SCIUTTO: Thanks so much, everybody. Thank you, admiral, appreciate it.

ROGERS: Yeah, thank you.

SCIUTTO: It's a privilege, pleasure to have the time to grill you in front of so many people.

[LAUGHTER]

ROGERS: I am here to be grilled.

SCIUTTO: We have the -- the benefit today of -- of some news, which I know you love to talk about, story on the front page of The New York Times about Iran, and Iran finding out in advance about -- or just discovering a U.S. effort to continue to attack its system, and then responding with its own retaliation beginning in August of 2012, including these attacks on -- on U.S. banks.

First question I want to ask is how much of an alarm -- how much alarm to you that Iran was able to discover this?

ROGERS: Well, my first comment would be I honestly have not read what we're talking about.

SCIUTTO: OK.

ROGERS: So, I'm not in a good position.

SCIUTTO: Well, it's in NSA...

(CROSSTALK)

SCIUTTO: So it's an NSA document...

ROGERS: ... haven't read The New York Times today.

SCIUTTO: If -- if, well, let me summarize for you, because it's an NSA document. Assuming it's true, and you can also say it's a -- you have no knowledge of it, but a document saying -- and it was written by your predecessor, but saying that Iran discovered a program by the U.S. following the Stuxnet virus a couple years later to infiltrate its computer networks.
And that in part, in response to that U.S. effort, that Iran then carried out its own wave of retaliatory attacks, three waves of attacks beginning in August 2012, including attacks that targeted the U.S. banking system.

So, I suppose the first question then is, does that sound accurate to you?

ROGERS: Again, I -- I don't want to comment if I haven't seen the specifics. Now, in broad terms, though, if I could, if you want to have a -- a broader discussion about -- So, do the actions that nation-states takes in cyber lead to responses in others? I certainly understand that.

You know, I -- the United States, like many nations around the world, clearly, we have capabilities in cyber. The key for us to -- is ensure that they are employed in very lawful, very formulated, very regimented manner. I think you saw that in the president’s direction to us in terms of PPB-28, Presidential Police Directive 28, in which he laid out about a year ago. So, in the conduct of signals intelligence, here’s the specific framework that I want to make sure you use. These are the principles that I want you to be mindful of. And this is the legal kind of basis that we'll continue to use. So, that all remains applicable.

SCIUTTO: Well, let me approach it differently and in more general terms, because -- because the point that this story raises, and we'll separate ourselves just from the specifics of the story, is a danger that a number have mentioned, including yourself, the idea of making cyberattacks more costly in order to deter them.

The follow-on the danger is, if you're making those attacks more costly by carrying out your own attacks, are you starting a vicious cycle of -- of attack and retaliation? And do we see that with, for instance, a country such as Iran? And that, of course, goes back even further when we look at the Stuxnet virus.

ROGERS: Right. So, my comment would be escalation is not something that’s unique to the domain of cyber.

SCIUTTO: True.

ROGERS: So, just as we have developed frameworks over time to help us address the issue of escalation in the more kinetic, more traditional realm, I think cyber is in the same kind of arena.

SCIUTTO: Do you believe that you have addressed it sufficiently? And, for instance, this event -- are there others that give you concern that it leads us down a dangerous path, that everybody is looking for ways to deter? We’ve certainly seen the damage, and God knows not just Iran, countries such as China, that these attacks can cause. So, you do want to raise the cost, but you also see the danger of a follow-on sort of cycle.

ROGERS: Well...

SCIUTTO: Are you comfortable that we have a handle on how to deter America’s adversaries from cyberattacks without creating a further problem?

ROGERS: I think, clearly, the concepts of deterrence in the cyber domain are still relatively immature. We clearly are not, I think, where we need to be, where I think we want collectively to be.
This is still the early stages of cyber, in many ways. So, we’re going to have to work our way through this.

And it’s one of the reasons why, quite frankly, I’m interested in forums like this, because I’m interested in a broad set of perspectives, many of which are going to be different, you know, from what I bring to the table. But I’m interested, how do we collectively as a nation come to grips with some fundamental concepts, like deterrence in the cyber arena? How are we going to do this? Because you look at what you see is happening in the world around us, and the threats we’re facing in cyber continue to grow.

SCIUTTO: No question. Well, let’s look at the bigger threat. You have Iran, where -- where there’s clearly a history back and forth. You have Russia, source of frequent attacks on the U.S., both in the private sector and the government sector. And you have China. I spent a couple years in China dealing with this every day, where you have enormous costs to the business community, in -- in the billions, the tens of billions of dollars. Plus, as we know, they target government institutions and -- and apparently have had some success stealing secrets.

People talk about the coming cyberwar, but when I look at that, just as an observer and as a reporter, it looks to me like we’re already at war to some degree, a low-level war, but with these countries, these -- these are attacks with real consequences, real capabilities.

ROGERS: Clearly I would argue that history has shown us to date that you can name any crisis, you can name almost any confrontation we’ve seen over the last several years, and there’s a cyber dimension to it. Whether it’s what we saw in Georgia, whether what we saw in Ukraine, Iraq, the challenges associated with ISIL. This is not something isolated.

And I think our -- among our challenges as we move forward is, so, if cyber is going to be a fundamental component of the world we’re living in and the crises and the challenges we’re trying to deal with, so how are we going to work our way through that?

What we’re trying to argue is, over time, if we can get to the idea of norms of behavior, if we can develop concepts of deterrence that lead us to collectively to get a sense, first of all, just how far can you go, what’s aggressive, what’s not aggressive, what starts to trip response thresholds? You know, those are all questions of great interest, I would argue, for all us.

SCIUTTO: Well, sounds like you’re saying we’re not there, that we -- we haven’t even defined the concepts of deterrence. It sounds like you’re saying we’ve got a long way to go.

ROGERS: No, I think I used the word we’re not mature, and we’re clearly not where we need to be. You know, I don’t think there’s any doubt about that.

SCIUTTO: I want to ask you -- Leon Panetta used a phrase which I’m sure you’ve heard, he fears a cyber Pearl Harbor. What does a cyber Pearl Harbor look like?

ROGERS: The way I phrase it is my concern is an action directed against -- in my case, as a, you know, member of the United States military, an action directed against infrastructure within the United States that leads to significant impact, whether that’s economic, whether that’s in our ability to execute our day-to-day functions as a society, as a nation. You know, that’s what concerns me.
And you’ve seen some. You look at what happened with Sony. You look at what we’ve seen nation-states attempting to do against U.S. financial websites for some number of years now. You know, those are all things that, were they -- take that financial piece, were it successful, were our ability to actually, as private citizens, access our funds, if that were ever really contested, think about the implications for us as a nation, as individuals how we would try to deal with that.

SCIUTTO: Which states today are capable of carrying out such an attack like that?

ROGERS: Well, we’ve clearly previously talked about, you know, the big players in cyber, if you will, nations that we see active. It’s a matter of record. We have talked about our concerns with China and what they’re doing in cyber. Clearly, the Russians and others have capabilities. You know, we’re mindful of that. In general, you won’t see me going into a, well, here’s my assessment of every nation in the world around us.

SCIUTTO: No, I understand, but that’s two right there, China and Russia, already capable of carrying out such an attack. That’s concerning because we see them. Do -- do you find that they are in some of these smaller-scale attacks, I mean, there was even one that went into the White House computer system, not the sensitive system, but still. Do you find that they are on the one side kind of showing off their ability a little bit, and on the other side, testing, finding the weak points?

ROGERS: I think nation-states engage in actions in penetrating of systems in the cyber arena for a whole host of reasons among the two that you’ve identified, whether it be the theft of intellectual property. I think depending on the source you want to use, as a nation, we lose anywhere I’ve seen between $100 billion to something upwards of approaching $400 billion a year in the theft of intellectual properties.

Certainly, in the Department of Defense, it’s an issue of -- that’s been of great concern to us for some time as we watch nation-states penetrate some of our key defense contractors, steal the enabling technology, if you will, that gives us operational advantage as a military.

SCIUTTO: If I can, we’ve got a cyber audience here, and I -- and I want to go to the cyber audience and give everybody a fair amount of time. So, if I could touch on a couple other topics.

ROGERS: Sure.

SCIUTTO: Just out of -- outside of cyber, although related to. First on patriot -- Patriot Act with the (inaudible) of 215 on June 1st. I want to set aside just for a moment the privacy concerns, which, as you know, are -- are severe from some quarters, but...

ROGERS: And very -- I would comment, and very legitimate. Those are very legitimate concerns for us as a nation as we try to figure out, so how are we going to strike that competing requirement for security and acknowledging at the same time our rights as citizens is foundational to our very structure as a nation. It goes to who we are and what we are.

SCIUTTO: Do -- well, let me ask you since you -- since you brought that up. Do you think that the current, for instance, metadata collection, did that get that balance right?

ROGERS: I think that, number one, the metadata collection generates value for the nation. I honestly believe that, that it does generate value for the nation. Now, is it a silver bullet that in and of itself guarantees that there will never be another 9/11, or there won’t be a successful terrorist attack?
My comment would be no. If that’s the criteria you want to use, I would be the first to acknowledge it. It is not a silver bullet. It is one component of a broader strategy designed to help enhance our security.

At the same time, we also realize that in executing that phone record access, that we need to do it in a way that engenders a measure of confidence in our citizens, that it’s being done in a lawful basis with a specific framework, and that there are measures in sight, in place, to ensure that NSA or others aren’t abusing their access to that data. And that is fair and right for us as a nation.

SCIUTTO: Let me ask you a question, because I’d like you to -- to quantify the value that it has generated for the nation. Early on, when the program was revealed, and I was reporting this heavily at the time, the administration bandied about a figure, 50 plots thwarted. Then over time, that -- that figure was whittled down by -- by, among others, Senator Patrick Leahy, to a far smaller number, where -- where the metadata even down, he would argue, to zero where the metadata itself was necessary, where other programs could not have accomplished the same thing.

Can you identify a specific plot that without the bulk (ph) collection, we wouldn't have been able to have identified and stopped?

ROGERS: In a large, unclassified forum, I'm not going to do that.

(LAUGHTER)

SCIUTTO: Does one exist?

ROGERS: But I will say this, I -- I base my assessment on the fact that I truly do believe that it has generated value for us. Now, if you want to define value as, in and of itself, can you prove to me that without this, you wouldn’t have forestalled an attack, if you didn’t have this, you wouldn’t have been able to forestall an attack. The -- the criterion, I would argue, is if you use that, then it would argue things like, why do we maintain fingerprints as a government? If -- if you couldn't prove to me that collecting fingerprints in and of itself would forestall criminal activity, why would you do it?

SCIUTTO: But we don't fingerprint...

ROGERS: I would just argue that that's not the criteria to use in this case?

SCIUTTO: But don’t you think there’s a higher standard for this, because we don’t fingerprint everybody in this room. You fingerprint when you have a reason to fingerprint.

ROGERS: I think if...

SCIUTTO: In this case, the data’s collected regardless.

ROGERS: ... if you look, for example, at the amount of fingerprint information retained for under a very legal and valid...

SCIUTTO: Global entry.

(LAUGHTER)
Well, let -- let me ask you this, then, because the reason I started the question by saying set aside the privacy concerns for a moment, because it is others -- it's officials from inside the national security -- not industry, but -- but institutions of government, FBI and others, who are concerned that they will lose tools that they find extremely useful -- you know, the tangible -- ability to go after tangible things, hotel records, et cetera, in the battle to maintain phone metadata collection which they -- and speaking -- you know, quoting FBI officials rather than myself -- say -- see as less important.

ROGERS: To be honest, I've never heard that argument, nor is that a conversation that Jim Comey, the director of the FBI, have ever had, and we talk regularly...

SCIUTTO: OK, so you don't -- you don't...

ROGERS: ... on this and other issues.

SCIUTTO: You don't think that the -- the fight over metadata could hold up, particularly when we speak in the renewal or extension of 215, other, more useful tools in fighting terrorism?

ROGERS: Is it possible? Yes. My -- my comment would be the value of this effort and the legal framework to continue it is a conversation we need to have in and of itself.

So, what do we think? And does the program as currently, with the amendments that were directed by the president, or changes that Congress may elect, because, remember, this is all derived from a law passed by Congress, the Patriot Act, specifically section 215 of the act.

And should Congress decide as they look at -- because if no action is taken, the authority expires on the 31st of May, 2015. In which case, on the 1st of June, we would no longer be able to access this data in trying to generate insights and connections between activity overseas and potentially activity in the United States.

Let's remember, that's what drove this in the first place. In the aftermath of the 9/11 attack, if you read the 9/11 investigative report, one of the comments made in the report was, hey, look, you had, in at least one instance, phone connectivity between one of the plotters who was in the United States and back overseas. Hey, you guys should have had access to this. You should have connected the dots. You should have realized that there was an ongoing plot in the United States with a foreign connection.

That was the genesis of the idea of how can we create a legal framework that would enable us to make a connection between known activity overseas, tied to a nation-state group or set of individuals, how could we try to then take that overseas data and see if there's a connection in the United States? And how could we try to do it in a way that protects the broad rights of our citizens?

That was the whole idea behind it. So, I would urge us in the debate on this, and it's important that we have a debate, not to forget what led us to do it in the first place.

SCIUTTO: What are the prospects for renewal, extension, 215 specifically?

ROGERS: To be honest, this is where I'm glad to be a serving military officer.

SCIUTTO: You can differ.
ROGERS: I have no -- I have no idea. This is just beyond my expertise, and I realize it's a complicated issue. I understand that.

SCIUTTO: If you lose it, will that greatly -- hamper your ability, the NSA's ability, to -- to thwart terror attacks?

ROGERS: Do I think that if we lose it, it -- it makes our job harder? Yes. And on the other hand, we respond to the legal framework that is created for us.

We, at the National Security Agency, do not, do not create the legal framework we use. That is the role of the legislative branch and then our courts as the interpret the legality of those laws, that whatever framework is developed, we will ensure that it was executed within the appropriate legal framework. That's what I owe as the director of NSA.

SCIUTTO: Want to turn, if I can, to counterterror, another issue at the top of the agenda. A lot of talk -- when I speak to intelligence officials, they will acknowledge that terror groups have altered the way they communicate post-Snowden, and that's made a difference.

I just wonder if you could quantify or just described how much that's hurt your capability?

ROGERS: I would say that it has had a material impact in our ability to generate insights as to what counterterrorism -- what terrorist groups around the world are doing. I'd rather not get into the specifics, because I don't want there -- them to have any doubt in their minds we are aggressively out hunting and looking for them. And they should be concerned about that, and I want them to be concerned, quite frankly, because I'm concerned about the security of our nation. I'm concerned about the security of our allies and their citizens. So, anyone who thinks this has not had an impact, I would say, doesn't know what they're talking about.

SCIUTTO: Do you have new blind spots that you didn't have prior to the revelation?

ROGERS: Have I lost capability that we had prior to the revelations? Yes.

SCIUTTO: How much does that concern you?

ROGERS: It concerns me a lot.

SCIUTTO: Yeah.

ROGERS: Given the mission of the National Security Agency, you know, given our footprint around the world, I mean, us as a nation, you know, when I think about our ability to provide insights to help protect citizens, wherever they are, whether they be out there doing good things to try to help the world, whether they be tourists, whether they be serving in an embassy somewhere, whether they be wearing a uniform and they find themselves in the battlefield in Afghanistan or Iraq today, clearly, I'm very concerned, as well as our key allies and friends.
SCIUTTO: So, how do you respond to that? Do you -- do you develop new -- sounds like an obvious question, but -- but have you found yourself forced to develop new capabilities to make up for the lost capabilities?

ROGERS: Right. So, you know, to be successful, we have to be an adaptive learning organization. And as the profile of our targets change, we have to change with them.

SCIUTTO: I wonder if I could turn again, once again, because I do want to give time to the audience, but -- but this time back to intelligence reform, to some degree.

So, recommendations 24 and 25, we haven't talked about it -- this was big -- this was big news a year and a couple months ago, but it's sort of been, as you -- as often happens in Washington...

ROGERS: I hope you know I haven't memorized them.

(LAUGHTER)

SCIUTTO: No, that's right.

ROGERS: Both numbers (ph).

SCIUTTO: Neither have I, I just happen to remember -- I just happen to know they're 24 and 25, but one was splitting civilian -- splitting Cyber Command, military leadership, civilian, leader of the NSA. Of course, we have you.

ROGERS: Right.

SCIUTTO: Do you think that's a problem?

ROGERS: No, I would argue where U.S. Cyber Command, in particular -- so the specific point is, as many of you may be aware, I am both the commander of the United States Cyber Command, so an operational organization within the Department of Defense, as charged with defending the department's networks, as well as, if directed, defending critical infrastructure in the United States. That's my U.S. Cyber Command role.

In addition, I'm also the director of the National Security Agency. In that role, two primary missions. One is foreign intelligence, and the second is information assurance. And as -- given the cyber dynamics that we're seeing in the world around us today, that information assurance mission becoming a more and more critical importance.

So, discussion in the past, about a year ago now, a little bit longer, about, so should you separate these two jobs? Should you have an operational kind of individual running U.S. Cyber Command, and then have an intelligence kind of individual running NSA? And should you cab (ph) the two apart?

The decision was made at the time, which I fully supported, and when I was asked as -- you know, being interviewed for potentially to fulfill these jobs, my comment was, given where U.S. Cyber Command is in its maturity and its journey right now, it needs the capabilities of the National Security Agency to execute its mission to defend critical U.S. infrastructure and to defend the department's networks. That in combining both intelligence and operations in the same way we have seen in the
lessons of the wars of the last decade, that integrating these almost seamlessly generates better outcomes. That's the case here, in my mind.

SCIUTTO: And the president obviously...

ROGERS: Has come to that conclusion.

SCIUTTO: ... has come to that conclusion.

Do you think the pressure is off to some degree? I mean, you remember the pressure, and this is -- this is when your predecessor was still in the -- in the hotseat, but this was an enormous focus from inside and outside Washington. But people don't talk about it a lot, and we know we have this deadline coming up June 1st, but it's not the same tenor.

Do you feel that the pressure is off -- the worst fears and concerns have either been allayed or forgotten?

ROGERS: I wouldn't say forgotten. I think we've gotten to a place where people say, OK, so now we have seen this work under two different individuals. We seem to be comfortable that the construct is workable, that the construct is generating value, better outcomes, if you will. But if that were to change, we'd clearly have to re-look at it again.

SCIUTTO: Thank you very much. I'm still going to ask you questions, but I want to give folks -- folks a chance to answer as well -- to ask some questions, as well.

I know we have a microphone going around. I also know that we have questions coming in via social media. I'll wait for those. Why don't we start with the crowd since you guys have taken the trouble of coming here today? If I can -- well, just right -- right here in the center of the audience. And she's coming right behind you.

Thank you, by the way. That was great.

QUESTION: Yes, admiral, thank you for coming. We were talking about the Sony attack earlier, and we heard that the Justice Department is investigating it as criminal matter, and we've seen sanctions from the Treasury Department.

What exactly is your role in this? You -- not just identifying this, but do you see any action that you intend to take or have taken in response to this?

ROGERS: Well, I'm not getting into the specifics of what, as a member of the Department of -- Defense -- putting on my U.S. Cyber Command role, if you will, what we may or may not do. I think the president's comments about we're going to start with the economic piece, and then we will look at, over time, the potential of additional options, or different applications and capabilities. The -- the positive side, I think, is the immediate actions. Remember, the hack -- the destructive piece occurred in late November.

On the positive side, several months have passed now. We haven't seen a repeat of the behavior, which, I think, in part was part of the entire intention, to say, hey, look, this is unacceptable and that we don't want this to happen again. That seems to have had, at least in the near term, the desired effect. Although I will be the first to admit, as I had said coincidentally just a couple of weeks
before, I had been testifying in the House, I’d said, look, I think it’s only a matter of time before we see destructive offensive actions against critical U.S. infrastructure, that I fully expected, sadly in some ways, that in my time as the commander of the United States Cyber Command, the Department of Defense would be tasked with attempting to defend the nation against those kinds of attacks.

I didn’t realize that it would go against a motion picture company, to -- to be honest.

SCIUTTO: If I could just follow on -- on that. During this one phenomenon, in a way, with regard to North Korea, is that China has, to some degree, come around on being alarmed by some events inside the political structure there.

How much help did you get from China, if at all, knowing that internet is routed via North Korea’s internet is routing through China? Did they help out in any way?

ROGERS: I mean, we reached out to the our Chinese counterparts to say, hey, look, this is of concern to us, and it should be of concern to you, that in the long run, this kind of destruction -- destructive behavior directed against a private entity purely on the basis of freedom of expression is not in anyone’s best interests, that this is not good.

And so that, you know, they were willing to listen. We’ll see how this plays out over time. On the positive side, we were able to have a conversation, which we were grateful for.

SCIUTTO: Was the U.S. behind the retaliatory attack on North Korea?

(LAUGHTER)

ROGERS: Let’s make some headlines.

(LAUGHTER)

SCIUTTO: Not gonna go there.

ROGERS: Not gonna go there.

SCIUTTO: Did China offer any material help other than listening?

ROGERS: I’ll be honest, I didn’t work that specific aspect of the problem set. So, my knowledge of the specifics of the PRC’s response is just not high.

SCIUTTO: OK.

ROGERS: I apologize. It just wasn’t the area that I worked.

SCIUTTO: OK.

Go over here. Where’s the microphone? Oh, sorry. There’s one -- since the microphone’s there, we’ll go there, then we’ll try to get to the other side of the room.
QUESTION: Good morning. It’s David Sanger (ph) from The New York Times. Good to see you again.

ROGERS: David, how you doing today?

QUESTION: Good.

ROGERS: And I apologize I did not read The New York Times today.

(LAUGHTER)

QUESTION: You’re killing (ph) me (inaudible)

Only my mother reads me that early in the morning.

(LAUGHTER)

QUESTION: My question to you goes to the question of encryption, something that has come up here recently. You saw in the fall, when Apple turned out a new operating system for the iPhone 6, it basically put all the encryption keys into the hands of the users and said if they get a request, either a legal request from law enforcement or one from you, all they could really hand over from the phone itself would be gibberish.

You’d have to go break the code.

They’ve made it pretty clear in recent times, even when the president was out in California last week, that they plan to extend that encryption eventually up into the Cloud, and so forth. And we’ve heard the FBI director, James Comey, say that this is creating a -- a dark hole that is going to get in the way of their investigations.

We haven’t heard very much from the intelligence community on this, and I wonder if you would talk a little bit about this whole phenomenon of basically handing the keys to users, how it would affect your own abilities, whether or not the computing capability you’re building up now is designed to be able to try to break that, and what other solutions you might have?

ROGERS: So, broadly, I share Director Comey’s concern here. And I’m a little -- perplexed is the wrong word, but the most of the debate that I’ve seen has been it’s all or nothing. It’s either total encryption or no encryption at all.

And part of me goes, can’t we come up with a legal framework that enables us, within some formalized process, a process that I would argue neither NSA or the FBI would control, to address within a legal framework valid concerns about. If I have -- indications to believe that this phone, that this path, is being used for criminal, or in -- in my case foreign intelligence, national security issues, can’t there be a legal framework for how we access that?

Now, we do that in some ways already. If you look at, for example, we have come to the conclusion as a nation that the exploitation of children is both illegal and something that is not within the norms of our society. So, we’ve created both a legal framework that deals with things out there that would -- passage of photography and imagery that reflects the imagery of the exploitation of children. We’ve also told companies, for example, and you can screen content for that, that that’s
inacceptable -- unacceptable, excuse me, that it violates not just a law, but a norm for us as -- as a society.

So, from my perspective, we have shown in other areas that through both technology, a legal framework, and a social compact, that we have been able to take on tough issues. And I think we can do the same thing here, and I hope we can get past this well, it’s either all encryption or nothing, that we’ve got to find some -- what are the levers that we could create that would give us the opportunity to recognize both the very legitimate concerns of privacy, which I share as a citizen, as well as, I think, the very valid security concerns about, hey, look, if these are the paths that criminals, foreign actors, terrorists are going to use to communicate, how do we access this?

We’ve got to work our way through that.

QUESTION: I walked around to the other side of the room so I get the microphone this time. Thank you.

There have been reports from cybersecurity analysts and from the Snowden documents that the United States is engaged in spyware for purposes of surveillance.

How significant is spyware to the NSA’s surveillance capabilities?

ROGERS: Well, clearly, I’m not going to get into the specifics of allegations. But the point I would make is we fully comply with the law. PPD28 provides a very specific framework for us about what is acceptable and what is not acceptable, and what are the guiding principles that we have to keep in mind when we’re conducting our foreign intelligence mission.

And we do that foreign intelligence mission operating within that framework. That’s the commitment that, you know, I make as the director. Hey, we got a legal framework, and we will follow it and we will not deviate from it.

QUESTION: Sorry. Oh.

QUESTION: Hey.

QUESTION: He’s taking the microphone.

QUESTION: Bruce Schneider (ph). We haven’t met. Hi.

Wait, it’s -- the answer, yes, very significant. And to the other -- your other question -- it’s not the legal framework that’s hard, it’s the technical framework. That’s what makes that problem hard. That’s why we’re stuck with all or nothing.

My question is also about encryption. It’s a perception and a reality question. We’re now living in a world where everybody attacks everybody else’s systems. We attack -- we attack systems. China attacks systems. And I’m having trouble with companies not wanting to use U.S. encryption because of the fear that NSA, FBI, different types of legal -- legal and surreptitious access is -- is making us less likely to use those products.

What can we do, what can the intelligence community do, to convince people that U.S. products are secure, that you’re not stealing every single key that you can?
ROGERS: Right, right.

So, first of all, we don't. Number two, my point would be that's the benefit to me of that legal framework approach, that, hey, look, we have specific measures of control that are put in place to forestall that ability, because I think it's a very valid concern to say, hey, look, are we losing U.S. market segment here? You know, what's the economic impact of this?

I -- I certainly acknowledge that that's a valid concern. I just think between the combination of technology, legality, and policy we can get to a better place than we are now, realizing that we are not in a great place right now.

SCIUTTO: You know, on that point, it's not just encryption, but -- but you speak to high tech executives, they talk about tens of billions of dollars in business loss, whether you're talking in social media, cloud computing, et cetera.

Should that not be part of the cost-benefit analysis of something like phone metadata collection, et cetera? And now, that's not -- frankly, it's not really a question for you, it's a policy question, but I'm going to ask it to you anyway. Sounds like you're acknowledging that that broader impact, those broader costs, have to be part of the decision.

ROGERS: I mean -- I certainly think we need to acknowledge that there is an impact here, but I would also say, look, let's not kid ourselves. There are entities out here taking advantage of all this to make a better business case for themselves. There are entities out there using this to create jobs and economic advantage for them. Let's not forget that dimension in all this, even as we acknowledge that it is a dimension to this problem set.

SCIUTTO: Just to move the microphone around, maybe -- do we have a question from someone from the media?

ROGERS: Somebody in the back.

SCIUTTO: Do we have a social media question at all, or do you want to wait?

(UNKNOWN): (OFF-MIKE)

SCIUTTO: Fine. We'll wait for a little bit. Let's move the mike to...

(UNKNOWN): (OFF-MIKE)

SCIUTTO: OK.

ROGERS: Stretch. Stretch.

QUESTION: Thanks. Patrick Tucker (ph) with Defense One.

A couple of reports come out in recent weeks about ISIS using the dark web to raise money through Bitcoin, the dark web basically a bunch of anonymous computers, a bunch of anonymous users that are still able to find each other.
Can you speak a little bit to that problem in terms of intelligence collection of the dark web? What does it mean to you, and -- and how are you going about finding a solution to some of these -- these really big problems of how to find people using that, that don’t want to be found, but are effectively using it for fund-raising, in particular ISIS?

ROGERS: Well, clearly, I’m not going to get into specifics, but let me just say this. We spend a lot of time looking for people who don’t want to be found. That is the nature in some ways of our business, particularly when we’re talking about terrorists or we’re talking about individuals engaged in espionage or other activity against our nation, or that of our allies and friends.

In terms of what are we trying to do broadly -- I mean, first, I -- I would acknowledge, clearly, it’s a concern. ISIL’s ability to generate resources, to generate funding, is something that we’re paying attention to. It’s something of concern to us, because it talks about their ability to sustain themselves over time. It talks about their ability to empower the activity that we’re watching on the ground in Iraq, in Syria, Libya, other places. So, it’s something that we’re paying attention to.

It’s something that we’re also doing more broadly than just the United States. This is clearly an issue of concern to a host of nations out there. I won’t get into the specifics of exactly what we’re doing, other than to say this is an area that we are focusing attention on.

SCIUTTO: As -- as we move -- move across here, just to follow on the question regarding ISIS, because when we speak to counterterror officials, they talk about ISIS supporters here in the U.S., and you know, different level of the problem than you have in Europe, for instance, and certainly in the Middle East.

Since the web is the principal form of radicalization for -- for a lot of these, particularly lone wolves, right, or folks who don’t travel, it must be pretty easy to track, is it not? If -- if it’s happening on the web, et cetera, can you identify pretty quickly and easily someone who is going down that path?

ROGERS: I mean, it -- it’s not quick and easy. And remember, as national security agents, we are a foreign intelligence organization, a foreign intelligence organization, not a domestic U.S. law enforcement or surveillance organization.

So, when it comes to the home-grown kind of in the U.S., that’s really not our focus. Our focus is on the foreign intelligence side, attempting to find the connections overseas, and then, quite frankly, partnering with FBI and others to say, OK, so if we generated insight about activity we’re seeing overseas, hey, how does this tie into activity that we may or not be able to detect in the United States? And that’s why partnerships are so important to us, because we are a foreign intelligence organization.

SCIUTTO: Actually (inaudible) I mean, it’s one of those folks here make contact with folks over there.

ROGERS: Right, right.

SCIUTTO: That’s what I’m saying. Is that -- I imagine that’s not as easy as it sounds, but it must be trackable.
ROGERS: It's not easy, but it's something that we pay attention to. It’s something we track. It’s where we partner closely with the FBI, as we say, OK, so we’ve seen this. There may be a U.S. connection here. Hey, this now becomes a law enforcement issue...

SCIUTTO: Right.

ROGERS: ... (inaudible) foreign intelligence issue.

SCIUTTO: Right. Understood.

Take right here.

QUESTION: Hi. Ethan Chau (ph).

ROGERS: Hey, Ethan (ph).

SCIUTTO: Hi.

As director of NSA and United States Cyber Command, do you think we’re positioned effectively to address the new cyberspace as a new domain of war fighting? And how does that differ from land, air, and sea? And do you think we need improvements, and in what aspects?

ROGERS: So, do I -- do I think we’re where we ought to be? No. No. Part of that is just my culture. My culture as a military guy always is about you are striving for the best, you are striving to achieve objectives. You push yourself.

I would say we’re in a better position in many ways than the majority of our counterparts around the world. We’ve put a lot of thought into this as a department. U.S. Cyber Command, for example, will celebrate our fifth anniversary this year. So, this is a topic that the department has been thinking about for some time.

In terms of, well, what makes it challenging, what makes it difficult, is -- let’s look at this from a defensive standpoint. And one of the points I like to make is, so, we’re trying to defend an infrastructure that has been built over decades, literally, and most of which was created at a time when there really was no cyberthreat, that we’re trying to defend infrastructure in which redundancy, resiliency, and defensibility were never design characteristics.

It was all about build me a network that connects me in the most efficient and effective way with a host of people and let’s me do my job. So, you didn’t worry about, well, were people going to attempt to -- when we designed most of these, concerns about people’s ability to penetrate those networks, to manipulate data, to steal data, really wasn’t a primary factor.

So, there’s also a component in the department as we’re looking to change our network structure to something that those were really core design characteristics. So, that’s a challenge.

And then, clearly, we’re trying to work our way on the offensive side through -- so, and it kind of goes to one of the questions, Jim, that you had previously asked. How do we do this within a broader structure that jives with the law of armed conflict, because, remember, when you’re looking at the application of cyber as an offensive tool, it must fit within a broader legal framework. That legal framework, the law of armed conflict, international law, the norms that we have come to take for
granted in some ways in the application of kinetic force, dropping bombs. We’ve got to do the same thing in the offensive world, and we’re clearly not there yet.

SCIUTTO: Where’s the mike? This gentleman’s been patient over here.

QUESTION: Admiral, my name’s Hugh McElref (ph).

ROGERS: Hi, Hugh (ph).

QUESTION: I’m a retired Navy cryptologic officer, among other things.

ROGERS: A fine man. You’re a fine man.

QUESTION: And I was remarking with another colleague, who may still be here, that we were having the same discussions 20 years ago. Now, there -- there has been progress. There’s Cyber Command. There’s the NSD at FBI. But why is it taking us so long to grapple with this compared to, say, the advent of nuclear weapons, and we have the National Security Act of 1947?

ROGERS: Well, my first comment would be, and a guy who was a cryptologist a few -- 20 years ago, I sure don’t remember having those conversations. In terms of -- can you say the -- the last part about it again? You were talking about duration, why has it taken so long, right?

QUESTION: Right. Look, I do not want to minimize the -- the progress, and -- and your position I view as progress, but it is taking us a long time. If it’s not 20 years, then it’s 15, and that compared to a much more compressed time scale for other cataclysmic changes in national security in the middle of the last century.

ROGERS: Well, I -- take for example, the nuclear example that you used. You know, we take for granted today the nuclear peace as something with very established norms of behavior, well-established principles of deterrence. My comment was you know how long it took to -- we take it for granted now, because we look at over almost 70 years since the actual development of the capability.

We take it for granted now, but if you go back in the first 10, 20 years, we were still debating about well, what are the fundamental concepts of deterrence, this whole idea of mutually assured destruction, that didn’t develop in the first five years, for example. All of that has taken time.

Cyber is no different. I think among the things that complicate this is the fact that cyber really is unsettling in terms of the way we often look at problems. So if you look at the military, we often will use geography to define problems. It’s we have a Central Command. It’s why we have a European Command. It’s why we have a Southern Command, for example.

Cyber doesn’t recognize geography. If you look at the typology of that attack from North Korea against Sony Picture Entertainment, it literally bounced all over the world before it got to California, infrastructure located in -- on multiple continents in multiple different geographic regions.

Cyber also doesn’t -- doesn’t really recognize this clear delineation that we as a nation have generally created over time about what’s a function of the private sector, what’s a function of the government and how does this whole national security piece. Cyber tends to blur that because the reality is, for example, if I go to work and I’m using at work literally the exact same software, the same
devices I’m using at home on my personal systems, it just has blurred the lines, so that makes it very, very complicated.

But I -- I share your frustration in the sense that it’s not as fast as I wish it were. But it isn’t from a lack of effort and it’s not from a lack of recognition, if that makes sense.

I think you -- oh, look at --

SCIUTTO: Oh, you got one. Fantastic. Let’s go --

QUESTION: (OFF-MIKE)

SCIUTTO: Then we’ll go cyber.

QUESTION: Thank you, Admiral, for coming. My name is Alex Stamos. I’m the CISO at Yahoo.

ROGERS: Hey, Alex.

QUESTION: So it sounds like you agree with Director Comey that we should be building defects into the encryption in our products so that the U.S. government can -- can decrypt --

ROGERS: So that would be your characterization, not mine.

(LAUGHTER)

QUESTION: Well, I think -- I think -- I think Bruce Schneider and Ed Felton (ph), and all of the best public cryptographers in the world would agree that the -- you can’t really build back doors into crypto, that it’s like drilling a hole in a windshield.

ROGERS: I’ve got a lot of world-class cryptographers at the National Security Agency.

(LAUGHTER)

QUESTION: And I’ve talked to some of those folks, and I think some of them agree, too. But --

ROGERS: So, we agree that we don’t accept each other’s premise, so you tell me what --

(CROSSTALK)

(LAUGHTER)

QUESTION: So, OK, there we go. We’ll agree to disagree on that.

So if -- if we’re going to build defects/back doors or golden master keys for the U.S. government, do you believe we should do so -- we have about 1.3 billion users around the world -- should we do so for the Chinese government, the Russian government, the Saudi Arabian government, the Israeli government, the French government? Which of those countries should we give back doors to?
ROGERS: So, I'm not going to -- I mean, the way you frame the question isn't designed to illicit a response.

QUESTION: Well, I mean, do -- do you believe we should build back doors for other countries?

ROGERS: My position is, hey, look, I think, number one, that this is technically feasible. Now, it needs to be done within a framework. I'm the first to acknowledge that. You don't want the FBI and you don't want the NSA unilaterally deciding so what are we going to access and what are we not going to access? That shouldn't be for us.

I just believe that this is achievable, and we'll have to work our way through it. And I am the first to acknowledge there's international implications to this. I think we can work our way through this.

QUESTION: So, you -- you do believe that, then, we should build those for other countries if they pass laws --

ROGERS: I said I think we can --

QUESTION: You can work through it.

ROGERS: -- work our way through this.

QUESTION: So, I'm sure the Chinese and Russians are going to have the same opinion, sir.

ROGERS: No, I said I think we can work our way through this.

QUESTION: OK. Nice to meet you. Thanks.

(LAUGHTER)

ROGERS: Thank you for asking the question. I mean, there's going to be some areas where, you know, we're going to have different perspectives. That doesn't bother me at all.

One of the reasons why, quite frankly, I believe in doing things like this -- and when I do that, I say, look, there are no restrictions on questions. You can ask me anything because we have got to be willing as a nation to have a dialogue.

This simplistic characterization of one side is good and one side is bad is a terrible place for us to be as a nation. We have got to come to grips with some really hard fundamental questions. I'm watching risk and threat do this, while trust has done that. No matter what your view on the issue is, or issues, my only comment would be that's a terrible place for us to be as a country. We've got to figure out how we're going to change that.

SCIUTTO: For the less technologically knowledgeable, which would describe only me in this room today, just so we're clear, you're saying it's your position that in encryption programs there should be a back door to allow, within a legal framework, presumably -- approved by whether it be Congress or some civilian body, the ability to go in a back door?
ROGERS: So back door is not the context I would use because when I -- when I hear the phrase back-door I think, well, this kind of shady. Why wouldn't you want to go in the front door and be very public? Well again, my view is look, we can create a legal framework for how we do this. It isn't something that we have to hide per se. You don't want us unilaterally making that decision. Again, I'm the first to acknowledge that, but I think we can do this.

SCIUTTO: But you want that -- that ability. You want that capability. I do want to get to the back, but do -- do we have a social --

ROGERS: We've got a social.

SCIUTTO: -- media question?

QUESTION: We have a collection.

SCIUTTO: Fantastic. Why don't we do -- we have 13 minutes to go. Why don't we do a couple, and I do -- I see you in the back, so we're going to get there as well.

QUESTION: Well, first I would just note that according to the internet and some of our high profile Twitter users in here, we are now trending. So #newamcyber is actually trending. So you should continue to tweet throughout the conference.

SCIUTTO: Where -- where are we in relation to "Birdman?"

[LAUGHTER]

QUESTION: OK, so here is a selection. Based on the previous comment about back doors for Russia and China, Christopher Kesogoian (ph) -- Keesogoian (ph) -- by the way, I may pronounce half of these things incorrectly The question is, are foreign governments spying on cell phones in Washington, D.C.? Are our phones secure? And if so, what could be done?

ROGERS: Did you say -- I apologize I didn't hear the beginning.

QUESTION: Oh, OK.

SCIUTTO: Are foreign governments --

QUESTION: Are foreign governments spying on our cell phones in Washington, D.C.? Are our phones secure, or what should be done?

ROGERS: Do I think there are nation-states around the world that are attempting to generate insights as to what we are doing as individuals? I think the answer to that is yes. The second question was do I think --

QUESTION: What do you think we should do about it?

ROGERS: Oh. Well, I -- one thing we always do in the department, I remind people is, don't assume that -- you know, there's a reason why we have unclassified system in the Department of Defense, the reason we have classified systems and unclassified systems. And so for DOD users, I
always remind them, hey look, we’re potential targets, so make sure you’re using your cell phone, for example, in an appropriate way, just as I make sure that I use mine.

I mean, otherwise -- you know, it’s where the standards of encryption that we talked about -- again, I’m not arguing that encryption is a bad thing, nor will you hear me say that security is a bad thing. Hey, I’m a U.S. person, I’m a U.S. citizen. I use a cell phone, I use a laptop, I want those systems to be every bit as secure for myself and my children as you do. I’m just trying to figure out, so, how do we create a construct that lets us work between these two very important viewpoints.

QUESTION: OK. So that question, I’m sure, came partially out of the concept of encryption of commercial cell phones. So on that point, from Russell Thomas, or MrMeritology, what can be done institutionally to make collaboration between the private sector and the government marginally better on cybersecurity?

ROGERS: I mean, I think clearly, I would second the thought. I mean, I think clearly, this is an area of significant improvement. I think on the government side, we’ve got to simplify things. One thing I constantly tell my counterparts is look, let’s be honest. If you were on the outside looking in at the U.S. government in the area of cybersecurity, we can be very complex. We have got to simplify this.

We have got to make this easy for our citizens, for the private sector and for us to interact with each other to ultimately get ourselves to a position where we can share information real-time in an automated machine-to-machine way because given the speed and complexity of the challenges we’re talking about in cyber, that’s where we’ve got to get, and we’ve got to work our way through how are we going to do that.

In the U.S. government, Homeland Security, the Department of Homeland Security, clearly plays a central role here. As both the director of NSA and the commander of U.S. Cyber Command, our capabilities support them and other U.S. government partners in our attempts to do that.

SCIUTTO: On that topic, as a journalist, I’ve asked the NSA whether my cell phone communications have been monitored in any way. As I submitted through proper channels, I got a response. We appealed, and we got a stock response, which others have gotten.

I’m a journalist. I lived overseas for a long time. As part of my work, I spoke to people who I would imagine you might want to listen to, some in the terror community, et cetera. Why as an American and a law-abiding American, why won’t the NSA tell me if they’ve looked at my phone communications?

ROGERS: Well, first, if you’re asking me directly, I don’t know the specifics for you, but I would

SCIUTTO: But it’s a policy because they’ve told others the same thing.

ROGERS: So what I would say is look, it is a matter of law. To do focused collection against a U.S. person, I must get a court order. I have to show a valid basis for why we are doing that. Is there a connection with a foreign nation -- i.e., that U.S. person is acting as an agent of a foreign government? And yes, that does happen out there. Is that U.S. person part of a group -- in this case, let’s say ISIL as an example -- who is attempting to do harm. Now, I have to show a court a legal basis for the why, and it can’t just be, well, we don’t like journalists. What?
SCIUTTO: Well, I wouldn’t say like --

ROGERS: That’s not a valid legal reason.

SCIUTTO: So if it were to happen, you would’ve had to have a court order, but that’s something you wouldn’t tell the person who was involved.

ROGERS: No.

SCIUTTO: OK. All right.

QUESTION: OK, I have one more topical question --

SCIUTTO: One more, then we’ll go to the back.

QUESTION: -- if that’s possible. So from John Leprise (ph), the question is, based on last week’s announcement or research that Kaspersky has announced that there were -- there was news of firmware hacking, has the firmware of core network routers or repeaters been similarly hacked? And if so, would this compromise the architecture of the Internet? Technical question.

ROGERS: Check. My quick answer would be no. But in terms of -- I go to the first part. You know, I’m aware of the allegations that are out there. I’m not going to comment about them. But in terms of, based on what I’ve read, does that lead me to believe that the Internet has somehow been compromised? No.

QUESTION: Thank you very much.

SCIUTTO: Back of the room on the left.

QUESTION: I’m Mike Nelson. I’m a professor of Internet Studies at Georgetown, and I’m just recently started working for CloudFlare, which protects about a million Websites around the world from DDoS attacks, provides SSL encryption.

I was at the cyber summit the White House did a week-and-a-half ago, and one of the topics that you kept hearing in the hallways was about how American companies are very uncomfortable sharing information with the U.S. government if they can’t share that same information with dozens of other governments.

I’d be curious to know how we’re supposed to decide which governments are OK to share with and how we deal with the fact that the Belgians and the French and the Turks and everyone else wants to know what we’re sharing with you. And our customers want to know that, too.

ROGERS: Right. So again, it’s another reason why I think that legal framework becomes very important here. Now, I’ll be honest, now you’re getting into the specifics of an area that isn’t, you know, my personal focus. I certainly understand the concerns, don’t get me wrong. But my comment would be that idea is not unique to cyber, for example. You name the business segment, and just because we share something internally within the United States doesn’t mean we do so automatically everywhere in the globe. So I would argue cyber’s not exactly unique in this regard, nor is the challenge that it presents -- and it is a challenge; I acknowledge that -- to the private sector unique to cyber.
SCIUTTO: We have time for a couple more. Maybe way in the back here, too. This is another area where we haven't --

ROGERS: Yeah, let's get someone in the back.

SCIUTTO: -- to be geographically fair.

QUESTION: Listening to the conversation today, one thing that's fairly clear -- and you mentioned it -- we need to decide what the social norms are around which we build the policy and legal frameworks. But clearly, listening to Bruce Schneider and Alex Stamos and you, the social norms aren't worked out yet. So what's the process by which we get the dialogue going so we can figure out what those norms are, which has to precede figuring out what the policy and legal frameworks are?

ROGERS: So I think interactions like this are part of it. I think the interaction with our elected representatives. Hey look, they are the ones who create the legal framework that we use. So I encourage all of you, all of us as citizens to articulate our viewpoint, to help them understand the complexity of this issue and to help them understand just what our viewpoints are as we're trying to work our way through this.

The other thing that I -- at least for me, I'm trying to do outreach as well in the academic world because one of the things that I'm struck by is -- and it goes back to your question earlier, sir, talking about the nuclear piece. If you go back and look at some of the foundational work that was done on nuclear deterrence theory, for example, much of that back in the '40s and the 50s was done in the academic arena. You read much of the initial writings -- you know, Kissinger at Harvard, others -- there was a strong academic focus on so how are we going to understand this new thing we call the atom bomb or the hydrogen bomb?

And so I'm trying to see is there a place in the academic world for the same kind of discussion, hey, how do we get to this whole idea of the social norms and what are we comparable with?

SCIUTTO: One more just -- the way back here as well.

ROGERS: All the way in the back. You were so close.

QUESTION: Thank you. Leandra Bernstein, Sputnik International News. A question about --

ROGERS: I'm sorry. Leann -- was it Leann, did you say?

QUESTION: Leandra.


QUESTION: Oh. I'm with --

ROGERS: I didn't hear where you were from.

SCIUTTO: Sputnik International News.

QUESTION: Russian press.

ROGERS: OK.

QUESTION: So you've addressed the Kaspersky report, said you wouldn't comment. There was another report on the NSA/GCHQ hacking encryption keys in a sim card provider. Can you respond to that? I mean, you've said that we need to have a discussion, a public discussion, so how would you get that started by addressing these allegations?

ROGERS: So the first comment would be I've listened to these allegations for some period of time. This isn't something unique, per se. And again, my challenge as an intelligence leader is even as we try to have this dialogue, which I acknowledge we need, how do I try to strike the right balance between engaging in that broad dialogue and realizing that compromising the specifics of what we do and how we do it provides insight to those that we're trying to generate knowledge of, who would do harm for us as a nation.

And so as a general matter of policy, I have just said hey look, I'm not in public unclassified forums getting into the specifics of the what does -- in terms of the very specific things like you've referenced. I am not going to chase every allegation out there. I just -- I don't have the time. We need to focus on doing our mission but making sure we do it within that legal and authority and policy framework.

QUESTION: But just --

ROGERS: That's the promise that I make to all of you. That is what we do.

QUESTION: When private companies make these allegations against you, what's -- can you address that impact generally?

ROGERS: I'm not going to get into the specifics.

SCIUTTO: We've got time for one more. Since this is a cyber conference and we're trending, do we have another one on the Web?

QUESTION: You know what? I think (OFF-MIKE)

SCIUTTO: OK. All right. Fair enough.

ROGERS: You're ruthlessly efficient.

SCIUTTO: You are ruthlessly efficient. I think it's going to take us out of trending.

Here. How about right here in the front, probably be our last one.

QUESTION: Thank you. Joe Marks from Politico. I'm not going to ask you about encryption, wanted to ask about standing up CYBERCOM. You said earlier that you think that at this point, CYBERCOM and NSA still need to be dual-hatted. A lot of people in the services have said that a lot of the process of building up CYBERCOM has been sort of shifting people who already are working in this
field over to the cyber mission forces. Are you concerned that you aren't bringing enough new people, new cyber experts into the military and that you're taking away some native capability that ought to be in the services?

ROGERS: The short answer is no. And I say that -- remember, in the job before this, I was also -- in my previous job before these two, I was the Navy guy. So I was the service guy responsible for developing the Navy’s cyber force. So I’ve lived in that service world about how you man, train, equip, how you create a force, and now I find myself as the joint commander with overall responsibility across the department.

If I go back to when I started in cyber in the department about 10 years ago, boy, our ability to recruit, retain and train and educate a cyber workforce over time, I was really concerned about would this fit within the traditional DOD model about how we develop people, how we promote them, how we retain them over time.

Fast-forward a decade later, and I have been -- knock on wood -- pleasantly surprised by our ability to do that. And so for right now, my quick answer would be no, I’m comfortable that we’ve been able to gain access to the people that we need, that in so doing, I haven’t had to strip massive amounts of capability from other very valid, you know, similar requirements within the department. We’ll have to watch this closely over time, though, to see if that changes. There’s no doubt about that.

SCIUTTO: Since time’s up, final thoughts?

ROGERS: None other than I thank you for your willingness to engage in a discourse, and I think it’s a positive for us. Look, clearly, these are important issues to us, and yet we’re able to do this today without yelling and screaming at each other or pointing at each other and making acquisition -- accusations against each other.

We have got, as a nation, to come to grips with what’s the balance here, and there’s going to be a lot of different perspectives out there. I understand that. I’m constantly reminding our force, our workforce, be grateful that you live in a nation that’s willing to have this kind of dialogue. That’s a good thing for us.

And are there tensions along the way? Yeah. It’s not unique to cyber, and it’s not the first time in the history of our nation we’ve had challenges like this, and it won’t be the last. But if we really are willing to sit down and have a conversation, we can move where we need to be.

And with that, I thank you very much for your time.

SCIUTTO: Admiral Rogers. Thanks very much.

ROGERS: Thanks, Jim.

SCIUTTO: Really enjoyed it.

[APPLAUSE]

END