposite end is probably power, and health care is another one. The concern I have on the power side is we are already in the margins of capacity as a nation, if you just look at infrastructure versus demand. So we're already on the margins, as it were. The grid was built incrementally over time, and if you were building it by design from the ground up today, it wouldn't look like it does now, just the nature of a significant amount of capital investment over time in a very different world.

My power corporate teammates tell me, hey, look, you got to remember our challenge and our corporate model; we're a regulated industry. So to generate income, to invest in things like cyberdefense, I got to charge higher rates. To charge higher rates, I have to go to a regulatory body and get permission to do it. Hey, not a lot of enthusiasm, either in the general public or in the regulatory bodies we deal with, to jack up our rates. You know, so how do we generate the money that we need to make the changes?

One other comment about the sectors, if you will. The high end tends to get the most attention, but it – for example, if you – I said, hey, financial I'd probably put in the best position. If you look at the mid-

and smaller-levels of banks around the nation, they can't afford that kind of money. That's the level that in the financial sector in particular that really concerns me, is the mid- and the lower levels, because they just don't have the capacity and the resources.

The argument (sic) we're trying to make are, start at the top of the segment, partner with the biggest, and then as we generate those insights and we put in place capability, push it down all the way through the sector, into the smaller and the larger – to the smaller and the midsize ones. And that's what we're trying to do, working our way through the segment.

I always encourage, when I'm talking to private industry, I encourage you to get involved in whatever – we have the ISACs – different sectors that are out there, segments of the marketplace. I encourage you to get involved in the segment that you're a part of, because the insights of one can lead to the defense of many, I believe, and that's something very powerful for us. And it goes to that whole partnership and relationship piece. Man, we could be so much more powerful if we can gain the insights of many here. That would really be a positive.

MS. ZEGART: We have time for one last question. And we'll just – the lady right here in the blue scarf.

DIR. ROGERS: You're up, ma'am!

Q: I'm Kim Zetter. I'm –

DIR. ROGERS: Hi, Kim.

Q: Hi. I cover surveillance and security for Wired. I want to go back to your question that you answered about zero-day vulnerabilities and exploits, because last December the president's review board, which was tasked at examining some reforms for surveillance – one of the recommendations that they came forward with was that the government would not be able to use zero-day exploits unless for national security, extreme circumstances for intelligence gathering. Even then, they said that there should be a use-by date.

The president never responded to that. And then in your hearing in March, you were asked about these zero days, and you said what you said today, that the focus would be on disclosing rather than (using ?). There seems to be a – excuse me.

DIR. ROGERS: That's OK. Just take your time.

Q: I'm getting over a cold.

There seems to be a bit of a contrast, because the review board didn't think that that was happening. So is this a new policy that the government is using regarding zero days?

And the second question is, in your hearing, you referred only to zero days that were uncovered by the NSA. But the NSA uses – purchases a lot of zero days from contractors. So would the NSA be purchasing zero days for use and also disclosing them? What is the case here?

DIR. ROGERS: Well, let me talk about the first part first. And then – it was Kim, right? So Kim, you make sure and tell me if I've failed to understand what the question is.

So for the first part, I don't personally see a contrast. And what I tell people is, look, I have little interest in going back in the past. I'm focused on what I need to do and what I've been directed to do, and I'm focused on moving ahead. So when people ask me, well what about the past and what you guys did before, it's just not an area that really interests me. I haven't spent much time going back and asking myself, hey, look, walk me through the history of everything we've done on everything. I try to make sure I understand so what are we doing now, what's the direction we have, what are the constraints, the policies and the legal frameworks that are in place that we need to make sure we comply with. So the direction to us has been very clear: The default setting for you is going to be you're going to share the insights that you gain access to.

Q: So how does that work when you're purchasing zero days from contractors? Because clearly, the contractors are not going to want you to disclose vulnerabilities.

DIR. ROGERS: Again, we use the same standard.

Q: You would disclose zero days –

ADM. ROGERS: The default is – the default is, if I become aware of a vulnerability, the default is that we share it. Now, we also talk about, as you quoted from there, talk about the whole national security piece, and we use the methodology that I talked about previously. That's what I think I am under, so to speak, the direction I have to comply with.

MS. ZEGART: Well, we have come to the end of our hour. Thank you so much for spending so much time answering questions.

Please join me in thanking Admiral Rogers. (Applause.)

DIR. ROGERS: If I could, let me conclude with just two points. First, I thank you for your time, because there's many other things that you could be doing.

Secondly, if you had a question, I will be glad to stick around for a little bit, if you have a question that you wanted to ask and you just didn't get the chance to. I've got a little time; I'll hang around for a little bit.

OK? Thanks very much everybody. (Applause.)

(END)