THE ASPEN INSTITUTE

BEYOND THE BUILD:
LEVERAGING THE CYBER MISSION FORCE

Aspen, Colorado

Thursday July 23, 2015

LIST OF PARTICIPANTS

WALTER ISAACSON
President and CEO
Aspen Institute

DAVID SANGER
Chief Washington Correspondent
The New York Times

MICHAEL ROGERS
Director, National Security Agency
Commander, U.S. Cyber Command

* * * * *

BEYOND THE BUILD: LEVERAGING THE CYBER MISSION FORCE

MR. ISAACSON: Welcome everybody. I'm Walter Isaacson and thank you so much for being part of this wonderful homeland security conference. Thank you Clark for putting it on. Much of what we've talked about in the past day and a half keeps coming down to cyber. Cyber attack, cyber security, you know, cyber threat, cyber defense and there's really nobody better equipped to talk about this than Admiral Mike Mullen. He has the coolest -- I'm sorry, Admiral Michael Rogers.

(Laughter)

MR. ISAACSON: I know they shouldn't have let me do it. We do like Mike Mullen too and actually better than Mike Mullen is Admiral Mike Rogers.

ADM. ROGERS: We couldn't get Mullen, we went with Rogers.

MR. ISAACSON: He has the coolest title ever, the commander of the U.S. Cyber Command, also the director of the National Security Agency. It's very smart to have both those together. And very smart to have them both under you and also our friend who has maybe the 10th coolest title in the world which is chief Washington correspondent for the *New York Times*, our friend David Sanger. Thank you, David. Thank you Admiral Mike Rogers.

(Applause)

MR. SANGER: Well, thank you very much. Thank you all for being here. Welcome to Camp Isaacson where we all live in the tent for the evening, yeah, and thank you to my great friend Clark Ervin who has put on yet another terrific Aspen Security Forum.

ADM. ROGERS: Well done.

MR. SANGER: So I'm very honored today to be up here with Admiral Mike Rogers. I once did one of these public interviews with Mike Mullen. We'll have to see if we can beat that.

(Laughter)

ADM. ROGERS: We got two out of three, admiral and Mike, that's good.

MR. SANGER: It's good. And Admiral Rogers was commissioned in 1981. He then moved on as director of intelligence for the joint chiefs and the U.S. Pacific Command. I think when he and I first met, he was running Fleet Cyber. A lot of people don't -- didn't recognize at the time that the Navy had Fleet Cyber, but they were pretty busy. They were busy being attacked by the Iranians at the time, although I think that perhaps Admiral Rogers can't say yet who that was, but he got through that well enough to be the commander of the U.S. Cyber Command, and also director of the NSA. When the NSA commission suggested splitting the two jobs, President Obama looked at it and said, no. So there we have it.

He is graduate of the National and the Naval War Colleges. We was an MIT Fellow. He was a Harvard National Security Fellow and we've had many conversations on cyber issues in the 15 months since he took over. We've had a few vivid conversations about our coverage, but we seem to have managed to emerge from this able to still talk to each other. So I look forward to the next hour.

So Admiral Rogers, in 2007, if you go back to the National Threat Assessment which is turned out each year by the Director of National Intelligence and you look for the section on cyber, you will discover it was a really short read. The word cyber does not appear in the 2007 National Threat Assessment. If you go to the last two 2014 and 2015 it is listed as the number one threat to the United States ahead of Islamic state, ahead of North Korean nuclear programs, ahead of any other threat you can think of.

And if you think about just the past year, since we had a fair number of cyber conversations at last year's security forum, what have we had? We've had state -- attacks on the State Department and the White House that so shut down the State Department's e-mail systems that during the Iran nuclear negotiations last November we had State Department officials handing us their Gmail accounts so that we could all communicate. We had the Office of Personnel Management about which your boss, General Clapper, said -- I guess he hadn't gotten the memo that you weren't supposed to say who this was attributed to, so he said, you've got to salute the Chinese for what they did. I took that as a hint about who the leading suspect was.

(Laughter)

MR. SANGER: We're slow at the *New York Times*, but even I picked up on that one, yeah. We had an attack on the Sands Casino, talk about really going after America, that the current threat assessment said was attributed to Iranian actors. And then of course we had the mother of all recent cyber attacks, the North Korean attack on Sony for what was I think I can say without violating editorial judgment here was to prevent the broadcast of a truly bad movie.

(Laughter)

MR. SANGER: As one of your colleagues put it to me once, if people go back a hundred years from now and ask what started the conflict between North Korea and the United States and you play them the movie, they would probably come out on the North Korean side.

ADM. ROGERS: That's real good. That's real good.

MR. SANGER: That's right. Okay so that's a pretty long list for one year. So tell us first what's changed here or why is it that we're seeing this rash of state-sponsored attacks?

ADM. ROGERS: Well, I'll tell you what if I could before I answer the question, first thanks very much for all of you for taking time from busy lives to spend an hour hopefully thinking about and interacting on a topic that I think is very important to us as a nation about how we're going to secure these networks that increasingly are shaping our everyday life whether you're in the government, the private sector, or in our personal lives. On a personal note, who here is a local from Aspen? Local. The reason I ask that is I have never been to Aspen Forum and I got to tell you I've heard about it, read about it, I am blown away by just how beautiful this place is.

(Applause)

ADM. ROGERS: There's a reason why there's a lot of nice things here. So thank you very much for, you know, allowing me to be a guest in your community for a little bit. So in terms of -- so what's changed, I think you have several trends converging. You've got more actors generating more capability, investing more in this. You've got a perception I believe that to-date there is little price to pay for engaging in some pretty aggressive behaviors, whether it's stealing intellectual property, whether it's getting in and destroying things as we saw in the Sony attack, whether it's going after large masses of data, whether OPM being the most recent but go back to the summer of '14 and we saw a successful penetration of largest health insurance company in the United States and the extraction of most of the medical record and the personal data information that they had. So you've got these trends coming together of more capability, more actors in a sense I think at the moment that there's not a significant price to pay and so you see actors, nation states, individuals willing to do more.

The last point I make is we generally will spend I suspect a lot of time talking about nation states and I'm the first to acknowledge that tends to shape a lot of the way I spend my time both as U.S. Cyber Command and as the director of NSA. But I would also remind people probably the single greatest sphere of activity in the Internet world in terms of threat is criminal, is still criminal if you just look at volume.

MR. SANGER: But the most sophisticated attacks you've seen so far -- most of them, there have been some very sophisticated criminal attacks targeting Home Depot and a few others, but some of these most sophisticated -- and we'll get to OPM in a moment because it was so fascinating -- had been state-sponsored. Maybe you can take us into the room a little bit for the debate in the administration last November and December during the Sony hack. Because here was an unusual case where the U.S. government in fairly rapid order, 5 or 6 weeks, that's pretty rapid for the U.S. government, made the decision to name the suspect country, send the President out to basically say was the leadership of the country -- was knowing of this and to make the case that they would pay a price as you said.

This was different from the way you treated almost every other major cyber attack I can think of, I can't remember another one that brought the President to the press room to name another country. So what made the North Korean case different and tell us a little bit about the debate about the utility of naming them and threatening retaliation?

ADM. ROGERS: So first I'll -- I was part of that process -- but I'll -- if -- I'd rather prefer -- let me just talk to you about what my input was and what my concerns were, and I'll give you some contrary view points because there were people who had different viewpoints in this process.

The first thing that I think made Sony unique was just how public it was in the sense that you had the North Koreans very publicly in the months prior to this talking about how they were prepared to take action if this film was released. And then the fact that Sony was hacked and a wiper malware was launched internally in their system which ended up slicking and destroying hardware, taking out some of their software and also ended up destroying hardware components in their systems, that was all a matter of public record.

MR. SANGER: And most people here probably aren't aware of what the destructive nature was, maybe you can do a beat more on that, they lost about 70 percent of their computing capacity, is that right?

ADM. ROGERS: Right, I mean a huge impact for them and for example, on the trivia side their phone system and their network structure were intertwined. So when they lost their network structure, they lost their phone accesses in their offices. So the fact that North Korea had talked about taking direct action and a course of nature -- they clearly were trying to use cyber as a vehicle to achieve a coercive impact, hey, don't do this.

So one of my concerns was this time it was a movie, what if the next time a nation state, a group, an individual, an actor decides I don't like the U.S. policy, I don't like the U.S. product. I don't agree with this particular position taken by a company or taken by an individual. If we start down this road, this is not a good one for us as a nation.

Another thing that I thought was different in this case also was the fact significant issue, that you know, Sony has talked about the fact that, well, let's talk for a minute about what was taken.

The North Koreans once they penetrated Sony's computer system extracted all their e-mails, made a matter of public record because they posted it online, Sony's internal salary structure. Sensitive e-mails among leadership talking about their views on working with particular artistic talent, their view on how you would get certain individuals to cooperate with the company and the making of different films, for example hey here's what they tend to like, this is way to get them to partner with us, you had e-mails released about disclosures, conversations between members of the corporation about internal views, about policies, about each other. You had intellectual property in the form of their films for 2015 all stolen. Copies of it all taken, downloaded to them, and made publicly available.

In the scale of it, Sony had some ways encapsulated everything we had seen before. Theft of intellectual property, theft of personally identifiable information, destructive activity, the use of a nation state to use cyber as a coercive tool. So in the aftermath of all that, you know, my viewpoint was number one, we cannot pretend that this has not happened. We must acknowledge that it in fact happened.

Number two, I also felt strongly we must attribute this to the actor who did it. And in this case we also had very high confidence about who exactly it was. This was very high confidence, not only the nation state, but the specific actor within North Korea who did this.

The third and final thing that I'll let you kick it back was as my concern was if we do nothing, then one of the potential unintended consequences could be does this send a signal to other nation states, other groups, other actors that this kind of behavior is acceptable and that you can do this without generating any kind of response. I didn't think that was a positive for the nation.

My other concern quite frankly was so if you're in the private sector, you're a company, you're being -- you receiving this attention from another nation state in this case and if the government is not going to do anything, what does this drive the private sector to? Do we start to get under the hack pack? Do you get into cyber mercenaries? Do you get into this idea that the private sector believes well if I can't count on the government then I'm going to have to do this myself? And my argument was that is going to be incredibly destabilizing and quite frankly it will complicate my life because the number of actors are going to have to deal with out there within the cyber arena is really going to proliferate and it's hard enough as it is now.

MR. SANGER: Boy, wouldn't you have loved to have heard the conversation among the North Koreans when they saw the salary scales of the Sony executives?

(Laughter)

MR. SANGER: Well, you were on the NSA, you probably did hear the conversation and the --

(Laughter)

ADM. ROGERS: Now you know why David and I have these conversations.

MR. SANGER: So your concern was that if you let this go by then you were going to as you said encourage others to go do this. But you've had many other attacks on major corporations that were not quite as public, didn't attract national attention because they weren't in the moviemaking business, didn't have salacious e-mails about spoiled actors and actresses where the U.S. government basically said you're on your own. There were attacks attributed to Iran, denial of service on banks. There have been attacks on stock exchanges. There was the attack in which, believed to be China, took some of the designs of the F-35. And in all of those cases the U.S. government not only didn't make public the name, but also didn't sort of announce in some significant way what the penalty would be. At least in North Korea's case there was some modest sanctions announced later. So do you see this as a change of approach?

ADM. ROGERS: Well, I think in this case that the difference what made Sony so unique in some ways was this destructive piece. The other part I would remind you is remember what the President said when he came out and made the comments where we publicly acknowledged it, we attributed it, and then we talked about consequences. And one of the things he said was and we will respond at the time and place of our choosing. I think one of the points that we're trying to work is we're trying to generate policy and figure more broadly what's the right way to deal with this challenge because this is not going to be a onetime factor -- is a one size fits alls approach probably isn't optimal, that we need to look at each situation for its specifics and make a decision about what makes the most sense in that particular context.

MR. SANGER: Apart from those sanctions I referenced which were announced in early January and attributed to this, has North Korea paid any price for this?

ADM. ROGERS: Well, my comment would be it achieved the desired effect at least in the near term.

MR. SANGER: Which is to say the North Koreans haven't done --

ADM. ROGERS: Haven't seen another one like this.

MR. SANGER: Haven't seen one like this.

ADM. ROGERS: Doesn't mean it couldn't happen tomorrow, first to acknowledge that, but in the near term, knock on wood, it seems to have achieved at least the near term impact that we were hoping for.

MR. SANGER: So let's take you to OPM. So --

ADM. ROGERS: There I was.

MR. SANGER: There you were.

(Laughter)

MR. ROGERS: Another three letter agency.

MR. SANGER: Yeah, another three letter agency. Office of personnel Management, always on the forefront of the minds of Americans thinking about the operation of the U.S. government. In fact, some people, some of your colleagues argue that one of the reasons that they weren't paying enough attention to sealing up the records of an organization that keeps the security clearances of just about every federal employee and contractor, is that they weren't thinking of OPM as a National Security Agency. They were thinking of it as a big boring bureaucratic record-keeper, and I don't even think they knew that they kept a number of their records in the highly defended computer system of the Department of the Interior.

ADM. ROGERS: So we're going for laughs in this session. Is that my take away?

MR. SANGER: That's it. So tell us a little bit here, you've made the opposite decision, you haven't -- other than General Clapper's reference, there hasn't been an official sort of attribution; there has not been a declaration that the offender here would pay the price. And yet you could argue that the damage done here was on a vastly larger scale than Sony. And we were talking about millions of personnel records and not just names and social security numbers, but if anybody has ever filled out one of these standard forms that, you know, everybody you've ever met, everybody you've done business with, the names of your kids and so forth.

ADM. ROGERS: Right, every address you've ever lived --

MR. SANGER: Yeah.

ADM. ROGERS: -- every job you ever had. Well, let me step back first. One of the lessons from OPM for me is we need to recognize that increasingly data has a value all its own and there were people who were actively out there interested now in acquiring data, in volumes, in numbers that we didn't see before. So if you go back a couple of years, we had tended to focus on this idea of cyber in many ways as either focus on the theft of intellectual property, research and development, products, attempt to achieve market advantage to bypass decades of research and development effort and take advantage of the hard work of others.

And we really hadn't come to the conclusion that perhaps not only is that of concern, but you combine the power of big data analytics, and the fact that today the ability to bore through huge amounts of data and find seemingly disconnected and unrelated individual data points and bring coherent meaning and insight, something that wasn't there in the past, you combine those two things together, and one of my takeaways from OPM, and we're looking in this broadly across the government, it's a focus for our team within the Department of Defense, concentrations of large data now become incredibly attractive. It's not just about this idea of, hey, I want the plans for the F-35. Hey, I want to see what you're doing in acoustic technology. Hey, I want to see what you're doing in the development of advanced dye products for example, that the world we're coming into now as the target set is getting much, much broader, which from a defensive standpoint makes the job even more difficult.

MR. SANGER: So what do you think the objective here was? You said, the data itself is valuable. Valuable for what?

ADM. ROGERS: I think it does two primary things for you. Number one, from an intelligence perspective, it gives you great insight to potentially use for counterintelligence purposes. So for example, if I'm interested in trying to identify U.S. person to maybe in my country and I'm trying to figure out why are they there, are they just tourists, are they there from some other alternative, there's some interesting insights you can draw from the kind of data you're able to take from OPM.

The second reason that I think data becomes increasingly attractive is, we are watching -- in particular at the moment you see this most common in nation states and the criminal sector, we are seeing actors use their insights about people as individuals to tailor products in the form of e-mails that seem to you as a user so appropriate that you would receive it, it's from somebody I know, it's a topic that I really care about, it's an issue that I've been really focused on for a long time, as a vehicle to actually get you to open an e-mail, click on an attachment, click on a video link, it's not perhaps unrelated that it in the last nine months I am watching huge spear phishing campaigns coming out of several nations around the world directed against U.S. targets. They're not unrelated to me.

MR. SANGER: Are those state sponsored spear phishing campaigns, are they private, are they criminal?

ADM. ROGERS: You see both state and criminal entities using it as well.

MR. SANGER: Okay. Let me ask you briefly about one country that's been in the news a lot lately, Iran, and then I want to turn to your cyber mission forces that you've created. So we just concluded -- the United States has just concluded a big nuclear agreement with Iran that if successful would freeze their nuclear program for 10 to 15 years. While those negotiations were going on, the Iranians have made no secret of building up a very effective cyber core. They've done at least three or four big attacks that would become public, one on Saudi Arabia, two that we've discussed here already in the United States, including that casino that we talked about.

Could you see a situation in the next few years in which the Iranians take the kind of effort that they have put into nuclear, a weapon you can't really use because of the retaliation that happens, and put that focus and effort more into the cyber realm, a weapon that they've shown they can use.

ADM. ROGERS: Well, I would argue regardless of the nuclear piece, we have watched the Iranians increase their investment in cyber for a period of time now. This is not a new phenomena, and it's not something that in my mind is tied to this nuclear piece. I think they clearly have come to the decision that it represents capabilities and options that they believe are of value to them that potentially generate advantage for them and so they're investing in it, and it's something we pay great attention to.

MR. SANGER: So tell me a little bit about these cyber mission forces. We discussed them first here I think about 2 years ago. Ash Carter, when he was still the deputy secretary, came in, was kind enough to go through an interview as you have. And his argument at the time was that these mission forces were loosely modeled on special operations forces, that you needed a grouping that -- of specialists who could step into some very complex issues. You've reformulated them a little bit, so tell us a little about what they do, there's supposed to be 6,000 of them, is that right?

ADM. ROGERS: There's 6,000 individuals. So at the United States Cyber Command, three primary missions. The first is to defend the Department of Defenses' networks. The second is to generate this cyber mission force and I'll talk about that in a minute, and employ it across the department in a range of operations from the defensive to the offensive. And the third is, if directed by the President or the secretary, is to defend critical U.S. cyber infrastructure from significant cyber intrusion.

To do those three missions -- you know, we -- there was Keith Alexander there before me who actually stood the organization up; we came and I was part of that process as Fleet Cyber then. We came to the conclusion that to execute those missions, you needed -- just like any other mission set we have in the military, you needed trained men and women who were organized in units to execute the mission. And so we came up with this idea of teams, and we decided that because we have multiple missions we needed multiple kinds of teams. So simplistically we created three kinds of teams.

One kind is focused on defending networks. One type of team is focused on supporting combatant commanders around the world, Pacific Command, Central Command, and helping to use cyber as a tool to generate more options to support them in their operational objectives. And the third kind of team we created is to defend that critical cyber infrastructure from significant cyber intrusion. Each of the teams is slightly different. We gave ourselves 3 years from Fiscal Year '13 to fiscal year '16, to physically build that out. We said it would be about 6,200 dedicated individuals, and about 133 teams.

We're about half way through building the teams, and I would tell you right now there are -- the initial teams on the defensive side in that first mission set are deployed literally around the world defending DOD networks. I use them to deploy, to meet certain requirements. I, for example, just authorized -- the last thing I did before I left D.C. last night to be honest was I authorized the deployment of one team to work one particular issue somewhere in the world. The teams that are working --

MR. SANGER: I'm sure you are going to go on and explain what that was.

ADM. ROGERS: -- for the -- yeah, I was going to say no.

(Laughter)

ADM. ROGERS: The second kinds of teams those are allocated to support combatant commanders. Again, by half way through that, but you have those teams today aligned against missions as defined by Paycom, by Ucom, by CENTCOM, looking at areas of interest to generate more options in the cyber arena for commanders. And then thirdly, probably the most mature because it was the area we really started first because remember U.S. Cyber Command stands up and comes to -- starts to come to bear at the time and particularly we were really watching this Iranian attempt to knock down financial websites in the U.S., in the major banks and financial institutions in New York and elsewhere in the nation.

So that was kind of one of the primary initial areas of focus. It's the most mature. We've generated some really good capabilities that I think we can bring to bear to them, if we get some of these massive cyber intrusions against critical U.S. infrastructure, then we have some good capability there.

MR. SANGER: So what you're telling us is that if the President, and the secretary of Defense, and you so ordered, these groups would step in to defend private networks, might be banks, might be the next Sony case. But where do you draw the line there because President has made clear by both his decisions and his words, he doesn't want the U.S. government to be the one that is the primary defender of private networks? If it is, no private company will spend very much money on cyber defense.

ADM. ROGERS: Right.

MS. SANGER: They will all just wait for you to come in.

ADM. ROGERS: So that is not -- not the plan. Here's what the government signed up to, and this is what the broad strategy is. The U.S. government has designated 16 segments in the private sector whose cyber infrastructure has significant implications for the nation's security. So think about aviation, think about financial, think about power, think about the road, think about rail, there's 16 different segments. And what DOD said was so we believe that the nation is going to be turning to us to help defend it in the midst of potential crisis. And as a result what we said was, we will generate capacity that we could potentially apply if directed against those portions of those 16 segments.

We also talk about, when we talk about criteria, so what makes you decide how are you going to defend this versus defend that. One of the things we talk about and if you read the DOD cyber strategy which Secretary Carter just unveiled on Silicon Valley on the 23rd of April, five major components to that strategy, and one of them talks about how we will respond to cyber events of significant consequence in the private sector. Trying to make the point as David did, the government is not signing up to this idea of, well, don't worry if you're in the private sector, the government is going to defend everything.

In the end, it is all about our ability to create partnerships. It is about ability of the private sector and the government to team together to generate better outcomes for the nations. How can we take advantage, not just for us, but our allies as well? How can we take advantage of the insight and information that the government is able to generate along with the insight and information the private sector is able to generate to bring together a common picture?

MR. SANGER: So let's talk about how you put together that picture. So the private industry says they get a lot of data and frequently when they see the FBI warnings they say, well, these are about things we knew about already because we've seen them on our systems. You have a unique capability though that they're not allowed to do, which is, as a Navy guy, you can create early warning radar of a cyber nature, put in networks that are around the world, many of the foreign networks under the authorities that the NSA has, and so forth. We read about a lot of this during the Snowden disclosures.

So that you would have nodes where you would actually see an attack massing and those same nodes could be used to counter an attack. Once you put it in, it's like the port that a doctor might put in to both examine the patient and apply a treatment. So to the degree that you can tell us, how active are you in putting this early warning radar in networks around the world? And how critical is that in being able to determine whether an attack is coming in? Can you do it without it?

ADM. ROGERS: So clearly we think it's an important part of the strategy. Specifically we have said NSA will use its foreign intelligence mission to generate insights as to what key cyber actors around the world are doing. And the idea is rather than just waiting at the point of termination where the attack lands so to speak, if we can get ahead of this problem set by getting insights at the point of origin where the attack is coming from before it originates that we can provide indications and warning to give both the government and the private sector heads up on, hey, this is coming our way and we need to be ready for it, here's what the target's going to be, here's what it's going to look like. These are the kind of we call it tactics, techniques, and procedures. This is what you're going to see. This is how you can best structure your defense to defeat it between NSA and U.S. Cyber Command. We try to do all of that with the private sector.

Partnering -- the final point is, remember, we're just one part of a much broader enterprise, both externally outside the government as well as internally in the government. DHS, the Department of Homeland Security, and the FBI, being probably within the U.S. government are two biggest partners in that regard on the cyber defensive side.

MR. SANGER: And how successful is the early warning? Think of the North Korea Sony case. You were able to build the case very quickly, that it was North Korea, and you said you even knew the actors within North Korea, but I take it you didn't see that attack massing or you would have done something about it before.

ADM. ROGERS: In some cases, it works very well, in other cases the challenges as I said, you need to have both ends of the string. In an optimal world, it's defense in depth, you want to work both sides of this. And so one of the reasons why the partnership is so important, I am not using NSA resources to monitor and safeguard U.S. networks. That's not our mission, it's against the law. That's not what we're here for.

But on the other hand, I do want to create a partnership where we're able to share information with each other. So in this case one of the things that frustrated me about Sony for example was Sony goes to the U.S. government, we come to the determination that Sony was a criminal act. FBI is designated as the lead. FBI comes to NSA, says, hey, we could use your analytic help, be a partner with us in working with Sony. Sony, I thought to their credit, I give them big accolades in this regard. They gave us everything we asked for.

So we said in order to generate the insights we need, here's the kind of detail we need. Sony did everything that we asked. We were able as a result of that to generate insights relatively quickly about, okay, here's what we're seeing, but my frustration with Sony was, hey, this is great, but the horse is out of the barn. It really doesn't get us where we need to be if I'm doing this after the fact. Why can't we have this kind of dialogue prior to the attack so to speak.

MR. SANGER: And is one of the reasons that people have been concerned about naming China other than your boss in the case of OPM, is that espionage kind of cases involve activity that NSA cyber command would do in response because espionage is espionage, is part of what the mission is and therefore that's in a category of basically permitted kind or understood actions between countries. So you me be able to put these advanced warning in, but you may not want to blow the whistle because you may not want to create a precedent in which espionage is not acceptable on either side.

ADM. ROGERS: I mean, I think it's clearly part of the discussion, but I'm not going to sit here and tell you, hey, it's the overriding factor that has led to the current decision to continue to review this and assess what the right long-term way ahead is. I'm not going to argue that that's the factor that has brought us where we are today, but I won't deny for 1 minute that it's a factor that you do think about in any regard. So what are the implications for the U.S. and our friends and allies, we thought about that when we are responding to Sony, we think about that in the OPM scenario. It's a factor we think about in every situation.

MR. SANGER: When I travel around the world, but particularly in Europe, I run into a lot of government officials whose desire to cooperate with you either on the NSA side or on the Cyber Command side has been dramatically limited by the Snowden revelations. In Germany just a few weeks ago there was another outbreak of revelations that suggested that the U.S. government was listening in on employees of the chancellor's office, not the chancellor herself. Of course there had been earlier disclosures concerning that. So tell us how you create these partnerships when you've got countries from Germany to Brazil to many others who are talking about walling off the Internet to keep you out?

ADM. ROGERS: Well, I'd only remind you, I reflect the statement by Chancellor Merkel herself in the last few weeks. Even as we're working our way through issues of concern between our nations, the intelligence relationship between our nations remains critical because she specifically said in the last month or so the relations with NSA is critical to Germany's security, that the information NSA provides to Germany and as well as a broad set of partners around the world. There's a reason why we continuing having relationships, I haven't lost a single partner because of any of this. Why? Because we still generate value for them in terms of the information we share with them and that is critical I think for both of us.

MR. SANGER: Have you changed the way you look at targeting American allies and partners, so do you now go through the list and say, gee, if this operation becomes public, the kind of damage it's going to do to us may be greater than whatever intelligence I'm getting out of it?

ADM. ROGERS: And so the aspect of cyber security in that question is?

(Laughter)

MR. SANGER: Well, because you've got partners who are telling us -- no matter what Chancellor Merkel said, you've got partners who are publicly saying we're going to hold hearings, we don't want this level of cooperation. Or we want to create our own part of the Internet that is separated all from everybody else.

ADM. ROGERS: So I remain confident in our ability to partner with nation states around the world as long as we generate value that helps them.

MR. SANGER: Okay.

ADM. ROGERS: Without that value I'd be the first to admit that that change is dynamic, but because we are able to generate value and insight which helps defend their citizens, help defend their interests and ours, you know, I remain comfortable, hey, we'll work our way through all this.

MR. SANGER: And let me ask the same question about working with your Silicon Valley partner. So when Secretary Carter was out in Silicon Valley for that same speech --

ADM. ROGERS: Right.

MR. SANGER: -- he went out, met a number of Silicon Valley entrepreneurs, said, look, we need your help in ways that we've never had it before. We had it during the Cold War, I'm not sure we have it now. And you've had Apple and Google and others announce encryption techniques that they've said were designed specifically to assure their users that the U.S. government, the Chinese government, the Russians or anybody else isn't getting into their stuff. So how is that changing the dynamic of your ability to cooperate within --

ADM. ROGERS: I mean, we continue to partner with industry. I'm out in the Valley fairly regularly because quite frankly my attitude is that we have got to have a dialogue with each other, we have got to work our way through this. We at its heart both I would argue particularly on the NSA side, but one of the comments I make at NSA to the workforce is at its heart we are an organization that employs technology to defeat technology. And much of that technology on both sides of the equation is developed by others outside the organization.

Partnerships are critical to the future for us and we can't allow the current dynamic to stop that. The positive side for me is most people, you know, have gotten to a position where they're willing to talk. I had also highlighted, if you look at the telephone metadata issue in 215 (phonetic), 18 months ago I think the discussion largely was, hey, this program is dead, we're never going to do this again. And yet I think we are able to step back and ask ourselves, so is there value with the appropriately controlled legal framework for NSA to be able to access in a controlled manner for a specific purpose under a specific set of rules, is there value in NSA being able to access that.

The decision, law was passed, yes. Difference in the new structure, hey, NSA won't hold the data, the providers will. My attitude was a good example of we can work our way through this and we can get to a position where we can try to address both of the imperatives that face us.

MR. SANGER: Since --

ADM. ROGERS: Let me finish both imperatives real quick.

MR. SANGER: Oh, sure.

ADM. ROGERS: The imperatives to me and they are two imperatives, it isn't one or the other, it isn't about, well, what are the trade-offs you've got to make.

The rights of each and every one of us as individuals to have an expectation that the capabilities of the government will not be used against us indiscriminately or abused is foundational to our structure as a nation. At the same time --

(Applause)

ADM. ROGERS: At the same time, we've got to acknowledge we live in a world right now where there's a lot of groups and organizations out there who had -- if they had their way forums like this would never exist, the idea that as a private citizen you could go sit down, talk to a group of senior government or private leaders and ask a question about, hey, talk to me about policy X, Y or Z, why do you do things this way. Hey, I don't agree, here's what I see, you'd never see that in this world. And so we've got to acknowledge that there are groups out there who want to destroy what we are and who we are. And so we've got figure out how do we meet both these imperatives and the, you know, U.S. Freedom Act, I think is a good example of, hey, we can get to a middle ground here.

(Applause)

MR. SANGER: So your middle ground is that the telecoms by and large will be holding on to this data and you'll be able to go get court orders in the FISA court or other courts to go get it. Technologically that's a bit of a trick to pull off, tell us where that stands right now, how quickly do you think you'll be able to get the U.S. government out of the business of retaining this bulk collected data?

ADM. ROGERS: So under the terms of the legislation we have 179 days from the date the law was passed on the 29th of June. I think the trigger date now is November 29, 2015. Under the terms of the legislation we must have transitioned to the new program no later than 29 November, 179 days after the law was passed. So we're in the midst of the process of doing that right now. I'm comfortable that we're going to be able to do it. I have yet to run into a technical problem or a lack of cooperation that leads me to believe, boy, this is going to be problematic. I think we can get there and we can do it in the time-frame with the organizations we have been working with previously.

MR. SANGER: And if you develop a lead of an individual who may have been in contact in the United States or elsewhere with a suspected terrorist, do you believe that having that database spread out across many different telecoms now, you'll still be able as quickly as you were before to go track down that conversation and figure out --

ADM. ROGERS: I mean, there is no doubt, there are trade-offs. We've got the continued existence of the program. We've got the ability to access the data which I thought was important because I thought it generated value. It's not a silver bullet that in and of itself guarantees we're going to stop every terrorist threat against the United States. You will never hear me say that, it is a tool that helps us provide insight and when put together with other things helps us to build the picture. If you are an intelligence professional, if you watch the movies half the time it's, well, there is this one silver bullet that does everything.

In my experience as an intelligence professional for 30 years, it normally doesn't work that way. It's our ability to bring together a lot of different things to try to create a more broader picture. So we're going to have to work our way through it. I think we are going to be fine, I just don't really see major issues there. The other thing I liked is the legislation also provided for an emergency proviso where if we feel that we're in an immediate threat, authority is granted to the attorney general to direct that the data be provided to us, but then we have to go back, inform the court in writing as to what we did and why and the court has to come back and tell us do they agree or do they disagree. So we don't get a blank check.

MR. SANGER: A last question for you and then we're going to open it up for the audience. A few years ago if you came to this conference you would have heard a lot of people warning against a future cyber Pearl Harbor.

I think that was the one that Secretary Panetta used when he gave his first big cyber speech. What we've been discussing here for the past 45 minutes have not been a cyber Pearl Harbor, it's been short of war operations, it's going after a company like Sony to try to stop a movie, it's collecting up vast amounts of data from a ill-protected government database, it's going after healthcare data that may give people insights into many citizens of the United States. But it is not shutting down the cell phone systems. It's not --

ADM. ROGERS: Yet.

MR. SANGER: It is not yet. So here's my question. Do you think the threat is evolving into something bigger, but perhaps less dramatic than what we first discussed or do you think that the threat of turning off vast amounts of infrastructure, the power systems in New York -- we had that a day a few weeks ago when you had in rapid succession a problem with the New York Stock Exchange, a problem with the Wall Street Journal on their website and a problem with United Airlines --

ADM. ROGERS: Airlines, right.

MR. SANGER: -- all in the same morning. You must have been thinking, gee, could this be the morning we were worried about.

ADM. ROGERS: Oh, yes. Is this it?

MR. SANGER: So tell us what -- which of these you were most worried about and in what order, how do you rank them?

ADM. ROGERS: Well, put more broadly, hey, what concerns me, you can see we're watching a steady ratcheting up of activity. If the trends continue the way they are, then I don't think the destructive piece that we saw in Sony is a one-off, we're going to see more of that. I don't think that the theft of, you know, large data segments, not just intellectual property, but large data segments, that's not going to stop. The intellectual property piece will keep going, the criminal piece isn't going to go, isn't going to change. As I look, if I -- so somebody asked me, so what do you think is going to happen in the next couple years? I think you're going to see nation states start to create partnerships with a broader set of actors as a way to attempt to confuse attribution, so it makes it harder for us to tell policymakers, here is who it was, it was this nation, this particular actor, because remember, a policy response in broad terms always starts with the first question I always get, who did it, always starts with who did it. Then it's how did they do it, why did they do it. So you're going to see nation states attempt to secure our ability to say who did it.

MR. SANGER: Through criminal groups?

ADM. ROGERS: You'll see criminal groups. I'm already watching that unfold now. You'll see other similar kinds of things with other groups. To date the terrorist world has tended to use the Internet as a recruiting tool, as a means to disseminate ideology, to generate resources and money. You've heard ISIL publicly talk about this idea about why don't we get into the hacking business, so if you start to see actors out there outside the nation state world suddenly start to think that cyber is a weapon system, offers an attractive set of capabilities that would be really worrisome. Put it another way, what I tell people in our own organization is I believe that during my time as the commander of United States Cyber Command, I will be directed to deploy capability from U.S. Cyber Command to defend critical U.S. infrastructure either in anticipation of or in the aftermath a significant cyber event.

MR. SANGER: You haven’t yet.

ADM. ROGERS: It's one of those 16 segments. Not yet, but it's the when, not the if to me.

MR. SANGER: Great. Well, we're going to go out here.

ADM. ROGERS: So you're feeling pretty good right now.

MR. SANGER: Yeah.

(Laughter)

(Applause)

ADM. ROGERS: You're feeling pumped.

MR. SANGER: So we will grab a few questions here. We'll ask you to wait for a microphone, give us your name and ask a short and crisp question. Right here.

SPEAKER: Admiral, Charlie, General, from (inaudible). Good to see you sir.

ADM. ROGERS: Hi, Charlie.

SPEAKER: Recently DOD issued this Law of War Manual, has pretty good chapter on cyber operations. My question is, do you feel that you have the rules of engagement that you need, are they still evolving or what?

ADM. ROGERS: So clearly whether you want to talk rules of engagement, authorities, we're clearly still working our way through this. The fundamental principle to me is, we built a good framework in the kinetic world. It's a good departure point for us. So I look for the same kind of broad trends, proportion of response, appropriateness of response, the specificity and discreetness so to speak of the response. The same things that have conditioned my life in the kinetic world as a serving military officer for 34 years, that's the kind of point of departure for me intellectually in the cyber world. You see that in the framework in the Law of War, I think you'll see that continue to play out further for us.

MR. SANGER: Okay. See, we had a hand that was right over back in here, we had -- I don't see it now. So I will go back right over here, yeah.

SPEAKER: My question refers to something that Director Comey said yesterday at the forum. He was talking about the fact that ISIL is one of the things that he worries about most and then he mentioned encryption apps as how it is so difficult for him to follow this. So talking to you about the same thing, is it the length of the bit codes that is making it so difficult for you to decipher these encryption codes from ISIL?

ADM. ROGERS: I won't get into the specifics because I'm not interested in letting an opponent understand exactly what it is that we tend to focus on. I would just say broadly commercial encryption right now represents a significant technical challenge that was highlighted in the media leaks. We've watched terrorist groups around the world really focus on that. The standard process we watch now, terrorist actor reaches out via social media, tries to generate as much contact with as many people as possible, creates initial contact in social media. Once they believe that the person they're talking to might be of value to them or might be interested, you'll immediately get a reference to switching to an encrypted application as a way to bypass security and law enforcement's ability to physically access the contents of the conversation. We're watching that play out all over the world now.

For me it's a foreign security and national security challenge. For director Comey he's seeing the same trends in the United States, you know, I don't do that because we're an informed intelligence organization, but he sees the same trend in the ISIL world. But now you're seeing the same trends where it comes the day-to-day activity in law enforcement in terms of crime.

And so I think broadly what we're trying to come to is, so as a nation given the change in technology, how do we address the need to ensure that people can't use this technology to attempt to violate the law or do harm to others, whether it's our nation or other nations. And we're trying to figure out I think collectively what's the best way to do that realizing there's no one single answer and no one single side of this issue whether you're the government or the private sector has the answer. This is all about how do we get together and sit down as a nation and figure out how we're going to do this, what's the right answer, is it technology, is it policy, is it a legal framework. I suspect it will be some combination of all of that, but we need to have this dialogue and figure out what's the right way ahead.

MR. SANGER: Okay. We've got time for just one or two more. Gentleman right here.

SPEAKER: Yes, I wonder if you would explain more about the appropriateness of response and I'm -- you know, is it a cyber, is it military, is it financial, and how that relates to the type of cyber crime that is committed?

ADM. ROGERS: So one of the things we talk about is, for example, just because someone comes at us in the cyber arena doesn't mean the response has to be in cyber, much like one of the things we talk about it in appropriate. So if I'm on a ship and I'm off an enemy coastline and the enemy fires a missile at me, I have the inherent right to self-defense, I can shoot down that missile. I then do not have the authority to use every weapon system on my ship and decide I'm taking out every cruise missile site in that nation. You know, that's not the framework we've created all the time. That's part of this idea to me of appropriateness of response. And so much as we've done in the kinetic world, we're trying to do the same thing in the cyber domain. So what is appropriate, what is the right context, what is the right application here and there's no one-size-fits-all, every situation is slightly different.

SPEAKER: And probably to just follow that one beat further, when you go into the new cyber strategy that the secretary brought out, there is a brief reference to preemption, something we hadn't debated in Washington since Iraq days. But I could imagine a situation in which you saw a major cyber attack looming against an American corporate target, a government target, cell phone network, whatever. Could you imagine a situation in which the United States would act preemptively primarily by cyber means, but not necessarily by cyber means, to stop either a private actor or a state sponsor from launching an attack on the U.S. that you knew would be down --

ADM. ROGERS: So just as we have those kinds of discussions in the kinetic world, I fully expect we'll have those kinds of discussions in the non-kinetic world and we'll decide at the time and place and the specific set of circumstances what's appropriate and what's not appropriate.

SPEAKER: Have you had a case yet where you have seen something coming and you had to have that debate?

ADM. ROGERS: I don't know if I'd phrase it quite that way. Clearly we've had circumstances where we see things coming and we're able to provide warning. Again part of it goes to what's the purpose. You know, we'll sit there and try to talk about, so what's the intent on the part of the actor. So every situation is a little different. If we could let's take a couple more questions --

MR. SANGER: Sure.

ADM. ROGERS: -- because you guys came a long way in here and you waited, so it's the least we can do.

SPEAKER: Admiral, my name is (inaudible), I'm one of the Aspen scholars. I'm curious when it comes to these sort of cyber forces that you're trying to stand up, how are you recruiting and training and how are you getting people who may not be necessarily be interested in a 20-year career in the military and putting on a uniform, or, you know, may have smoked pot in the past 7 years, who may have the type of skills that you are looking for?

ADM. ROGERS: I thought I was going to hear, well, I have this friend whose smoked pot one time.

(Laughter)

SPEAKER: And then maybe go on to the private sector and more generally raise the level of cyber hygiene, that was something that was talked about earlier today.

MR. SANGER: I'm sure none of the coders you needed have ever touched pot.

ADM. ROGERS: So on the positive side we are not having a problem to-date either accessing the talent we need or retaining it. That is driven in no -- and that's not unique to cyber, I would argue it's the same thing in almost every segment of the U.S. military. Our advantage to me is the ethos of the institution, the idea of service and sacrifice, the idea of mission, hey, I'm doing something that matters to the nation, I'm doing something that's relevant and matters to the greater good. And then also the fact that quite frankly we're going to let you do a lot of neat stuff you really can't do anywhere else.

(Laughter)

ADM. ROGERS: That's another aspect that I go to mission. I get a lot of people who say, you know, I really want to get into some of that stuff. The net impact is to-date we have been able to recruit in both the numbers and the quality and we've been able to retain them. I always worry is that going to stay the same over time. When I think about the future, the comments I make both at NSA and U.S. Cyber Command are the traditional pattern we've had where our workforce tends to stay with us for decades. When I'm out in the Valley, their model is, you work for us anywhere from 2 to 5 years and then you move on. You know, they are amazed when I tell them, our average, the high-end workforce that I use and some of the neat cyber stuff we do, they'll be with us 20-30 years because they love the mission, they love what they're doing, they get this sense of return and really self-actualization.

One of the things I think we need to do the future is how can we create a model where people can spend time with us, go to the private sector and come back. Also how can we create a model where people from the private sector can come into us and it isn't necessarily at a starting level; hey, why can't you come join us at the mid-level, why can't you come be a senior with us. Hey, it doesn't mean that we're going to grab you from the private sector and say, how would you like to be the director of NSA, but it does mean, hey, we could put you in a significant leadership position where you could be helping to shape the future for us and how we're generating technology and how we're applying technology. You really could bring value in that regard. That's what I want to get to.

And the last segment that interests me, and this one always gets the lawyers going, one of things that strikes me in all aftermath of media leaks, I'm watching two cultures that think they understand each other, but are talking past each other. When I talk to my workforce about, so tell me what you think about you teammates out there, you know, working in the Valley for example, I'll often get, hey, they're focused on money, hey, they are just interested in short-term returns. Then I will say, stop. If you ask them what their vision is, we are harnessing the power of technology to change the world for the better.

Hey, I tell my workforce that ethos is good for the nation and I'd love to have people like that with that ethos in our workforce. Likewise when I go out to the Valley, I will sometimes get, well, your workforce is the one that didn't want to work with us or wasn't good enough to come work for us and I'll often say, now, let me understand this, you recruit my guys like there's no tomorrow.

(Laughter)

ADM. ROGERS: So you're telling me that this is a workforce that really, you know, they weren't good enough. Let's not kid each other. I just watch these two segments at times really talk past each other. Each thinks they understand the other. I'm not sure they do. And so one of the things I have talked to the team not only about our people going out, but hey why can't we get private industry to come in and work with us, hey, company X, Y or Z, you want to send somebody in to work for us -- work with us for one year on an internship kind of program, get a sense for who we are, how we organize, what we do, what we don't do, what technology is important to us, what do we -- where could we get value from what you do, so you understand what we do; I really like to see how we can model the workforce of the future a little differently just because I think it's where we're going to be driven anyway.

(Applause)

SPEAKER: Thanks David, and thank you, Admiral, for sharing your thoughts with that.

ADM. ROGERS: We gave --

SPEAKER: And I am surprised I have to bring own my microphone as well.

ADM. ROGERS: There you go. Oh, good.

SPEAKER: My name is (inaudible) with ZDF German television, so I had a long way to come here. Thank you for giving me the chance. Number one question would be, there have been so many documents coming out of the Snowden leak plus the WikiLeaks, David mentioned it in recent weeks, but there has been next to nothing in all those documents on Russia and on China. So there are people who are suggesting, well, maybe there's a reason to it, there could be an orchestrated intelligence operation behind it. How do you feel about those theories and if I may because David brought it up, I have to ask the other question as well, in those recent documents from WikiLeaks of course and David mentioned it, there was the proof that German government officials and not few, many were targeted by NSA and I understand that you won't give me a specific answer, but hypothetically --

(Laughter)

SPEAKER: -- what would be the reasoning about -- behind spying on friends?

ADM. ROGERS: So let me take the second one first. As a matter general policy I just don't talk about the specifics of intelligence operations. So broadly what I tell people is, look, every nation is trying to understand the world around it. We have specific tenets that drive what we do. We have shared with our allies around the world what those broad tenets are, what we do in broad terms and why. There's a rationale for everything we do, it is tied to a specific national security objective. We are very specific in sharing with our allies around the world to include our German teammates the insights that we were able to generate. We very much acknowledge and realize that we're part of a broader partnership and that this is relationship, has to generate value for both sides.

In terms of the first part of the question, it's not by chance to me that the leaks that you have seen publicized to date sure seem to be oriented as an attempt to drive a wedge, to try to harm relationships. There's -- you're not saying hardly anything about, you know, some of our very traditional kinds of targets and I think all of us would feel very comfortable as a nation, well, I hope you're paying attention to that, I hope you're generating insight against that threat, I hope you're generating knowledge that helps ourselves and our allies deal with it and anticipate it. Instead to me much of what you're seeing seems to be focused to achieve very specific outcomes. So I just think it's up to us to step back, use our own experience, use our own perspective and decide, so what do we believe, what do we not believe.

MR. SANGER: Gentleman straight back here. There's a mike coming to you.

ADM. ROGERS: Disadvantage of being in the middle sir.

MR. SHAPIRO: Thank you General -- Admiral. Steve Shapiro and thank you David for calling me.

ADM. ROGERS: Hi Steve.

MR. SHAPIRO: With all the discussion of the recent cyber policy and its release and the concept of significant consequence, although we've touched on this in an earlier panel or two, I am curious still about drawing the line between cyber espionage and cyber military or .gov et cetera et cetera. It seems like it's an almost arbitrary line and in this regard I'm struck by recent news reports with respect to the OPM breach which can do significant damage to national security that it's being treated with the etiquette of Cold War espionage. We're not -- not only are we not giving -- making attribution, but we're not even taking steps to backwash the data and perhaps damage it for future use, we're essentially according to the news reports doing very little in this regard because it's under the category of espionage. So I wonder if you could comment on how that line is drawn, whether you think it's a real line, and if you do, are you gritting your teeth while this is, well, this nothing is going on.

ADM. ROGERS: So the first comment I would make is just because you're not reading something in the media doesn't mean that there's not things ongoing. So I would argue let's step back and see how this plays out a little bit. So -- and I'm the first to acknowledge ongoing dialogue. More broadly about how do you get into this, well, how do you define consequence, how do you define significance, is it you want to do it by some dollar figure, hey, if you cross some $100 million, $300 million, $1 billion threshold, is it loss of life, is it significant impact on day-to-day life for Americans, is it a threat against the value. One of the things we're talking about in the aftermath of Sony was does this represent an attack against the very values of our nation, freedom of expression, you know, freedom of the media, freedom of the press and we're asking, have we tripped the threshold here because we've gone against our values and our legal framework.

The conclusion we've come to is every situation is unique, we need to do it on a case-by-case basis and when you don't work our way through what are the implications of if you do or you don't so to speak, publicly attribute as we did in the Sony case where we came to the conclusion, we felt we needed to acknowledge, attribute, and talk about consequence and do it publicly.

MR. SHAPIRO: Take us through the analysis of this case where (inaudible) national security --

ADM. ROGERS: Well, because OPM is an ongoing issue, I apologize, I'm just not going to get into the specifics of the ongoing discussions here. But I would acknowledge, hey, to date we have taken a different response to OPM. There's a thought process there, but I am the first to acknowledge, we have to date taken a different response to OPM. One last question. Take someone over here. Oh-oh, you're out, sir, she's pointing you out.

SPEAKER: First of all I want to thank you for coming

ADM. ROGERS: No, no, thank you.

SPEAKER: -- and this has been a very thoughtful discussion.

(Applause)

SPEAKER: And unfortunately there is so much that has been read and we hear in the news and there's been a lot of talk about we're really not ahead of the curve in terms of being prepared for this type of work, these attacks and I was just wondering, someone said 10 years to 15 years that we're kind of behind and I'm not trying to say that that's a good thing, but is it something that what can we do to either catch up or not look at it that we're behind?

ADM. ROGERS: So we are clearly behind where we need to be, I would argue collectively as a nation and in many segments within the nation to include the government. The positive side is always around (phonetic) people, the first step to solving a problem is recognition. So we're -- boy if I go back just 3-5 years ago, the debate's about, well, yeah, but is this something that's really important, is this something I should really put resources against, is this something that really would be significant? Yes, I got the science-fiction thing here, Rogers, but, you know, is this thing going to be real? I mean, we used to have those discussions, we sure don't have those discussions anymore, so we've got recognition of the problem.

The challenge I think that we're dealing with is a couple things. We need a fundamental change to our culture in terms of how we prioritize this, the way we look at it. Traditionally we viewed cyber and cyber security, well, this is something so specialized, so technical that a small segment of my workforce does this. This is what my chief information officer, my chief technologist does, this is what my IT guys do. As a member of a board, as a member of the C-suite, as the CEO, that's not my job, that's what they do. I pay them good money because the expertise is so unique, go do your thing.

Clearly that has got to change. I think there are also in the culture piece it's got changes of recognition that every single one of us in this domain is a point of vulnerability. Our cyber behavior drives in no small part my ability to defend DOD's networks. If I had good -- if we had good fundamental user behavior, I'd probably kill 80 percent of the problems that we deal with just because of basic cyber behavior. So there's a requirement here for all of us. Also we've got to acknowledge, we've got to make fundamental resource investments here.

The networks of the world that we're living in now were largely designed in an era in which defensibility was not a core design characteristic, redundancy was not really a primary design factor, and resilience, the ability to be penetrated and take damage and keep working, none of that, what tended to shape our network structures was costs, get me the best output at the lowest price, ease, hey, look, don't make this complicated, don't get me into these complex encryption screens, don't make me carry tokens around with me. Make my life easier, I want instantaneous access anywhere to whatever I need. I think we've got to clearly acknowledge, we need a fundamentally different network structure here.

You know, put it another way, with our current network structure, at times I feel like I'm -- I, we are fighting with one hand tied behind our back. I'm going this thing is inherently indefensible, and if we don't change its dynamic we're on the wrong end of the cost curve here and we're on the wrong end of the mission outcome curve. And that as a military guy, it drives me up the wall. My culture is get ahead of problem sets, see the problem, anticipate, get ahead of it, optimize yourself for success, see the environment you're dealing with and anticipate.

The current structure is really not optimized for us to do that. So you're seeing investments being made both within the department, within the government, but we're doing this in a framework in which overall budgets are declining, money is tight, and we're trying to ask ourselves as a nation so how much do we want to spend here. And that conversation is being held for each of us individually, it's a topic my wife and I talk about, what's the right level of security investment for us at home in terms of cyber, corporate entities, towns, I'm sure Aspen is thinking to itself, hey, I've got a lot of interesting information from the taxpayers in this community, what am I doing to ensure that the records, the information that our citizens are providing us whether it's a town, whether it's a state, whether it's the federal government, is being appropriately protected.

The other part I make to everybody is it took us decades to get where we are. We are not going to fix this problem in a year, and so oftentimes we have this incredibly short focus. Hey, let's do this six-month campaign. This is hard work that's going to take years to get where we need to be and just like we're seeing in the counterterrorism threat area with ISIL and others, this is not a problem set we're solving in years. Dedicated long-term multidimensional aspects of this problem and we've got to be dedicated in the long haul. And with that I just thank you all very, very much for your time.

(Applause)

MR. SANGER: Thank you very much. Thank you Admiral Rogers. Great conversation.

(Applause)

* * * * *