NATIONAL PRESS CLUB LUNCHEON WITH NSA CHIEF ADMIRAL MICHAEL S. ROGERS

SUBJECT: CYBER SECURITY CHALLENGES FOR THE UNITED STATES

MODERATOR: THOMAS BURR, PRESIDENT OF THE NATIONAL PRESS CLUB

LOCATION: THE BALLROOM, WASHINGTON, D.C.

TIME: 12:30 P.M.

DATE: THURSDAY, JULY 14, 2016

THOMAS BURR: (Sounds gavel.) Welcome to the National Press Club. My name is Thomas Burr; I'm the Washington correspondent for the *Salt Lake Tribune* and the 109th President of the National Press Club. Our guest today is Admiral Michael S. Rogers, the Commander of the US Cyber Command, the Director of the National Security Agency, and the Chief of the Central Security Service.

I would like to welcome our Public Radio and C-SPAN audiences. And I would like to remind you that you can follow the action live on Twitter using the hashtag NPClive. That's NPClive. Now it's time to introduce our head table guests. I'd ask each of you to stand briefly as your name is announced. Please hold your applause until I have finished introducing the entire table.

From your right, Jen Judson, land warfare reporter at *Defense News*, and the co-chair of the Press Club's Young Members Committee; Tony Capaccio, Pentagon correspondent at Bloomberg News; Max Lederer, publisher of *Stars and Stripes*; Elizabeth Bumiller, the Washington bureau chief of *The New York Times*; the Honorable John Warner, former Secretary of the Navy and former United States Senator from the Commonwealth of Virginia; Kasia Klimasinska, Bloomberg News breaking news reporter, and chair of the Press Club Speakers Committee.

Skipping over our speaker for just a moment, Kevin Wensing, a retired U. S. Navy captain and the Press Club Speakers Committee member who organized today's event; thank you, Kevin. Erik Meltzer, senior news production specialist at the

Associated Press; Jerry Zremski, Washington bureau chief of *The Buffalo News* and a past president of the Press Club; John Donnelly, senior defense writer at *Congressional Quarterly* and the chairman of the Press Club's Press Freedom Committee; and Viola Gienger, senior editorial and writer at the United States Institute of Peace. Thank you. (Applause)

Our guest today, Admiral Michael Rogers, is wearing many hats. As the head of U. S. Cyber Command, he is tasked with defending the Defense Department's networks and protecting critical U. S. infrastructure. As the Director of the National Security Agency, he gathers foreign intelligence to monitor what nations, states, groups and individuals are doing in the cyber arena and that could pose a threat to the United States.

He accepted those responsibilities in April 2014, during the times when the public was still outraged about the scope of the NSA's phone and internet surveillance exposed by massive leaks from a former NSA contractor, Edward Snowden. While he was in office, hackers successfully intercepted networks of Sony Pictures and U. S. government personnel agency. Attacks on Sony initially caused the company to cancel the release of a comedy movie and crippled thousands of computers. The Obama Administration responded by tightening sanctions on North Korea blamed for the attacked.

Admiral Rogers warned that the country should brace itself for more intrusion of that kind. He points to Russia and China as the biggest hacking threats saying that hackers from North Korea and Iran also represent challenges. Still, during his Senate confirmation hearing, Admiral Rogers admitted that one of his most demanding tasks is to get Americans comfortable with NSA's actions, such as collecting phone record data including the numbers used. NSA espionage practices have been criticized by civil liberties groups, technology companies and U. S. allies. Rogers faces the challenge of having to explain his work through the general audience and for foreign partners while keeping most of the details and findings secret from our enemies.

He has a unique opportunity to talk both about the NSA and the U. S. Cyber Command at the National Press Club luncheon today. Please help me give a warm welcome to Admiral Rogers, National Press Club. (Applause)

ADMIRAL ROGERS: Boy, I got to tell you what I thought I heard there was please let me help me give it to Admiral Rogers. (Laughter) I just thought, well, this is going to be an interesting conversation.

So first and foremost, thank you all very much for being here and to the National Press Club, thank you for the opportunity. I'll share a few thoughts with you and then I'm interested in a dialogue, take your questions on any topic. To those who joined us electronically, thank you very much as well for taking time for a conversation that I hope generates value for you and also helps me to learn because I'm always interested in how do you generate more insights, how do you generate outcomes. Ultimately, my view is that's what ultimately job is.

If I could, I'm going to add two things to what you heard in the introduction about the responsibilities of Cyber Command and NSA. But oh, before I forget, before I say that, my compliments to the Club. I have never been at a function and had cookies with the label of the organization. I got to tell you, that's amazing to me. My day is made. When I go back to Fort Meade after this and tell them, "Look at the cookies this place had." (Laughter)

So what I want to say is in addition to what you heard on the U. S. Cyber Command side, operate and defend the Department of Defense's networks, defend if directed by the President or the Secretary of Defense critical elements of U. S. infrastructure against significant events of cyber sequence, of significant cyber consequence. The third mission that you didn't hear outlined was also generate the capacity and employ it across the range of the defense and the offense to support broader military operations around the world. And we have publicly acknowledged that we are doing offensive actions right now against ISIL in cyber and the fight in Syria and Iraq. And I'll be very up front with you and tell you I'm just not going to go into any more details. I like to be very honest with people. I'm often asked in forums like this, "Well, can't you give us more details?" And I'm going, "No, I'm just-- we're in a fight against an adaptive learning adversary and I have no desire to give that adversary greater insight." So apologize to you in advance. I'm just not going to go down that road with you.

The other item I would highlight with the National Security Agency, we highlighted in the introduction our foreign intelligence mission, the use of signals intelligence in the foreign environment to gain insights into what nation states, groups and actors are doing that are of significant concern to our nation, friends and allies. And that is much broader than just cyber.

The second mission for NSA, and one that is growing in increasing importance, is information assurance. We had always been responsible for developing the cryptographic standards and the security standards for classified systems within the Department of Defense, but over the course of the last decade or so, increasingly NSA in its information assurance mission, is being called upon to provide defensive insight as to how you stop penetrations. And once a network is penetrated, how do you drive the opponent out and then how do you configure the structure so they can't get back in?

That has been a huge growth for NSA over the last few years. In some ways, I often somewhat internally joke with the team, we find ourselves becoming the FEMA of the cyber world for others, because increasingly we're just being called upon, "Hey, you have technical capability, you have capacity, you have expertise. How can you apply this as we're helping to defend both systems in the government but as I previously talked about, we were called upon to assist in the Sony response, for example. If you had told me as a military leader, as the Director of the NSA, that I was going to be involved in supporting a motion picture company and responding to how it was going to deal with a significant penetration, I'll be honest and tell you, "Boy, I don't think that's going to come up during my time." As the Director, I failed to anticipate that one miserably. OPM, we

were part of a broader team that provided expertise within the government and response to the aftermath of that.

What I thought I'd do, then, is just highlight kind of where I think we are in both of those mission sets, if you will, and then I'll be glad to take any questions on any topics from you. So United States Cyber Command, the senior of the two jobs. It's actually where the fourth star comes from, not the NSA job, the Commander of Cyber Command job, is considered within the military structure the senior of the two responsibilities.

As the Commander of U. S. Cyber Command, I find myself as a very traditional operational commander within the department, much like CENTCOM, PACOM. I'm at a slightly different level, but we all realize what the impact of cyber is, and will be, across our department. And so we are working hard as an organization, as many other organizations are, as many other elements within the government are, to insure that as a department, we have the capacity and capability to continue to operate within the face of adversaries who are determined to use vulnerabilities inherent within the cyber framework, networks, weapons platforms, and to exploit those vulnerabilities, to attempt to negate our ability to execute our mission as a broader department.

That is priority number one for U. S. Cyber Command, is to insure that our networks and our data and our key platforms and capabilities are fully capable of operating in the face of an adversary or adversaries who want to take away those capabilities. So that's mission number one for us.

To do that, as well as the other two missions you heard me outline, we are generating within the Department of Defense a dedicated what we call the cyber mission force. It's a force of dedicated, focused, trained and organized cyber professionals designed to provide the department a high end of capacity and capability. There are 6,200 people within that force. We're about halfway through the build. I have to add, those 6,200 individuals are divided into 133 teams. The teams are specialized. Some are defensive, some are offensive. And that capability, I have to deliver at what we call a fully operational capability by 30 September, 2018. So just over two years. We're going to reach the goal, is to reach IOC, or initial operating capability, for that entire force by 30 September of 2016, so that's only three months away so I'm focused right now on making sure that the initial operating capability that we meet that timeline and the team is fully started and ready to go.

It’s an example in some ways of how cyber is different than some areas because demand at the moment exceeds capacity. This is the one mission set that I've been involved in as a military professional for 35 years. We're not even waiting until a team is fully constructed. As soon as we get a cadre, we are putting teams on targets. Think about what that means. You will not find in DOD, we don't take a fighter squadron and say, “Well, you've got 5 of your 24 aircraft, we're sending you to Afghanistan.” We don't say, “Hey, we got a brand new carrier coming out of the yards. You've done your builders acceptance trials, but you haven't done your workups, but we're forward deploying you to the Persian Gulf.”

The reality is, because of the dynamics of cyber, we need to apply capacity as son as we're generating it. And so we find ourselves in a situation, a little unusual in the military arena, as soon as we get a basic framework, we're deploying the teams and putting them against challenges. It's an interesting leadership challenge, about how you do that at the same time you're still trying to build that team. But in the end, I think it's the only option we have. We just can't wait, for example, until 30 September 2018 and say, "Well, now that everything is 100 percent fully trained, perfectly aligned, now hold us accountable for exercising the mission." It isn't going to work that way. There's just too many demands, there's too many requirements. But it is very different for us in the culture of the department.

I'm comfortable that we're going to meet those milestones. It's a lot of work. My compliments to the services. They're very committed to this, the department is very committed to this. You know, cyber is just one significant challenge within a breadth of challenges that the department is trying to deal with. I'm very grateful and very fortunate that the department leadership has acknowledged the challenges associated with cyber and in a declining resource environment is willing to invest in those challenges. Even as I acknowledge, it never goes as fast as you want, and it's never-- you're never where you want to be.

I'd never had a job before where I literally every day am thinking, how do I make sure we're staying ahead of the adversary? I just always feel like we are in a race to make sure we are generating capacity and capability and that we are doing it faster than those who would attempt to do harm to us.

And when you do this, as you watch what opponents are doing, as I watch behaviors out on the net, you just-- it's almost visceral. I just feel like every day we're in a race to generate capacity and capability before the adversary. That's invigorating, don't get me wrong, it's very invigorating, but it isn't without its challenges. Because every day in the cyber arena, you find yourself in contact against a wide range of adversaries. Nation states who are attempting to penetrate the department's networks, who want to generate insights as to how our networks are constructed, adversaries who are attempting to penetrate our networks because they're interested in taking information, data, insight and knowledge out of our networks and asking themselves how can they apply that to attempt to gain advantage over us, or attempt to negate the advantages we have because some of our capabilities for our war fighting mission within the department. So I would be the first to admit, you always get that sense of the challenge.

On the NSA side, I try to remind people, much like the department side, one of our challenges is requirements continue to grow; the expectations of the knowledge and insight that the intelligence community is going to develop for our nation and our friends of allies, it continues to get larger, excuse me, not smaller. And yet at the same time, budget is declining and you're trying to work, so how do you prioritize? How can you do things smarter, more efficiently? That's one of the reasons some of you may have heard about NSA 21, which is what we have created out at NSA with the idea being how do we

make sure that we are every bit as good five, ten years from now as we have been for the last five, ten years? The nation is counting on us to be able to sustain these capabilities to generate these insights, to do it in a lawful way, to do it in a way that generates confidence within the citizens that we defend. But the nation is counting on us to generate the insights.

And so we've got to ask ourselves, how do you do that in a world in which resources are declining, in a world in which the technical challenges that you're dealing with are just getting more and more complex?

The positive side, I would tell the nation, is you've got a great bunch of motivated men and women at the National Security Agency and in United States Cyber Command. They believe in their missions, they believe in doing the right thing the right way, and they are committed to doing it within a legal framework. And that is the commitment that I have made since day one in my role as the Director of NSA and the Commander of Cyber Command. We will do the right thing, the right way, in accordance with the laws of the nation. And when we get it wrong, we still stand up and acknowledge that we got it wrong.

Because I remind people, look, even with the great technology we have, at its heart Cyber Command and NSA are two enterprises powered by motivated men and women. And the most motivated men and women sometimes make mistakes. And we're going to be an organization, organizations, that stand up, own those mistakes and holds itself accountable because that's what the nation is counting on for us. And I think that I have no issue with that at all. That's fair, that's the way it ought to work.

Another challenge for us at NSA, as I said, so we've got these two missions; foreign intelligence and information assurance requirements growing in both segments, resources not keeping up. Again, that's another reason behind NSA 21. Hey, how can we do things smarter, more efficiently, more effectively, realizing this environment, I don't think it's going to change. So we got to ask ourselves, what are we going to do? If that's the case, what are we going to do?

You can't just keep doing the same thing the same way over and over again and always expect to get the same results. The world around us is changing and we have to change with it. Technology is changing, the expectations of our citizens, the fact that we're competing for the same workforce that the private sector is. How do you recruit, retain, insure that you create a workforce that's adaptive, that can change with technology, that changes with mission?

It's one of the reasons why I spend a fair amount of time out on the west coast, in the Valley and other places where I try to talk to my industry counterparts. "So tell me how you recruit your workforce. Tell me how you retain them. Tell me how you train them? What's effective for you?" We have got to create-- one of the biggest things that I'm interested in is the model within the military and NSA traditionally has been once we get you in the door, you tend to stay with us a long time. I'm not sure that that's a model

that's optimized for the future. Because if you look at the rate of change that's out there, I'm interested in a model where how can you potentially, for example, start with us but then go work in the private sector for a while and then come back? How can you make us smarter about the world out there and how can we make the world out there smarter about us?

Because one of the challenges I found in coming up on 2 ½ years I've been in these jobs, I'm watching two cultures at times talk past each other. I'm watching the culture that I'm a part of think they understand the outside world. Oh, it's about money. I go, "Stop. If you're out in the Valley, your view is you are harnessing the power of technology to change the world for the better. What's wrong with that as an objective? That's every bit as a value to our nation and the world around it as those in government who say, 'My mission is to help defend and provide for the security of our citizens and our friends and allies around the world.' Hey, we're not about money, we're about service to something bigger than ourselves."

And I watch these two cultures at times just talk past each other. Each thinking they understand the other. And my experience is, boy, we don't. And so that's one of the reasons why I'm interested, could we come up with a more permeable membrane where we can move people back and forth, so we can help to have a broader dialogue that's based on facts. Take the emotion out of this and let's deal with facts.

And then we'll make a decision collectively as a nation. What are we comfortable with, what are we not comfortable with? Because the imperative for us, I've always believed as a nation, is both to insure the security of our citizens, but to never, ever forget that we've got to do it in a framework that empowers the fundamental rights of those citizens. The governing document for our nation doesn't start talking about the power of the state, it starts talking about the rights of every one of us as citizens.

But that same document also talks about the role of government in insuring the safety, security and prosperity of its citizens. And so we got to figure out, how are we going to meet both of those incredibly foundational and important premises and tenets? Because it can't be one or the other. We've got to do both.

And I spent a lot of time as the Director of NSA, in particular, asking myself, "How do we do both? How do we do the mission in a way that engenders confidence and trust in a world in which confidence and trust is not easy to come by?" Don't worry about the whole issue that we're associated with NSA. I think we got to deal with the reality, is as a nation we got to be honest with ourselves. We have increasingly low confidence in many of the structures that we have created over time to govern ourselves, and to help insure our capabilities.

And so what's happening, you know, in my little slice of the world is happening in a much broader dialogue. And the sad part is, it isn't anywhere near as much as a dialogue as it needs to be. Angry people yelling and screaming at each other generally doesn't generate better outcomes of solutions. You can argue about this or a whole lot of other

issues. We've got to figure out how are we going to have a dialogue? And how are we going to figure out how we're going to keep moving ahead, and how are we going to do it in a way that engenders confidence at the same time that it's insuring our security and our basic rights?

And so collectively as nation, we'll work our way through those challenges. As I said, the foundational point for me is, as I always remind NSA, the touchstones for us, we always obey the rule of law. If we make a mistake, we acknowledge that mistake and we own it. We don't take shortcuts. That'll get you in trouble. You don't take shortcuts. I said, you keep those three things in mind, we're going to be exactly where we need to be.

On the U. S. Cyber Command side, one of my-- I've done this for a while now in multiple jobs, what the U. S. Cyber Command team hears me talk about is if you want success in cyber, if you want to generate cyber security capability, it's about speed, agility, precision. We got to be fast because in the world of cyber, the time factor is so compressed compared to many other things. I can remember early in my career worried about, as a cold war worrier, I'm that old, right in the heart of the cold war when I first started and we would talk about depending on the scenario, if a weapon was launched from a land mass or off a submarine, we'd have anywhere, if my memory's right, 12 to 25 minutes to try to decide how are we going to respond. Twelve to 25 minutes in the world of cyber? Boy, it's already happened now anywhere in the world that was the intended target. So speed gets to be really important.

Agility, we're working against adaptive adversaries who are constantly changing their targets and they're changing the way they go after the target. Responding the same way every time is not going to work over time. Adversaries get smart and they learn. That's what we do. We study opponents, we study their behavior, we study the way they work and we try to anticipate based on that knowledge what they're going to do. And I don't pretend for one minute we have perfect knowledge or insight.

So part of this is getting to a mindset that says how can we be agile? How can we change and adapt? That's not unique to cyber. You know, one of the maxims you learn in the military is no plan survives contact. You can come up with all the greatest plans in the world you want, but once you're in that fur ball, doesn't matter if you're in an air to air engagement, if you're on the ground in a tactical environment. Boy, once you enter that fight, you know, the plan is a point of deviation and you try to use your training and your knowledge to adapt to the environment that you find yourself in right now. It's no different for us.

And then precision. It isn't enough to be 99.9 percent accurate, you got to be a hundred percent accurate. You get one digit wrong in an 11 digit IP address and you are in a totally different place. You've got to get precision in what you do. And it's interesting to watch an organization try to bring those three imperatives together; speed, agility, precision. "So let me understand it, sir. You want me to be fast. You want to be able to change, but you're telling me to be precise." And I'm going, "You have grasped the concepts." (Laughter) That's what we got to do. And it isn't easy, I'm the first to

admit, but I think it really is the key to success for us in the future as we try to look at so how are we going to defend those DOD networks? How are we going to generate capability that provides operational commanders and policymakers a broader range of options.

And with that, rather than me talk at you, I look forward to the dialogue. Thank you very much again for being here today. If there's one thing you learn in a cyber mission, and this is true for government, it's true within our specific department, it's true more broadly, it's true in the private sector, this is the ultimate team activity. I have never been involved in a mission set in 35 years, I hit 35 years of commission service next month, I've never been involved in a set of activities where your success is so predicated on the behaviors and choices of other organizations. You have got to create strong partnerships and you have got to exercise those partnerships before you get into contact with an opponent.

If there's one thing life in the military teaches you, discovery learning when you're moving into contact with an opponent is an incredibly bad way to learn. It generates higher rates of casualties and loss, it's more resource intensive, and it really lowers probability of successful mission outcomes. Cyber's no different in that regard. We got to train, we got to exercise, we've got to try to simulate to the maximum extent we can. What do we think in our encounter before we actually encounter it. So they probability of success, we start at a much higher point.

And that's as much about culture. And let me conclude with that, I apologize. One other thought comes in my mind. There's definitely a strong technical aspect to this mission set, I'm the first to acknowledge that. But I always tell both hats, Cyber Command and NSA, don't ever forget that at the end, we're dealing with a choice that some human made on a keyboard somewhere else in the world. There was a man or woman at the other end of this.

Secondly, remember this is the one mission set that I can think of where every single user out there is both a potential point of advantage and a potential point of vulnerability. We don't give weapons to everyone in the DOD. We give a keyboard to everyone in the DOD. Literally, everybody's got access to an unclassified system, higher level classified systems, and suddenly now you find yourself in a scenario where if you're not careful, you've got to have the greatest technical solution in the world about how you defend the system, and yet bad user behavior, bad choices, start to make your defensive abilities really challenging, really difficult.

And so a big part of this is hey, even as we focus on the technology piece and making sure that we have sound networks and that our platforms reflect redundancy, resiliency and defensibility as core design characteristics, even as we do that, I also remind people never, ever forget the human dynamic in this. It's about making sure that our individual users understand that they will be making choices that have broader impact; at the same time, it's using strong leadership, good organizational skills, how do you create that high end cyber mission force that's optimized to deal with these

challenges? That's one of those missions at Cyber Command. You, as I said, if you could see the men and women that are doing that work, I just had this-- we do a major exercise series every year. We just finished it down in Tidewater last month, at the end of June.

And as I was bringing some people through-- in fact, this was a couple of people from the Hill, as a matter of fact, they were asking-- and I had never-- this was not pre-staged. I had never met this individual before. We're getting a brief from the team-- it happens to be a Navy guy in this case-- a young petty officer. And I turned to the senator, who I was escorting and said, "Senator, why don't you ask him about the journey that brought him to this job, and ask why he is doing this." And I did that honestly, not knowing the answer. But I thought, "Wow, this guy seems really motivated. He seems to really like what he's doing."

Sure enough, I thought he was pretty typical. He joined the Navy not to do cyber initially. He was an operations specialist. That's the skill set that we have in the Navy, that in that dark room on a ship where all our radar is and the tactical picture comes together, and all our weapons systems, it's where we fight from, we call it the combat information center on most ships, and he used to operate that equipment. And he said, "Hey look, I really wanted a different challenge." And so he walked the senator through, "Here's the training I got, here's the two tours of duty I've had now as a cyber professional." And the senator said, "Well, why are you still with the DOD? Why didn't you consider leaving. You could have made a whole lot more money on the outside."

He didn't miss a beat. He turns to him and says, "Because I can do things here that I can't do outside because I can make a difference and serve something bigger than myself and because they let me do some really neat stuff." And then he says, "Let me show you," and the next thing you know, he's right next to a touch screen. Bam, bam, bam. "Let me show you this, sir." And I'm watching, wow, this guy-- thank God we got men and women like this. He loves his job, he considers himself a warrior of the 21st century. He's dedicated to being the best he can be, and he's willing to work hard to generate more knowledge and insight so he can apply it in the defense of our nation. Even as he acknowledges, "Sure, I could do some other things on the outside." We are just so lucky to have men and women like that.

And with that, I look forward to your questions. (Applause)

MR. BURR: Well, thank you, Admiral. You started off by saying, I believe-- I believe you started off by saying you don't want to take any questions about ISIL, but this being the National Press Club, I'm going to make that my first question.

ADMIRAL ROGERS: You're going to make that your question. It's that communication effect that works so well for us.

MR. BURR: Exactly. We're journalists, after all. But without getting into methods that you probably can't talk about, how successful has the campaign been against ISIL?

ADMIRAL ROGERS: I'm just not going to get into specifics. You can keep asking, but I'm just not going to get into specifics.

MR. BURR: Second question. No, I'm kidding.

ADMIRAL ROGERS: Let me rephrase, your honor. If I-- I have this friend who-- (Laughter)

MR. BURR: Is asking for a friend as well. All right, I'll change gears a little bit. Admiral, this week you testified about the challenges of encryption for the Senate Armed Services Committee in a closed session. Without getting into anything classified, can you talk about some of these challenges that the NSA is working with them on?

ADMIRAL ROGERS: So, I was testifying before the Senate Armed Services Committee predominantly in my role as U. S. Cyber Command. But one of the things the committee wanted to talk about was, so what are your views of encryption? What are some of the challenges that you're working your way through? And I always start out by telling people, "Look, I don't know what the answer is. I don't come to this with, 'Oh, I know what the solution is.'"

I'm struck by several things. We're a nation of can do. You go out in Silicon Valley and you see motivated men and women who are harnessing the power of technology to create a different and a better world, who have created a center of innovation that is the envy, I mean literally, the envy of much of the rest of the world. Who have created capacities and capabilities that have empowered a level of knowledge sharing that this planet has never seen before. I mean, think about that. Our ability to access information in the format, in the medium of our choice literally any time, anywhere, none of our previous generations had that advantage. That has done some amazing things, generated unparalleled economic growth, learning, insight. Those are great things for us.

That same team, I say, you're all about the power of possibility. So can we start talking about what's the power of possibility here? Because right now, we're spending a lot of time talking about what we can't do. And I'm just struck by look, we're a nation of possibilities. Let's talk about what we can do, and then let's have a dialogue about what we should do, because those are not the same thing. Just because you can do something doesn't mean you should do something.

And I'd be the first to admit, hey, both at Cyber Command and as the Director of NSA, we're just one small part of a much broader dialogue. But oftentimes, I get asked, so what is the impact of encryption on your missions? And this is where really on the NSA side, and I remind people, we're watching a world where many actors of concern to this nation and those of our friends and allies, are harnessing that same technology that you and I are relying on to insure that our personal information is not compromised by

anyone. They're using that same capability, that same technology, to generate money, to coordinate attacks and to generate violence against us and other nations around the world.

And we got to ask ourselves, how are we going to deal with this? Encryption is a positive thing. It's fundamental to the future. I don't see a solution where we go, "Well, we don't need encryption, it's bad." I reject that idea. I don't know what the answer is, but again it goes back to my comment about could we really have a dialogue about this and start to talk about what's in the realm of the possible. And then let's facilitate a broader dialogue about what we should do. And this is something collectively as a nation, I would argue, you don't want the intelligence world telling you what the answer is here.

Likewise, I don't want a company necessarily telling me what the answer is here. I don't want a government agency necessarily telling me that. What I want is, for Mike Rogers, could we engender a broader dialogue as a society about what are we comfortable with here? And what makes sense for us. Realizing there isn't a single answer here. But this problem's not going to go away and it isn't just about insights about what's going on for foreign adversaries. You are watching criminals exploit our youth with guns, drugs, violence, using these same capabilities. And we got to figure out how we're going to deal with it, and how we're going to deal with it in a way that insures that our rights are adequately protected.

You know, the answer is not, "Well, just let the government do whatever it wants." And I don't know you're going to hear that from the government. I think we realize that's not what we're about. That's not what we should do.

MR. BURR: That leads into the next question, actually. Have Americans given up some privacy in order to bolster national security? Should they have to give up that privacy? Can privacy and security coexist?

ADMIRAL ROGERS: Well, I would argue step back, think more broadly than national security. I would tell you in the digital world we live in, the idea of anonymity is increasingly difficult to execute. Forget about the implications to national security, just more broadly. I think every one of us in our personal lives deals with this challenge all the time. You know, what does anonymity mean? What does privacy mean in the digital age of the 21st century? I'm not sure that it's exactly the same thing as the analog world of the 20th century.

And we're trying to figure it-- and I don't know what the answer is, but I'm just struck by wow, the world around us has really changed and there's a lot of implications for this that I'm not sure we all collectively fully understand. But we've got to put our mind to this and think about that, because questions like this are incredibly foundational for us as a nation.

MR. BURR: Do you think a cyber Pearl Harbor is inevitable? And what form might that come in, an attack on the power grid, the financial sector?

ADMIRAL ROGERS: So I generally don't use the phrase Pearl Harbor because the analogy in my mind was Pearl Harbor was a bit of a bolt out of the blue. I don't think any of us right now is surprised by the amount of cyber activity that we're seeing. You know, they say that awareness and recognition are the first steps to solving a problem. Well, the positive side is we generally have broad recognition and acknowledgement that we have an issue here now within the cyber arena. That wasn't the case, I would argue, five, ten years ago. We were still in the, oh come on, how big could this be? Really, that's not realistic. You look at what happened in the Ukraine in December with the power grid, you look at Sony, there's plenty of instances out there now. Hey, this is something real. And I don't see it stopping.

As you said in your opening remarks, I said that in my testimony when I appeared before the Senate for my confirmation hearing. It's the when, not the if, and we got to figure out how are we going to deal with this. And go back to my comments in my introduction. I don't want to start dealing with this for the first time when we're in the middle of a major significant cyber event. That's a bad time to start learning. I'd much rather start now.

And we're doing that, that exercise sequence that I mention that we do every year, there's two parts to it. The second part is we use as a tool to certify and train within the DOD, the first part we simulate how the DOD would partner with the Department of Homeland Security, the private sector, FBI and other elements to protect critical infrastructure in the United States.

We partner with private industry when we do that, we bring within the DOD both active guard and reserve. We bring DHS, the FBI together, other elements within the government. We actually create realistic networks that simulate real configurations out in the private sector and we ask ourselves, so how do we defend it? How do we respond? What are the lanes in the road, who has what responsibility? What's the best approach to solving the problem?

So we're working our way through it, but the size of the infrastructure that we have as a nation? I mean, we're the most advanced, arguably the most digitally driven nation in the world, certainly on the scale that we are. That's a whole lot of turf to make sure that we're trying to insure is sound and is defensible. That's a lot of work. And it’s work that's going to take all of us.

As I often remind my DOD teammates, if you think Rogers and his 6,200 high end warriors are the answer to this total problem set, we don't get it. It's about how do we apply those 6,200 as part of a broader team that's spread across our services and our forces. How do we tie that all together in an integrated, cohesive way that's focused on a common strategy and it’s got a common vision to how we're going to defend our networks, our data and our key platforms and capabilities? And I would argue it’s the same thing in the private sector.

MR. BURR: Well, talk to me, what does cyber war really mean in some ways? And when I ask the question, I'm trying to get to the point of when would more of the traditional response, bombing of a nation or something like that, respond to a cyber attack against the United States?

ADMIRAL ROGERS: So the first thing I remind people is look, the response to an event is driven by many factors. How would you characterize the event, what was the intent of the adversary, what was the impact of the activity? You wouldn't respond the same way to a very minor event that you would to something major and traumatic; the loss of power for a segment of the eastern seaboard would probably engender a very different response than one single localized entity that lost service for three hours but was quickly able to come back online.

So, I always try to remind people, my experience leads me to believe you don't have a one size fits all. That we've got to think about in a very nuanced way about how we do this.

The second point I would make is much is true that I found in the kinetic world, in the more traditional domains, just because somebody comes at you one way doesn't mean you've got to respond the exact same way right back at them. If you look at, for example, the way we as a nation opted to respond to the Sony penetration, we used the economic lever in the form of sanctions as the initial response, by design. One of the things, and I'm just part of the dialogue, is we need to think about what are the full range of capabilities and advantages that we enjoy as a nation and how do we apply those in a very focused, specific way in the response idea?

Not to, well, you just default to whatever they did to you, you got to go do to them in the exact same way. I'm not a big fan of that approach, personally.

MR. BURR: Thank you, sir. I talked about Edward Snowden in the introduction, but have we been able to fully assess the damage done to the United States intelligence efforts by Snowden and Bradley Manning?

ADMIRAL ROGERS: Let me phrase it this way. Do we continue to see impacts from all this? Yes. Will that impact continue to unfold over time? I believe it will.

MR. BURR: How big was the impact?

ADMIRAL ROGERS: I have publicly characterized it before previously as significant. I am watching targets of concern to this nation, our friends and allies, change their behaviors, change what they are doing expressly because of the insights that they have gained as a result of the disclosures.

And again, I try to remind people, take the emotion out of it. We all just need to deal with facts and then we'll collectively decide, so what are the implications to that?

MR. BURR: One of the reasons Snowden gave for his actions, there was no internal mechanisms required by law or executive order such as whistleblower protections, that allowed for a contractor to bring concerns to superiors or a third party. Has that been reconciled?

ADMIRAL ROGERS: I disagree with the premise.

MR. BURR: There are protections right now?

ADMIRAL ROGERS: I disagree with the premise. What's the next question? You'll find I'm a very direct individual.

MR. BURR: That's good. I had a lot of questions about Snowden so we can get to some of these. It's been three years since the Snowden leak. Americans now know as much as Snowden knew before he released his documents and the resulting outcry lead Congress to enact reforms. But given the many Americans and majority of the representatives in Congress agree the NSA practices needed to be reformed, should Edward Snowden still be prosecuted for espionage? And if so, what would that accomplish?

ADMIRAL ROGERS: That's a topic way beyond my role. I hope you realize this is not a line of conversation that's going to be particularly productive for you or for me, or all of you. But I'm willing to continue this way if you'd like to ask them.

MR. BURR: We like to ask them anyway. In retrospect, what should have the NSA done differently in the aftermath from 9/11 to the Snowden leaks?

ADMIRAL ROGERS: Well, clearly, we always want to generate more insight because that insight helps to protect lives, helps to defend our nation, helps to protect our allies. At the same time, I think one of the takeaways, and I think about this. So what does it mean to be a leader in the intelligence world in the 21st century? And how is that different from when I started my journey in this profession decades ago now?

Boy, I can remember, you know, the culture that spawned me was focus on the mission. You don't talk about what we do, you don't talk about how we do it, you don't even acknowledge what we do, you just do the mission. Now, you do it lawfully and you do it the right way, but you don't ever talk about it. You don't want to compromise what we do because you don't want to give an adversary advantage and insight that they can turn against you.

And yet I find myself now as a leader acknowledging, hey look, we have got to engender confidence in the nation we defend. And one of the ways to engender that confidence is we've got to be willing to have a more open dialogue. So for me, what I try to do is I'm willing to talk in broad terms about what we do. But the how we do it, that's kind of for me, at least, where I kind of draw the line and just say look, if we're starting to

get into the how, now I'm going to compromise capabilities that are going to provide an adversary insight and that's a bad thing for us as a nation.

And so for me, that's how I try to balance those things. And so I think to myself, you've seen it in the way NSA has declassified documents. You've seen it in the way we're trying to interact more with the public. You've seen it in the way we're trying to create partnerships in the academic world, as we're trying to build a workforce for the future about hey, so how do you have a dialogue that tries to strike that balance? About hey, broadly, here's what we do, and that you as a nation should feel comfortable that there's a level of oversight and control in what we do. And that we're just not acting in a capricious or spurious manner arbitrarily just doing whatever we do.

It doesn't work that way, guys. NSA is one executive order and four laws, four laws, that drive everything we do for our foreign intelligence mission.

MR. BURR: Don't you find that is more of a challenge, though? Because Americans hearing generalities and vagueness in "trust us, guys," doesn't really get them--

ADMIRAL ROGERS: You didn't hear me say trust us. I think one of the challenges is, again, step back to my comment about the broader context. Yeah, I'm a fan of history. If you go back to the 1970s when many of the mechanisms that are in place today were actually created in the aftermath of the Church and the Pike Commissions, the committee in the late 1970s in the Senate, the committee, said, "You know, we need to create a framework that strikes that balance where we can't publicly broadly talk about the specifics of what we do, but we want there to be a level of oversight of what we do and how we do it. And we need to do it in a way that our citizens should have a measure of confidence."

The mechanism that was created then was the idea of congressional oversight. Thus were born the CICI [?] and the HIPC. As the duly elected representatives of each and every one of us who is a U. S. citizen in this room, we gave complete openness to those individuals. And so if you look at the aftermath of the disclosures, what did you get initially? For both those committees on both the chair and the ranking member, in the immediate aftermath you got, "We have full knowledge and awareness of what NSA is doing. We're fully briefed into what NSA is doing. It is fully compliant with the law and we believe it generates value for the nation."

And yet collectively, what was our response? Hey, I'm not so sure I have that same level of trust. Why? I remind people, look, all this is happening in a broader context. Our belief in many of those governmental structures that we put in place is just not the same now as it was 40 years ago. Likewise, we created a court. Hey, how do we create a legal framework where for many of its actions, NSA and other elements within the intelligence world, have to go to an independent entity in the form of a judge and make a case on a legal basis for why they should be allowed to do what they're doing?

Let's use a judge, let's create a court. Thus was born the FISA court. Forty years later, though, you have people asking, okay, got it. Court, but look at the way you structured it. It hears the government's argument. It doesn't have an adversarial viewpoint, for example. Forty years ago, we thought that was a perfect construct. Now we find ourselves in a different environment with a different view of the world around us and we say to ourselves, "Well, maybe I'm not so sure about that."

So, I only highlight that to people to say step back, remember the context when all this is happening. The very mechanisms that we put in place to engender that trust, now in many ways have very different view from the citizens that they're supposed to generate that for. They just look at the mechanisms differently and say, "Well, I'm not so sure I get that same level."

So one of the things that I think we're going to be working our way through is what is the appropriate mechanism to provide that oversight and that level of trust? And again, that's something that broadly as citizens you need to be comfortable with. I shouldn't be determining that.

MR. BURR: Thank you, Admiral. We're going to be like best friends after this, right? All these tough questions--

ADMIRAL ROGERS: Could you ask me a question about Cyber Command at one point in this dialogue?

MR. BURR: I'll get to it. Sticking with one as the president's prerogative, I'm going to ask a little bit of a local question. Let's talk about the NSA's Utah data center, which has become in many ways a symbol of the agency's larger reach to our digital world. This is a very large facility. For some of you who don't know, in the Salt Lake City suburb, but is it fully operational? Have you experienced any problems in getting up and online? And with the growth of data needs, how quickly do we have to expand it or look for other locations?

ADMIRAL ROGERS: So, the Utah data center is one of several data centers that we have constructed that are designed to enable us, so how do you deal with this digital age where increasingly data sizes are growing? And so we consciously step back, and this was the decision about ten years ago, we need to create a framework that's going to enable us to safely store, secure and access that data. And so the facility in Utah is one of those where we've tried to talk all that we've learned about how do you secure data, how do you control it, how do you put it in an environment where it stays safe, where it's in the right climate.

I mean, you put a lot of servers together, simple things you don't probably care about, but heat generated. If you design data centers for the digital age of today versus the past, I never thought I'd get into studies of how you provide cooling and electricity and yet, we've done that. We've tried to do that. In fact, one of the reasons for the location in Utah, quite frankly, was some of the power aspects. And the facility's in place. I've been

out there once in my time as the director. We're in the midst of fully outfitting it right now.

MR. BURR: How quickly will you need to expand or have other data centers?

ADMIRAL ROGERS: Boy, I don't know. The only thing I can think of is full motion video and ISR airborne intelligence surveillance and requirements, you look at what we've done in the course of the war, the wars in the last decade, 15 years, we are operating with a level of airborne ISR today that 15 years ago we never, ever thought, envisioned. And at the time we said to ourselves, "Boy, you're never going to need anywhere near this." And yet now we say to ourselves, "Wow, the future has changed in ways we didn't anticipate."

So, I'm comfortable with capacity for right now. It's something we continue to watch, and if we feel we need more capacity, we'll go to the Congress, to the department and we'll request it.

MR. BURR: Let's talk about cyber for a second. Do you see cyber as a first strike weapon that could incapacitate the United States, or that we could use to incapacitate enemies? And should we integrate cyber into our military planning to defeat or deter potential rivals?

ADMIRAL ROGERS: So first strike is a policy question, that's not my role.

MR. BURR: But could it be? Could it be used as that?

ADMIRAL ROGERS: You got to come up with a better question than that. Could it be? (Laughter) So that's a broader policy piece. What was the second part of it again, because there was- I apologize. That, I thought, was a part-- hey, that's really in my wheelhouse. I can answer that part.

MR. BURR: Should we integrate this into military policy?

ADMIRAL ROGERS: Yes, we should, I believe. You know, our view within the department is cyber is a tool that we should make available to policymakers and operational commanders. It is a tool much like every other capability in our department. It should be used in a coherent, legal framework in which proportionality and the directness of response is very specifically assessed and measured, and is a primary criteria in the decision to apply it. And that any application of this capability in an offensive framework should be done fully within the law of armed conflict.

They same criteria that we use when we ask ourselves, should we drop a piece of kinetic ordinance in a spot on the Earth, we need to be asking ourselves those same kinds of questions. You know, we need to make sure that we use this in a proportional and appropriate manner. No different than any other piece of-- I'm not arguing it's exactly the same, but the thought process, very similar.

MR. BURR: Do you believe Congress has been responsive in effectively crafting a national cyber policy? And what else could Congress, the Obama Administration do that would help your direction in what you need at the Cyber Command?

ADMIRAL ROGERS: The way to put that, that would help you at the very end, very good. So, first of all, policy in broad terms is generally and executive branch responsibility. Congress provides specific insight and direction based on their perspective. As a department, we have outlined a comprehensive DOD cyber strategy. We've done it twice. The current version we signed out in April of 2015. You can see how that strategy has evolved over time. If you read the first strategy that we published in an unclassified way, I think it's the 2010-- I think it's approximately 2010-- very generic. Didn't talk about specifics much. Then if you read the strategy we've just published now, the current strategy in April of 2015, we built on what we did initially and for the first time we start talking about concept of deterrence.

We publicly acknowledge in an unclassified document that the department is generating offensive capability. Since that strategy was released, as I said, we've publicly acknowledged that we are using in area of hostilities against a particular adversary, some of these capabilities.

So you can see how this has played out over time. You'll see it continue to do that, I believe. But I'm the first to acknowledge, and quite frankly, it's one of the reasons why I'm here today, and I try to do things like this, we've got to get ourselves to a point where we can have a broader dialogue about some of these implications in cyber, both defensively and offensively for us as a nation. And what are we going to be comfortable with.

We've got to try to change the current dynamic. Now, we're all victims of the culture that spawned us, so I am a military guy, so that's the culture that I am from. That culture teaches me you want to get ahead of problem sets. You want to shape adversaries' actions, choices and behaviors. You want to drive adversaries to behaviors and choices that facilitate advantage for you, if possible. Not for them.

And yet, many, in some ways, in the cyber arena, as we're trying to work our way through those questions, day to day you feel like, well we're just responding. We're just reacting. That is both a resource intensive approach to doing business, it tends to put you always in a response and anticipatory set of actions, and it's a whole lot harder and it takes a lot longer.

And so I think over time, we've got to change the dynamic where we create concepts of deterrent, norms of behavior where actors in this space understand what is acceptable, what is not acceptable. What will elicit a response. We've done that in many other areas. We will over time, I believe, in cyber. It's just that cyber is newer than some

of these other areas. And so collectively, we all are still trying to work our way through a lot of different things.

MR. BURR: I'm going to ask two final questions just for fun, Admiral. Before I ask those last questions, quick announcements. The National Press Club is the world's leading professional organization for journalists, and we fight for a free press worldwide. For more information about the club, please visit www.press.org. I would also like to remind you about some upcoming programs. On August 1st, Jonathan Jarvis, the Director of the National Park Service will address the club. And on August 14th, the award-winning actor, Michael York, will speak from this podium.

Also, I'd please ask the audience to remain seated until Admiral Rogers has exited. I would like to present our guest with the traditional National Press Club mug. I promise you it's not bugged. (Laughter)

ADMIRAL ROGERS: Thank you. Thanks very much. (Applause)

MR. BURR: All right, so I'll ask you two final questions. First question, do you play Pokemon Go? Second question: as a Chicago native, do you think the Cubs will win the series, and is there anything the NSA could do to kind of get them out of that 100-year drought?

ADMIRAL ROGERS: So I am a-- so, I do not play Pokemon Go. I do not. Although I'm watching net utilization just jack up with this thing. Secondly, I'm from Chicago, lived there my whole life before I left for college and then joined the Navy and got my commission. I'm a north side guy, so I'm Cubs all the way. Boy, I sure hope we're going to win the World Series. Be interesting coming out of the All Star break, so we'll see if we get a little rest at the pitching rotation where it needs to be. Keep driving on. If you're a Chicagoan, this is the first time I can remember in my entire life what it means to be favored to win the division, let alone the pennant and the World Series.

I mean, I can still rattle off-- I can tell you the starting lineup for the 1969 collapse where the Mets overtook us in September. Such is the world that I live in as a Chicagoan and on the north side. Thanks.

MR. BURR: Well, thank you, Admiral, for being here and answering-- and trying to answer some of my questions there today. I'd like to thank the National Press Club staff, the staff of our Journalism Institute. Thank you, and we are adjourned. (Applause) (Sounds gavel.)

END