NOVEMBER 20, 2014

CYBERSECURITY THREATS: THE WAY FORWARD

U.S. HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

ONE HUNDRED AND THIRTEENTH CONGRESS

HEARING CONTENTS:

OPENING STATEMENTS

Rep. Mike Rogers (R-MI) [view pdf]
Chairman of the Permanent Select Committee on Intelligence

Rep. Dutch Ruppersberger (D-MD) [view pdf]
Ranking Member of the Permanent Select Committee on Intelligence

WITNESSES

Admiral Michael Rogers, USN [view pdf]
Director, National Security Agency U.S. Cyber Command

AVAILABLE WEBCAST

Hearing Video
http://www.ustream.tv/channel/hclive17

COMPILED FROM:

https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

National Security Agency

Hearing of the House (Select) Intelligence Committee

Subject: "Cybersecurity Threats: The Way Forward"

Chaired By: Representative Mike Rogers (R-MI)

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

Location: 2212 Rayburn House Office Building, Washington, D.C.

Time: 9:00 am EST
Date: Thursday, November 20th, 2014

Transcript by
Federal News Service
Washington, D.C.

REPRESENTATIVE MIKE ROGERS (R-MI): I call the committee to order.

We've got competing hearings with some of our members. There'll be members coming in and out during the course of the meeting.

Admiral, we appreciate you being here today.

The House Intelligence Committee meets today in open session to convene a hearing on the advanced cyberthreats facing the United States, as well as ongoing efforts to protect our nation and our economy from these dangerous threats.

Our witness for today's hearing is Admiral Mike Rogers, the commander of the U.S. Cyber Command and director of the National Security Agency. And as we have said multiple times, we're - you can't have enough Mike Rogers in the national security space, I think.

Admiral Rogers, we appreciate you appearing before us today.

As the Congress comes to a close, I wanted to take this opportunity to talk with the American people one more time about one of the most significant national threats that we face. I was a member of the HPSCI for several years before I became chairman, and I had the opportunity to see those cyberthreats grow in volume and complexity over that time.

As I took the gavel as committee chairman in 2011, I was determined to do what I could do to help American companies deal with these threats. And Dutch Ruppersberger and I sat down to try to, I think, craft a measure that dealt at least with a significant portion of that problem in a cybersharing bill.

I started talking publicly in as great a detail as possible about the countries like China and Iran that were preying on American companies. I wanted to raise awareness among companies being targeted, and also advance the debate about what the United States government needs to do to address these threats.

The highlight of that effort for me was the committee's October 2011 open hearing on cyber where both the ranking member and I called out the Chinese government for its industrial-scale campaign of cybereconomic espionage against American companies.

The brazen Chinese government campaign was no secret in the United States government or the private-sector cybersecurity community. But no one was talking about it publicly at that time. The United States was unwilling to call Beijing to account, and U.S. companies feared the Chinese government would punish them with crushing cyberattacks for having that public debate.

After we opened that debate here and called China out, we were able to have an honest conversation with the American people about the cost of this Chinese campaign and what needs to be done about it.

China's economic cyberespionage has certainly not diminished in that time. In fact, it's grown exponentially in terms of volume and damage done to our nation's economic future. Chinese intelligence services that conduct these attacks have little fear, because we have no practical deterrence to that threft (sic) - that theft.

This problem is not going away until that changes. China's economic cyberespionage is not the only threat we face now. Iran launched very challenging distributed denial-of-service attacks on our financial networks in 2012. With the DDOS tactic -- isn't -- it's not a new, and it's certainly not the most sophisticated of attacks. The scale and speed of which this happened was unprecedented and made the attacks very difficult to defend against. A sophisticated virus widely attributed in the press to the Iranian government also wiped out more than 30,000 computers at a Saudi Arabian state oil company, Aramco.

There has been a lot of talk over the years about hypothetical dangers of a cyber Pearl Harbor, and it's certainly become a bit of a cliché in cybersecurity circles. I would argue, however, that the threat of a catastrophic and damaging cyberattack in the United States critical infrastructure like our power or financial networks is actually becoming less hypothetical every day.

The Iranian attack on Saudi Aramco is a clear example that our adversaries have the intent and capability to launch damaging attacks. Moreover, there are growing reports of attempts to breach the networks and industrial control systems of our electric power operators and critical infrastructure operations.

Foreign cyberactors are probing Americans' critical infrastructure networks and in some cases have gained access to those control systems. Trojan horse malware that has been attributed to Russia has been detected on industrial control software for a wider range of American critical infrastructure systems throughout the country. This malware can be used to shut down vital infrastructure like oil and gas pipelines, power transmission grids and water distribution and filtration systems.

Not aware of a case yet where hackers gained access to one of these systems and used it to cause damage to American critical infrastructure, but I wouldn't take much comfort in that.

I believe our advanced nation state adversaries have the ability to cause such damage. These nations lack a strong motive at this moment to conduct such an attack and are deterred only by the fear of U.S. retaliation. Our critical infrastructure networks are extremely vulnerable to such a damaging attack, and we can't count on a deterrence if we're already in an adversarial position with a nation like China or Russia. And we can't count on the fact that less rational actors might also gain access to those critical systems.

It's not hard to understand how difficult it would be if the power or the water was shut off, but imagine if one of our adversaries was able to shut down key American financial transactions. Economy would grind to a halt. Even worse, imagine if a foreign cyberattacker altered or deleted key financial transaction data so that we couldn't verify account balances or what companies owe each other from day to day. It certainly would be chaos.

Most of our critical infrastructure providers are doing their best to better secure their networks. But if they get attacked by an adversary with the resources and capabilities of a nation state like China or Russia or Iran, it certainly isn't a fair fight.

The U.S. government has an obligation to help the private sector by sharing this threat information about potential attacks before they happen. Glad we had the opportunity to talk to the American people today about this vital issue. I'm hoping that this hearing can help focus members' attention on this issue and the need to pass cyberthreat information-sharing legislation before the end of 2014. We must be ready for a damaging cyberattack against our critical infrastructure. If the Senate does not act swiftly, both houses of Congress will have to start from scratch next year, moving new bills. Given the cyberthreats we face, this could be an unnecessary and dangerous delay when we are so close to an agreement that protects privacy and our economy and our national security.

Again, Admiral, thank you for being here. And I want to now turn it over to the ranking member for any remarks he'd like to make.

REPRESENTATIVE C.A. "DUTCH" RUPPERSBERGER (D-MD): Well, first, Mr. Chairman, thank you for having this open hearing. It's important that we let the American people know how serious this cyberthreat is.

I thank you, Admiral Rogers, for appearing before us today. You have a tremendous job. You're ready for the job. I know that you've been in, what, six months now and -- about seven months, and we're ready to work with you to make sure you get the resources you need to protect our country from the threats that we're talking about.

This committee has been sounding the alarm on the cyberthreat for years and has twice led the House passage of critical cyber legislation. But the threat has not waited on the full Congress to act.

In 2012 we warned of the coming danger as a huge Saudi oil company -- and the chairman referred to this too in his comments -- Saudi Aramco suffered a devastating cyberattack. The virus or malware erased data on 30,000 of the company's computers, replacing it with a picture of a burning American flag.

Then the threat hit our shores. We continued to warn as cyberattacks hit the United States, government computers, including at the Department of Defense, the U.S. Sentencing Commission, the U.S. Treasury -- and it goes on. But still the full Congress did not act.

The threat then spread further, now to our private networks. Target was struck -- or Tar-Jay (ph). Then as our banks, JPMorgan was -- were -- was hit as well as Visa and the Bank of America. In FY 2012, Department of Homeland Security responded to 198 cyberincidents across critical infrastructure sectors. And of these, 40 percent were in the energy sector. The energy sector continues to bear the brunt of our country's cyberattacks because hackers recognize that the energy sector is our country's Achilles heel.

The effects of an attack would send a shockwave through our economy. Remember how a single fallen tree in Ohio back in 2003 triggered a blackout for nearly 50 million people. Just think about what a cyberattack would do. It could be catastrophic.

We're watching the threat grow and spread. Attacks have hit the State Department and the White House. The danger is not waiting. So what's the full Congress waiting for? Thanks to Chairman Rogers' leadership and the -- this bipartisan committee, the House passed its cyber legislation. This legislation would fix a dangerous gap in our nation's cyberarmor, the inability to share threat information between the public and private sectors.

The private sector owns about 80 percent of the Internet, which makes it difficult for the government to help protect our networks. Right now if your house is broken into, you call 911, and the cops come. But if a company gets cyberattacked and billions of dollars are stolen -- which has happened in the United States, and it is happening -- they can't call a cyber-911 line in the same way.

On the other hand, the government may have cyberthreat information. But currently there's no legislative framework in place to share it with the private sector. It's like being able to see Hurricane Sandy heading up the East Coast but not being able to warn anyone that it's coming.

That's what our cyber legislation does. It enables this crucial two-way information sharing of cyberthreat information. It's the description of the burglar. It's the trajectory of the coming storm. That's what's being shared, not private information.

The Senate has its own cyber legislation, which is very similar to ours but which has not passed the full Senate. Chairman Rogers and I have been working very closely with Chairman -- with Senator Feinstein and Senator Chambliss on these issues in the Senate. We need to move quickly to reconcile the two -- these two issues and pass this legislation. The threat is not going to wait.

So thank you, Admiral Rogers, to take the time today to come before us about the cyberthreat. And Chairman Rogers, again, thank you for having this open hearing so that we can educate our American citizens on this threat and what we need to do.

Thank you.

REP. ROGERS: Thank you very much.

Admiral Rogers, the floor is yours. Welcome, and it's good to know in seven months you haven't bumped into anything too significant. So congratulations.

ADMIRAL MICHAEL ROGERS: Well, Chairman, thank you very much. Vice Chairman and members of the committee, thank you for the opportunity to talk to you today on a topic that clearly is of critical importance to the nation and of critical importance to each of here today.

I'll keep my opening remarks very short, as I -- and I think the interaction between us will generate the greatest value.

I would start by first thanking Representative Rogers for your time, and this will be the last time, I suspect, that I'll be testifying before the committee during your tenure as the chairman. And I just want to say thank you. I thank you as well as your fellow leadership with Representative Ruppersberger on the truly nonpartisan nature that you have created. I think that's a great example for all of us. It serves the nation well. And as an individual that interacts with your committee on a regular basis, I thank you for that. It certainly makes my job better and, I think, easier. And I think more importantly it gets to better solutions, which I think is what we are all about no matter where we are in this room.

I would start out by highlighting I don't think there should be anybody's mind that the cyberchallenges we're talking about are not theoretical. This is something real that is impacting our nation and those of our allies and friends every day. And it is doing it in a meaningful way that is literally costing us hundreds of billions of dollars, that is leading to a reduced sense of security and that has the potential to lead to truly significant, almost catastrophic failures if we don't take action.

It also highlights to all of us, I think, that there is no one single group or party -- party in the sense of whether it be government, whether it be the private sector -- the challenges here are so broad that the idea that one sector or one individual organization is going to solve this, I just don't think is realistic. It is going to take a true partnership between the private sector, the government and academia to address the challenges we have.

I think the work that you have done on the legislative side is critically important, because we need a legal framework that enables us to rapidly share information, machine to machine and at machine speed, between the private sector and the government, and do it in a way that provides liability protection for the corporate sector, as well as ensuring that the very valid concerns about privacy and civil liberties are addressed.

I think we can do that. I think you've done that. The challenge clearly is achieving the political will and the political consensus to pass that. I leave that up to you fine women and women. What I'll try to focus on is, so, what do I think within the realm of responsibility of U.S. Cyber Command and the National Security Agency? What do we need to be doing?

In my hat as the National Security Agency - I'll talk about that first - primary roles for us, to ensure that we are generating insights that aid the public sector as well as government - the private sector as well as government, in terms of what's the cyberthreat out there. What's coming at us? How can we give timely advance information that help us be in a position to respond and defeat those efforts getting into our systems, whether that be on the private side or in the government?

In addition, NSA has a primary role in ensuring its information assurance expertise is available to help both the government and the private sector in defending its systems and generating the standards and approaches to how you defend capability and ensuring that our expertise is available to help.

From the U.S. Cyber Command perspective, three primary missions for us: Number one, to defend our department's network. So I find myself, as many people do, just as the private sector does, just as many other elements in the government responsible for defending the cyber infrastructure of a large global organization.

We're taking a series of steps in the department to do that. It never goes as fast as you would like, but I'm very comfortable about the rate of progress and the plan we have to do that.

The other thing we're trying to do at U.S. Cyber Command is we're tasked with generating the cyber mission force, if you will, the men and women who are going to be addressing the department's cyber need, from the defensive to the offensive; and then, lastly, to be prepared, if directed by the president and the secretary of defense, to provide DOD capability to defend critical U.S. infrastructure.

As I think many of you are aware, the U.S. government has designated 16 segments within the private sector as being of critical significance to the nation's security. Think water. Think power. Think aviation, financial - 16. U.S. Cyber Command is tasked to be prepared to provide DOD capability to defend that infrastructure.

We continue to move along in that journey. We're about halfway through, the department has, between fiscal year `13 and fiscal year `16. So we have about four years to generate that capability, if you will. We're about halfway through that journey in time. We're about 40 percent in terms of actual generation of the force to date. Again, it's progressing well. We continue to learn insightful lessons as we continue through this.

I always remind people this will be an iterative journey, and where we are right now is not necessarily where we're going to end up. We're all trying to learn here. And cyber is an environment, a mission set, that continues to change.

And with that, I think I'll just answer any questions on any topic you might have.

REP. ROGERS: Thank you, Admiral.

Mr. Conaway.

REPRESENTATIVE MIKE CONAWAY (R-TX): Thank you, Admiral.

Your last comments - that was actually the question I had written down to ask you about, and that is your efforts at recruiting and retaining the folks that you need to defend as well as attack, assuming they get the orders to do that.

Given that this skill set in the kind of colloquial wisdom doesn't look like a, you know, clean-cut, short-haired, wearing, you know, a white Navy uniform kind of person, how do you fold in the kind of - or find the folks with the mindset to be able to do these kinds of specific technical things and also have the mindset to be a good sailor as an example, or soldier?

ADM. ROGERS: Thank you, sir.

So I'd make a couple of comments. First, the workforce will be composed of both military and civilian. So one of the comments I make to people is that gives us the opportunity to have a pretty broad swath of individuals. If you come out to the National Security Agency today, you will see people with long ponytails, T-shirts, jeans; very casual, different approach to doing things, as opposed to what the military force looks like.

I think that's one of the advantages of a military and a civilian component to the workforce. We can get a broad range of capabilities and backgrounds. They don't all have to be the same. They don't all have to meet a military requirement, so to speak, in terms of physical fitness, standards of uniform and other things.

I'll tell you, when I started working in cyber in the department 10-plus years ago, my number one concern was how are we going to be able to recruit and retain the men and women that we need to execute this mission within the constraints we have within the department?

Ten-plus years into this now, and now, as the commander of United States Cyber Command, I would tell you I have been pleasantly surprised by our ability to do that, both in the uniformed element of the workforce and in the civilian element of the workforce.

REP. CONAWAY: I understand at NSA you'd have that blend. But in actual Cyber Command itself and then in the field, would you have a blend there as well?

ADM. ROGERS: U.S. Cyber Command is the same model.

REP. CONAWAY: OK.

ADM. ROGERS: It's military and civilian. Now, the ratios are different. At U.S. Cyber Command, we're probably 80 percent military, 20 percent civilian. At NSA -

REP. CONAWAY: Is there an issue with pay differential between the two workforces, people doing the same job, one of them wearing a uniform getting one scale, someone sitting beside them with a ponytail, T-shirt and flip flops -

ADM. ROGERS: I've never heard - I've never heard that -

REP. CONAWAY: OK.

ADM. ROGERS: - that issue raised.

REP. CONAWAY: All right. And about retention, we've got - at Angelo State University in San Angelo, Texas, we've got a great cybertraining facility as well as at Goodfellow Air Force Base. We spend - and these are all uniformed folks being trained at Goodfellow - a lot of money and a lot of time giving these kids tools that are very valuable in the private sector. So what's the retention issues that you're dealing with?

ADM. ROGERS: Right. So, knock on wood, to date retention has exceeded our expectations. I think that's largely due to the fact - and it's not unique to cyber - you can look on almost any military set, skill set. We are not going to compete on the basis of pay. Where we're going to compete is we will attract people who have - who will be attracted to the ethos and culture, this idea of serving something bigger than yourself.

We will attract people who like the idea of service to the nation as a core part of what they do in life. We will attract people who are attracted to the idea of you are doing something that matters to this nation and you are helping to defend this nation.

We will attract people on the basis of we're going to let you do some really neat things. And we're also attracting and retaining people on the basis of, in our culture, in our model, we're going to give you responsibility at a pretty junior or young age. That seems to have really resonated with both the military and the civilian parts of our workforce.

REP. CONAWAY: Is there - and I asked this question at Goodfellow. We train an infantryman to use an M-16, and they know how to do it really well. It's pretty clear that when they leave, they don't take that weapon with them back into the private sector.

Is there an ethics element to these cyber-trained folks? Because they'll take that skill set with them and could go rogue if they don't have the right kind of mindset. Is there some part of that training and that constant reminding that we're giving you tools that, improperly used in the private sector, could do great harm?

ADM. ROGERS: Ethics is clearly a part of what we do as a force, as an organization, if you will. I think it's the same challenge, for example, when we provide military members sniper training. We remind them you're given this capability. We give you this training under a specific set of authorities for a specific mission. And it's not legal or appropriate to use this otherwise. And we do the same thing in the cybermissions.

REP. CONAWAY: Thank you, Admiral; appreciate your work.

I yield back.

REP. ROGERS: (Off mic.)

REPRESENTATIVE JIM HIMES (D-CT): Thank you, Mr. Chairman.

Thank you, Admiral, for being with us.

We heard last week from General Cartwright that more needs to be done to set international norms, something analogous to the laws of war, with respect to cyber. I'm wondering if you could take a few minutes to give us some sense, as somebody who's in the day-to-day mix here, about what some of the key principles might be for those international norms.

I'm obviously worried that in the absence of such agreements or norms, it may take a catastrophe and a retaliation to a catastrophe to force people to the table. So I wonder, could you give us a sense both what you think those norms would look like and, secondly, how we could help catalyze that agreement around the world?

ADM. ROGERS: Well, firstly, I would strongly concur with General Cartwright's comments. We have got, I believe, to develop a set of norms or principles for behaviors in this space, because, absent that kind of thing, being totally on the defensive is a very losing strategy to me. It will cost a significant amount of money. It leads to a much decreased probability of mission success. That's just not a good outcome for us in the long run.

And as you yourself referenced, and Representative Rogers did in his opening statement, there doesn't seem to be a sense of risk among nation-states, groups and individuals in the behaviors we see in cyber, that you can just do literally almost anything you want and there isn't a price to pay for it. That's not a good place, I would argue, for us as a nation, and I would argue, more broadly, for us internationally to be in.

So what we’re trying to -- and I’m not the primary in this, but what we’re trying to make an argument, if you will, collectively is we need to develop a set of norms and behaviors that we can fundamentally agree with as a starting point for how we’re going to behave and act within this environment. I’ve seen an initial set of points that the White House has developed and, in fact, has shared -- have been raised in a couple of United Nation forums. We’ve talked about things like treat certs as hospitals, every nation-state should have its computer emergency capabilities left alone, every nation-state -- that would be destabilizing -- you want every nation to have the ability to respond to cyber emergencies. You don’t want to take that capability away.

We need to define what would be offensive, what’s an active (warrant ?) Those are all issues we’re trying to come to grips with right now. And in the absence of any current definitions or any current expectations of behaviors, now, we’re all in the -- left in the place where we’re trying to guess what the intent is and we’re trying to guess how far things are going to go. That’s just not a good place for us to be.

REP. HIMES: So in addition, you highlighted one principle there, I guess some sort of agreement not to attack a nation’s emergency response capability. What else? What else would you suggest? I mean, obviously, you know, there’s a difference between taking down a sovereign’s internal IT capability and, you know, trying to steal a commercial secret that’s probably in law or at least in the laws of war some difference there.

So what else in addition to sort of isolating response capabilities --

ADM. ROGERS: There’s discussion about do we want to put in standards about critical infrastructure for a nation-state. If you’re -- if you’re going to go down that road, then that’s a step beyond these norms and behaviors. Therefore, you’re opening yourself up to potential repercussions. So the idea of critical infrastructure, some discussion about nation-state application against the commercial sector is a way to steal intellectual property for nation-state gain, you know, that -- we have always argued that that is not within the U.S. vision. We don’t do that. We have always argued that’s not appropriate for the role of a nation-state. I think that would be among them.

Going after, as I said, infrastructure. If you looked at going after things that could lead to loss of life, if you looked at going after things that could lead to loss of control, you know, as outside the norms of behavior, that those are the kinds of things we’re having discussions about, what -- how do we build the framework if you will.

REP. HIMES: Do you, as you sort of look at the discussion internationally happening here, do you have any confidence that this debate or this discussion is going to advance? And in particular, are we going to be able to draw in bad actors like China and Iran? Or is it going to, in fact, take some demonstration of capability against them to get them to the table?

ADM. ROGERS: I don’t know, is the short answer. I’m hoping it’s not the latter. Clearly, there’s ongoing dialogue.

You know, the other complicator in this is I often will hear people use the kind of nuclear analogy in terms of how we were able to develop over time to develop the concepts of deterrence, norms and behaviors. I try to remind people to remember the challenge of the nuclear analogy is when we started most of that work back in the 1950s and the 1960s, you had a capability -- in this case, nuclear weapons -- that were controlled purely by nation-states, no individuals or groups, by a very small number of nation-states -- you know, two really, to start with initially when we had these initial discussions.

That’s very different from the cyber dynamic, where we’re not only going to be dealing with nation-states, but we’re going to be dealing with groups, with individuals, when we’re dealing with a capability that is relatively inexpensive and so easy to acquire, very unlike the nuclear kind of model. That makes this really problematic.

REP. HIMES: Yeah, yeah. Thank you. Thank you very much. Thank you, Mr. Chairman.

REP. ROGERS: Admiral, there’s -- recently, there’s been some disclosure of Trojan Horse malware on power networks and critical infrastructure. Can you talk about what the intention may have been? Can you talk about that threat a little bit? What -- if you have any attribution to any organization or nation-state that may have been involved? And kind of put it in context about --

ADM. ROGERS: Right.

REP. ROGERS: -- what this -- what this really means for the national security interests of the United States.

ADM. ROGERS: So we have seen instances where we’re observing intrusions into industrial control systems. What concerns us is that access, that capability, can be used by nation-states, groups or individuals to take down that capability. In fact, as you saw with Aramco, for example, to destroy or be destructive with that capability.

We clearly are seeing instances where nation-states, groups and individuals are aggressively looking at acquiring that capability. What we think we're seeing is reconnaissance by many of those actors in an attempt to insure they understand our systems so that they can then, if they choose to, exploit the vulnerabilities within those control systems.

Those control systems are fundamental to how we work most of our infrastructure across this nation. And it's not just the United States, on a global basis. They are foundational to almost every networked aspect of our life, from our water to our power to our financial segment to the aviation industry just as examples. They're so foundational to the way we do -- we operate complex systems, you know, on a national basis.

It's one of the areas when -- people often will ask me so what are the coming trends that you see. I think the industrial control system and the SCADA piece are big growth areas of vulnerability and action that we're going to see in the coming 12 months, and it's among the things that concern me the most because this will be truly destructive if someone decides that's what they want to do.

REP. ROGERS: If -- or it was determined that that malware was on those systems, can you be a little more definitive on what does that mean? If I -- if I'm on that system and I want to do some harm, what does that do? How does that impact the broader -- do the lights go out? Do we stop pumping water? What does that really mean? And the fact that it was there, does that mean they already have the capability to flip the switch if they wanted to?

ADM. ROGERS: Well, let me ask (sic\answer) the last part first, if I could. There shouldn't be any doubt in our minds that there are nation-states and groups out there that have the capability to do that, to enter our systems, to enter those industrial control systems, and to shut down, forestall our ability to operate our basic infrastructure, whether it's generating power across this nation, whether it's moving water and fuel, whether it's moving, you know, some -- I'll highlight those because those tend to be the biggest focus areas that we have seen.

So once you're into the system and you're able to do that, it enables you to do things like, if I want to tell power turbines to go offline and stop generating power, you can do that. If I wanted to segment the transmission system so that you couldn't distribute the power that was coming out of power stations, this would enable you to do that. I mean, it enables you to shut down very segmented, very tailored parts of our infrastructure that forestall the ability to provide that service to us as citizens.

REP. ROGERS: So if -- and you've determined that nation-states have that ability.

ADM. ROGERS: Yes, sir.

REP. ROGERS: And there was a public report, the Mandiant report, that referred to Chinese -- attributed to the Chinese government hackers being on our -- some of our critical infrastructure systems. Is there any other nation-state that you believe has been successful in getting on those systems?

ADM. ROGERS: There’s probably one or two others. I apologize if I could -- we consider that classified, and so in an open hearing, I apologize, but I’m not really comfortable with spelling out specifics. But I would say there is more than one nation set out there that we watch, that we believe has these capabilities.

REP. ROGERS: So -- and the thrust of that question is really to say that it isn’t a one-off --

ADM. ROGERS: Right.

REP. ROGERS: -- according to that public report. There are multiple nation-states who both have the capability and have likely actually been on those networks at some point.

ADM. ROGERS: Definitely more than one. And the other point I would make is we’re watching multiple nation-states invest in this capability.

REP. ROGERS: And when you say invest in it, can you talk about that, what that means? That’s -- this is an important, I think, turn of events here.

ADM. ROGERS: So when I say invest in this capability, we see them attempting to do reconnaissance on our systems, attempting to generate insight about how our networks are structured. We see them doing research in this area. We see them attempting to steal information on how our systems are configured, the very specific schematics of most of our control systems, down to engineering level of detail so they can look at where the vulnerabilities, how are they constructed, how could I get in and defeat them?

We’re seeing multiple nation-states invest in those kinds of capabilities.

REP. ROGERS: Right. And what -- so that -- you mentioned this next group, so you’ve seen the international organized crime organization certainly starting to develop their capabilities, and we’ve seen in some cases them using nation-state-like techniques. Can you flesh that out for us? So now you’ve highlighted the nation-state threat, and this would, I would argue, is probably that one down that gives us pause for concern.

Can you talk about that threat and what it means and why It’s so difficult for the private sector to try to defend themselves against those threats?

ADM. ROGERS: So what we had traditionally seen in the criminal sector was criminal actors, gangs, groups, penetrating systems and trying to steal information that they then could sell or use to generate revenue. So credit card information, selling personal information on - there's actually a market out there to sell personal information on individuals. They had been stealing - we had been watching them and observing them stealing data associated with generating revenue.

The next trend that I think we're going to see in the coming near term is you will start to see, I believe, in many instances some of those criminal actors now engaging not just in the theft of information designed to generate revenue but also potentially as a surrogate for other groups, other nations. Because I'm watching nation states attempt to obscure, if you will, their fingerprints. And one of the ways to do that is to use surrogate groups to attempt to execute these things for you.

It's one reason, for example, while we're watching criminal actors start to use some of the tools that we historically have seen nation states using now, you're starting to see criminal gangs in some instances using those tools, which suggests to us that increasingly in some scenarios we're going to see more linkages between the nation state and some of these groups. That's a troubling development for us.

REP. ROGERS: So cyber hit men for hire, really, serve nation states. I had a lot more on threats but I'm going to do this quickly, but I just want to ask this last question. So in this cyber sharing regime of which you talked about, certainly what our legislation proposes, there are concerns - and I think they're valid without the understanding of exactly how it worked, machine to machine real time, millions of pieces of information or packets at the, you know, speed of light.

How can we assure Americans that their personal information is not being read or collected or used by the NSA in that real-time, machine-to-machine sharing that would allow you to share what you know with your malicious source code, with the private sector, so they could protect their own networks?

ADM. ROGERS: I think there's a couple of ways to this. First of all, I remind people, this is about computer network defense, not about intelligence. Totally different missions with totally different objectives. The second point I would make is, we need to very publicly sit down and define just what are the elements of information we want to pass to each other and we want to make that very public. These are the specific data fields, this is the specific information that we need, both what does the private sector need and what does the government need.

From my perspective as the director of the National Security Agency, when we add, for example, private information into this, that complicates things for me because I have specific protections that I must provide to U.S. person data, for example, that will slow us down. That's not what we're interested in. That would be a negative for us. It will lead to a slower sharing of information and that's not what we want.

So I think sitting down and having a very public discussion detailing exactly what we're talking about when it comes to information sharing is one way to do that. And also highlighting what we're not talking about. This is not what we want to see. I don't want people's personal data. I'm not interested, and so I want names, I want addresses, I want - that's none of the kinds of things that we're talking about in this scenario.

REP. ROGERS: (Off mic.)

ADM. ROGERS: Right, and it's not.

REP. ROGERS: And this is not the NSA plugging into the private networks of the United States and monitoring those networks.

ADM. ROGERS: Which is exactly why we need to do this, because my comment is, look, you don't want NSA in that private sector network. I'm not in that private sector network. Therefore, I am counting on the private sector to share with us so tell - what I'm interested in from the private sector is, what I think I would owe the private sector is here's the specifics of the threats we think are coming at you. Here's what it's going to look like. Here's the precursor kinds of activities we think you're going to see before the actual attack. Here's the composition of the malware we think you're going to see. Here's how we think you can defeat it.

What I'm interested in learning from the private sector is, so tell me what you actually saw. Was the malware that you detected written along the lines that we anticipated, was it different? How was it different. Help me understand when you responded to this what worked for you and what didn't work. How did you configure your networks? What was effective? What can we share with others so that the insights of one now come to the aid of many? That's the kind of back-and-forth that we need with each other.

REP. ROGERS: And you made a very interesting point and I think it's one of the, I think, biggest perception problems of this whole debate. When you said the NSA is not on those American private sector networks, can you take just a couple of sentences - again, I'd add is important. Because unfortunately I think people would believe the NSA is on their private sector networks. It's not, which is candidly why the bad guys have so much opportunity to swim around in there. So can you just talk about that? This to me is one of the most important points if we can make clear to the American public today about what we're trying to do and why that part - why the fact that you're not on there and don't want to be on there is so important.

ADM. ROGERS: So the National Security Agency is a foreign intelligence organization, it is not a domestic intelligence organization. There are specific legal constraints placed on us when it comes to collection against U.S. persons. U.S. persons includes the definition of a U.S. entity in the form of a company. We're specifically legally limited from doing that. We do not have a presence on U.S. private networks inside companies. That's not what we're about, that's not what our mission is. It's because of that lack of awareness, if you will, on our part that I'm saying, look, I need a partnership here. We need to exchange information.

And on the first - you don't want us on those private networks. You know, if I was a CEO of, pick a major bank, I wouldn't want to be telling my shareholders, well, you know, NSA's inside our network. That's not the way we work. But I would, I would think, want to tell my shareholders, hey, look, we have a proactive sharing relationship where we are gaining the benefits of the insights that NSA is generating in terms of what is likely to come at us and we're sharing with them, here's what we're doing, here's what's effective, here's what hasn't been effective. This is the help we need from you. That's the kind of relationship I think we need.

REP. ROGERS: Important point. The NSA is not on American domestic networks, but the Russians, the Chinese, the Iranians and multiple other bad actors are. Mr. Ruppersberger.

REP. RUPPERSBERGER: Yeah. I also want to get into the trench later but I think the chairman has raised a very important issue. It's one of the things that we've been dealing with in developing legislation to protect our country, to protect our businesses from losing billions of dollars. We spend a lot of time negotiating, and thanks to this committee and the chairman's leadership, we've been able to put together a bill that unfortunately has not passed in the Senate about the FISA bill that gives you the authority to do what you need to do.

What I'd like to do is to get - for you in this open hearing so the American public can understand what the checks and balances are for the NSA and the fact that, again, your focus is not on American people and the argument from privacy a lot is what could happen. And I think that debate is good. I'm glad in this country we have the privacy groups who focus on that and debate that so we can come together and learn and develop legislation that deals with the issue of privacy protections, and if in fact someone at NSA breaks the law that they'll be held accountable.

The bill that we passed, and unfortunately it hasn't gone in the Senate, dealt with a lot of issues of bulk collection. The perception, unfortunately, of the American people is that because the government controls so much of just strictly a phone number, nobody's name, nobody's address, but there was still a perception to the public - unfortunately the national media pushed it out pretty far too - that somehow NSA was listening. It wasn't the case.

So this committee came together. We developed legislation to take bulk collection away from the government. And now if in fact, you know, you all find a terrorist situation in Yemen, you get that information, you immediately turn it over to the FBI because you don't have jurisdiction in this country, and then with this legislation we have has pre-judicial and post-judicial review for the FBI basically at that point to move forward and attempt to protect us in in fact we need to protect us.

Also we are not listening to Americans at all. If we are listening to Americans, an American's a target, we have judicial review, the same thing we do in the United States with criminal cases. You know, we get the court - if we need to have a search and seizure or a wiretap, we have to get the court. That's our check and balance in this country. And by the way, the checks and balances we have in this legislation are the most stringent of any country in the world.

So it's important, I think, the message that has to get out now is that -- is that we do have privacy concerns, we do have constitutional issues, and there are checks and balances. And if in fact someone does break the law, they'll be held accountable. I'd like you to get into more specifics. The chairman raised the issue on what happens if you do break the law and why you have the checks and balances that you're not going to be listening to Americans, you don't have the jurisdiction to begin with, and that's turned over to the domestic side in this country with the supervision of the court, privacy groups overseeing it, that type of thing. Its' a long question, a short answer maybe.

ADM. ROGERS: Yes, sir. So in broad terms there's a legal aspect this country with the -- with the supervision of the court, privacy groups overseeing it, that type of thing. It's a long question, so a short answer maybe.

ADM. ROGERS: Yes, sir. So in broad terms, there's a legal aspect to this in terms of there is a court of law, whose authority and permission we must gain. We have to formally petition the court if we're going to do focused collection against a U.S. person. To do that we have to prove to a court of law that there's either a connection with a foreign nation, so they're acting as an agent of a foreign government, or they're affiliated or connected with a terrorist organization or an entity that is attempting (to do ?) harm to U.S. or U.S. persons. We have to make a legal case to a court. We have to present a level of evidence that suggests, hey, the court should grant us permission to do that.

REP. RUPPERSBERGER: And that evidence is reasonable, articulable suspicion; it's a RAS test?

ADM. ROGERS: Right. So first there's a legal control on just how we can collect against U.S. persons, so to speak. In addition, the Congress as the duly elected representatives of the citizens of the nation conducts an oversight function. It's one of the primary roles, you know, that led to the creation of the HPC and the SSC in both houses, the idea that our elected officials would be briefed on what we do and have oversight and knowledge of what we do and how we do it that would act as the representatives of our citizens to ensure that there was an external party monitoring what we do, having awareness of what we do, being briefed regularly on what we do, being formally notified -- as you're aware, I do formal notifications to the committees, say, hey, as a matter of record I want you to know we're doing this, want you to know we're doing that, I want you to know we've run into the following challenges.

There's an oversight mechanism to this in addition internally. We have created a pretty extensive oversight and compliance set of mechanisms that govern things like how we control our data, who has access to that data. There's training requirements for every one of our employees that has access to any of that such data. We control the numbers of employees who have access to that data. If you look at the bulk record, the phone issue, for example, under the Patriot Act, Section 215, it was something on the order of approximately 30 people out of an organization that numbers in the tens of thousands.

Again, we try to ensure that we maintain tight control of the data that we've been granted legal authority to collect. We don't retain that data indefinitely. We have different -- we have defined windows as to how long we can retain data. And once we complete the window, we purge all that data and remove it. We don't hold data forever.

We also are required to ensure that we maintain protection of the data from the moment we collect it to the moment we purge it. So we don't sell data, for example. We have to maintain strict controls over the information that we've been granted authority to collect.

When we are doing bulk collection overseas, for example, when we become aware of data that specifically is tied to a U.S. person, we have to stop what we're doing, and we have to either make a decision in our own mind, OK, is there a legal connection here with either a nation state or a group that we need to go to the court to get permission, or do we just stop collecting? We have to make that decision. We have to make a legal case if we want to continue, if we're going to target someone.

So there's the legal framework to what we do. There's a series of protections and oversights to what we do both external to the organization in multiple branches of our government. There's also a series of controls in place within the organization. You know, I -- it's one reason why I would say, look, you can certainly disagree about the legalities in terms of, hey, is a law good, is a law bad. My responsibility as the director of NSA is to ensure that we comply with the law. And there shouldn't be any doubt in anybody's mind. We comply with the law. And when we fail to do so, we will hold ourselves accountable.

REP. RUPPERSBERGER: All right. Just one thing, because I want other members to (have some ?) questions --

ADM. ROGERS: (Sure ?).

REP. RUPPERSBERGER: -- on the issue of threat. Technology experts were recently interviewed by the Pew Internet and American Life Project. And a majority of these technology experts said they believe a major cyberattack will happen between now and 2025, which will be large enough to cause significant loss of life or property; losses, damage, theft at the levels of tens of billions of dollars.

Do you share this grim assessment with the majority of these experts? Why or why not?

ADM. ROGERS: I do.

REP. RUPPERSBERGER: OK. Well, then explain.

ADM. ROGERS: Now, what I have told my organization is I fully expect that during my time as the commander we are going to be tasked to help defend critical infrastructure within the United States because it is under attack by some foreign nation or some individual or group.

I say that because, as you've already highlighted, we see multiple nation states and then in some cases individuals and groups that have the capability to engage in this behavior. We have seen to date this behavior actually, as you saw in the -- as you raised in the Aramco piece, we've actually seen this destructive behavior acted upon, executed. We have actually seen physical destruction within the corporate sector, knock on wood, that has been largely outside the United States, but it has happened. We have seen individuals, groups inside critical U.S. infrastructure, you know, that has a presence, that suggests to us that this is -- this vulnerability is an area that others want to exploit.

All of that leads me to believe it is only a matter of the "when," not the "if" that we are going to see something dramatic.

REP. RUPPERSBERGER: Thank you. (Inaudible.)

REP. ROGERS: And you're seeing attacks now, some you're able to repel --

ADM. ROGERS: Right.

REP. ROGERS: -- but you're under attack today.

ADM. ROGERS: Yes, sir, every day.

REP. ROGERS: Is U.S. government cybernetworks under attack today?

ADM. ROGERS: Sir, people trying to gain unauthorized access, people attempting to steal data, potentially people attempting to manipulate data.

REP. ROGERS: And that's happening today. This is not some theory, this is going to happen in 2025.

ADM. ROGERS: No, this is not theoretical.

REP. ROGERS: What you're saying is it might -- they might just get through before 2025, is that correct?

ADM. ROGERS: I don't think it'll -- we'll have to wait till -- unfortunately my comment would be I bet it happens before 2025.

REP. ROGERS: Ms. Bachmann.

REPRESENTATIVE MICHELE BACHMANN (R-MN): Mr. Chair, I just want to thank and compliment you and the -- Ranking Member Ruppersberger for holding this important hearing, as this committee has spent a great deal of time on this issue. I think that, Admiral Rogers, your compelling testimony makes it clear to the American people that we need to even redouble our efforts on this area and make sure not only are we paying attention but we're taking direct actions to protect the American people and our economy from cyberespionage and -- as well as our military espionage.

I've had occasion to travel to China in August, and it was very clear that the Chinese saw no difference between cyberattacks on military versus espionage and they were open to doing both of them.

Thank you for this important information that you're putting out. As we know, the technology is changing rapidly and increasing rapidly. And one area that a lot of people are beginning to be engaged in and yet people have fears about is the area of cloud computing, mobile and cloud computing.

So could you talk to us a little bit about -- and as a follow-on to the ranking member's question -- are there bad actors that you have detected -- and I don't know if this is classified information or not -- can you let this committee know, are there bad actors that are -- that you have already detected in the mobile and cloud computing? And how does this advance toward mobile and cloud computing change cyberactivity and cyberattacks going forward for the private sector as well as for our government?

ADM. ROGERS: Thank you, ma'am. So, yes, we have observed both the cloud, if you will, as well as mobile handheld digital devices becoming -- being attacked, being exploited. The mobile arena in particular is an area where, as I look to the future, if you ask me, so, again, what are the major trends you're going to see in the next 12 months, efforts against the mobile side (is ?) one of the top three that I would kind of highlight to say, hey, look, this is a coming trend in no small part because if you look at the proliferation of devices, it's -- the greatest growth these days is not in the traditional corporate, fixed large network structures; it's in -- and this is both true for us as individuals, as citizens, as well as for most of us in terms of business -- you see the same phenomenon in government -- we are all turning to mobile digital devices as vehicles to enhance our productivity, the ability to work wherever we want, whenever we want.

The flip side is those same things that make it attractive -- the ability to spread this outside of secure spaces, the ability to use it in all sorts of environments almost universally in any place -- that also represents an increased potential for vulnerability.

REP. BACHMANN: So, Admiral, can you speak a little more specifically to that? Are -- is mobile and cloud computing -- is -- in your opinion, is -- are the American people and American companies more vulnerable through mobile and cloud versus the servers or less or equal?

ADM. ROGERS: On the cloud side, you can see arguments on either way. In general I am supportive of the cloud idea, because my view is one of the challenges to defense is the broader, if you will, of a structure you have, the more you have to defend, the greater the probability of people penetrating you. One of the things that I find attractive about the cloud is it collapses, if you will, your attack surface down to smaller. Now, the flip side, though, is where people who don't like it would argue, well, you're kind of putting all your eggs in one basket. So if somebody gets into the basket, they get right to all the eggs. That is certainly true.

The flip side is -- I would argue is this enables you to protect that basket a whole lot better than having multiple baskets with the eggs spread around and with the baskets all connected, as it were. And I apologize -- I never thought I would be testifying -- (laughs) -- using an analogy about baskets and eggs. So I'm supportive of the cloud. I think it's the right way to go.

REP. ROGERS: We're looking for a new cliché in cyberdiscussions. You may have given it to us right there.

ADM. ROGERS: In terms of the mobile piece, it is really going to be problematic, because part of the whole idea of mobile is --

REP. BACHMANN: And it doesn't matter which mobile device, right?

ADM. ROGERS: Yeah, it already --

REP. BACHMANN: You don't -- any distinction.

ADM. ROGERS: Now, the way the whole network --

REP. BACHMANN: I don't want to lead you. I just --

ADM. ROGERS: No, no. The way the whole network, in some ways, is structured, the idea that you're just going to pull down whatever application you like -- I'd only highlight to people, remember, those applications have a lot of potential vulnerabilities in them. Look at -- you look at all of us. We're out consciously searching for applications that make our lives more productive, that make things easier, more convenient for us, and also represents a lot more potential vulnerability.

REP. BACHMANN: I appreciate that. Well, I see my time is up, so I yield back. Thank you, Mr. Chairman.

REP. ROGERS: Thank you, Ms. Bachmann.

Mr. Schiff.

REPRESENTATIVE ADAM SCHIFF (D-CA): Thank you, Mr. Chairman.

And Admiral, thank you for your service to the country. You have, I think probably, undoubtedly, the most difficult job within the IC, and we're grateful that you took it on.

I wanted to ask you a couple legislative questions, one on the cyber bill. One of the major differences between the House and Senate proposals involves the sharing of information between the government and private sector, and what requirements we'd place on the private sector to remove private information before sharing it.

Last month, in comments before the Chamber of Commerce, you mentioned that the NSA doesn't need or want private information as part of the cyberthreat information and that, in fact, receiving that information makes your job harder. Given that, does it make sense to require private companies to make a good-faith effort to strip irrelevant personally identifiable information before sharing cyberthreat information with the government or other entities?

And then on the other program, you made reference to the metadata program. As you saw, the USA Freedom Act failed to get the votes to move forward earlier this week in the Senate, which probably pushes that into next year. It means we have to start all over again.

Is the NSA, though, nonetheless moving forward with working with the telephone companies to prepare for the new paradigm where the companies will hold onto their own data? There's nothing in statute that requires the government to gather bulk data, so you could move forward on your own with making the technological changes so that we don't have to wait until next year. So are we making progress on the technological adaptions that we'll need to make?

ADM. ROGERS: So, sir, two parts to your question, and the first part about should we attempt to -- if I misparaphrase, please just tell me -- should we attempt to filter up front, if you will, before the data is pushed to the U.S. government, the removal of any privacy?

REP. SCHIFF: Yes. Should we ask the private companies to make reasonable good-faith efforts to remove any personal information before they either give it to the government or share it among the private sector?

ADM. ROGERS: Right. I think that's all part of that point I was trying to make about let's define all this up front, so we're just not willy-nilly pushing information for the sake of pushing information. We should define exactly what we want, what we need and what companies are going to provide, just as the companies should expect us, the U.S. government, to define up front just exactly what, and what are you not, going to give me and share with me.

So I do agree with this idea of we should build this all up front so we have clear delineations of exactly -- before the data ever gets to us, we should have clear delineations of just what we're going -- what the private sector is going to be sharing with the government.

In terms of your second question -- could you refresh my memory?

REP. SCHIFF: Second question is, are you moving forward already in working with the telephone companies to make whatever technological adaptions have to be made so they can retain their own data, rather than the government collecting it in bulk, since both the DNI and the administration support moving to that model? And there's nothing that prohibits you from doing that; you don't have to wait for the USA Freedom Act. Are you moving forward with those technological changes?

ADM. ROGERS: The shorter answer is no, in no small part because the corporate side has also indicated to us, we'd rather wait and see just what the specifics are going to be of any requirements before we start getting into making changes or starting to have discussions about the specifics of making changes.

I think part of the reason for that, I think on both our perspectives, has been the hope that we were going to come to a solution in the near term. One of the questions now I'm trying to consider is OK, so if we're unable to gain the consensus in the window that we thought, what are the implications of that? Meaning, do we need to start to reach out and have some discussions now? I don't have an answer to that in my own mind yet, to be honest.

REP. SCHIFF: With respect, Admiral, there is no statutory mandate of any kind for the government to collect bulk metadata. The administration and the DNI have said it's no longer necessary, that the telephone companies can hold onto their own data. The only reason the program exists is that the government went to the FISA Court to ask it to bless the program.

There's nothing preventing the government from going back to the FISA Court and saying, we're going to come to you on an individual, case-by-case basis, and doing so. So there's no reason, if you think this is the correct policy, that you have to wait for the Congress to mandate you to do it.

ADM. ROGERS: In fact, that is the current policy that we're acting on right now. The president, in his remarks on the 17th of January, directed us to use that legal court construct. We've been doing that since January, even as he indicated -- and he would turn to the Congress then to, hey, enact the legislation that makes the long-term changes that you think are appropriate.

But we've already been directed to use that model. We now have to go to the court to access the data.

REP. SCHIFF: So is the government then no longer collecting the bulk metadata?

ADM. ROGERS: The data continues to be provided to us. We now, to access the data, have to go to the court to get permission to access the data.

REP. SCHIFF: But why continue to gather the bulk metadata, if both the administration and the DNI don't think this is the best approach?

ADM. ROGERS: I guess I'm confused, because I don't think I've heard the president or the DNI say that the access to the data is not of value. What I think I have heard is the question gets to be, who should hold the data? What the president directed in his remarks on the 17th of January is we'll continue to implement the program as it is right now, while the Congress works through how we're going to make the long-term changes. We will continue to do that on a 90-day interval, so every 90 days right now we have to go back and ask for continued permission.

REP. SCHIFF: One last comment. I know I'm out of time. If the administration believes, and I understand that they do, that the better model is to go to a paradigm where the companies hold onto their own data, it doesn't make sense for us to continue the collection of bulk metadata. We're not -- you're not legally required to, and there's no reason not to move to that model and begin that transition now.

I'll yield back, Mr. Chairman.

REP. ROGERS: Mr. Langevin.

REPRESENTATIVE JAMES LANGEVIN (D-RI): Thank you, Mr. Chairman.

Admiral, thank you for being here today and for the work that you and your team are doing at NSA. Obviously, it's important work to the country.

So we had a discussion just a few minutes ago about some types of things we're seeing in terms of cyberintrusions. Obviously, over these past several weeks the American people have seen a disturbing number of cyber-related incidents, including the State Department, the White House, the National Oceanic and Atmospheric Administration, the U.S. Postal Service and the industrial control systems that control our critical infrastructure, where we found some very concerning malware on those control systems.

And these of course come on the heels of other major attacks, such as -- or intrusions -- such as at JPMorgan Chase, Target, Michael's, Saudi ARAMCO, the South Korean banking attacks. On

"60 Minutes" last month, FBI Director Comey said there are two, and I quote, "two kinds of big companies in the U.S., those who have been hacked by the Chinese and those who don't know they've been hacked by the Chinese." And obviously, other nation-states are doing this, or criminal enterprises, et cetera.

So to date, we've seen these cyberincidents mainly focused on data breaches and industrial espionage, but obviously what keeps me up at night, and I'm sure you as well, is the worry that we could face a true cyberattack, which we haven't really seen yet occur that actually causes significant damage where attackers seek to get the same kinds of effects through cyber that traditionally you'd see through use of kinetic weapons.

And we know that that technology's out there, as you know, and so my question is, we know who and how we would respond if we saw an attack using kinetic weapons, missiles or bombs. We have either the Pentagon or the law enforcement agencies would respond to protect us in those cases, or National Guard. But what confidence can you give to the American people, what can you say to the American people that would give them confidence that we have a plan in place and we know how to respond if either we saw an attack was in the planning stages ready to be executed, or if it was being - the order was given to be executed and we saw it underway and that we could stop it.

At this point is there sufficient mechanisms in place absent presidential authority, or would it require only presidential authority to step in and order an intervention whereby we could prevent that attack and protect our country, protect our critical infrastructure, et cetera? Do we basically - have we had a bridge in place to deal with the bureaucratic and legal hurdles? Or does it take presidential authority at this point?

ADM. ROGERS: The short answer is I'm pretty comfortable that we have a broad agreement and a broad sharing of how we're going to do it, who would do what. The roles are clearly defined. Boy, if I go back two years ago, 18 months ago, we were spinning our wheels about, well, who's going to do what. We're way past that. We've got good delineation within the federal government as to who has what responsibilities. We've got good broad agreement as to how we would go about providing that capability and the scenario you had talked about, with attacks against critical infrastructure.

Clearly presidential authority is required for part of it. For example, for me as a DOD entity to provide support, you know, in the U.S. to partner with others outside the DOD arena, that's required. If part of the response, for example, was going to be an offensive capability, yes, I would need approval of the president to do that. We've got a broad agreement on that.

The challenge to me is, we've got to move beyond the broad agreement to get down to the execution level of detail. I come from a military culture, and the military culture teaches us you take those broad concepts and agreements and then you train and you exercise and you do it over and over, and that's what we've got to do next.

REP. LANGEVIN: So what about less direct attacks, the lesser things, cybercrime, cyberespionage? One could certainly argue that the hundreds of billions of dollars lost to cybercrime and cyber espionage, some of which is highly methodical and systematic, are really a massive threat to the American economy, to competitiveness and jobs. When does that become economic warfare and how do we respond?

ADM. ROGERS: First of all, I think we're still trying to come to grips with when does it become economic warfare. We clearly have tried to make the argument that we try to differentiate between the capabilities of the nation state and trying to understand the world around it versus applying the capabilities of a nation state against the private sector of another nation to generate economic advantage. You know, that tends, for example - that's the major difference, among the major differences between us and our Chinese counterparts, where we have argued we don't accept that premise, we don't use our capabilities to go after private industry and other nations, to use that as a vehicle for us to gain economic advantage. That's not what we do.

To your broader question, I think, though, the shorter answer is we're clearly trying to work our way through all those issues. We tend to treat it right now - you talked about criminal actors. We tend to treat it right now as a law enforcement issue, so the FBI, for example, the primary lead there with Director Comey. I would argue clearly that approach is not achieving the results that we want. You know, we're spending our time dealing with the repercussions of the penetrations.

What I'd like to do is, how can we forestall those penetrations in the first place, and as we've already talked today, that's about those norms, that's about those rules of behavior, that's about those ideas of deterrence. Clearly those are areas where we still have a lot of work to do.

REP. LANGEVIN: Thank you. I appreciate your answer, I appreciate the work you're doing. My time's expired. I have a question I'll submit for the record on cyber mission teams, but thank you for what you're doing. I yield back.

REP. ROGERS: Great.

Ms. Schakowsky. And there's about a minute 15 seconds left on the clock.

REPRESENTATIVE JAN SCHAKOWSKY (D-IL): I'm going to be very brief. On the other side of this, what can you say to assure the American people in the absence of legislation that would address their concerns over the mass collection of metadata and concerns about privacy that, despite the failure of the Congress to pass legislation, what you may be doing differently that could assure them that their privacy is protected?

ADM. ROGERS: So what we're doing differently, as you heard in the president's remarks on the 17th of January, he indicated, hey, while I haven't seen NSA violating the law or attempting to systematically undermine the rights or the privacies of our citizens, I'm concerned about the potential for abuse. Therefore, I'm going to overlay a couple of additional requirements on NSA. So for example, with the metadata, I want you to now go to the court. It's not enough that you use your own authority as the director, so to speak. Now I want you to go to the FISA court to convince a judge that you should be granted access. We didn't use to have to do that.

He also directed - we used to be able when we went into - in those instances when we went into the data we used to be able to what we do - what we called three hops, the amount of times we could follow the string, so to speak. The president came back and said, I tell you what, again, I want to put another level of protection in there. I only want you to do two hops, if you will, if you think there's a connection. So we're not authorized now to follow the string, as you will, as deeper as we used to be able to do. Those are - in terms of the metadata, those are probably the biggest changes that we've dealt with.

In addition, he's provided broad guidance in the form of PPD-28, which is unclassified document that the government has generated, which in a very public, unclassified way outlines the general principles that we want to make sure that we apply in conducting signals intelligence, the mission of NSA. So we're putting those principles in place.

In addition, we've completed over the course of the last 15 months or so a pretty fundamental review of everything NSA does, what we collect against. That's all been reviewed to ensure that we're comfortable from a policy perspective with what we're doing.

REP. SCHAKOWSKY: Thank you.

ADM. ROGERS: Yes, ma'am.

REP. RUPPERSBERGER: One thing on that, Jan, most of what the admiral just said is in our bill, that the Senate unfortunately did not take up. And you were part of putting that together.

REP. SCHAKOWSKY: I realize. Right.

REP. ROGERS: And just quickly, so - and I think this is so important because I think there was some confusion here. When you're obtaining the information for under the Section 215 via the court, are you're not? So don't you have to go to the court -

ADM. ROGERS: That is correct. I apologize. As I thought I indicated, so every 90 days we have to go to the court to get permission.

REP. ROGERS: And so the court overviews, or oversees -

ADM. ROGERS: Oversees the program, continues to look at the justification -

REP. ROGERS: Is there content on those phone calls?

ADM. ROGERS: No.

REP. ROGERS: Are you taking, collecting, storing content -

ADM. ROGERS: No.

REP. ROGERS: -- on phone calls obtained under Section 215?

ADM. ROGERS: No.

REP. ROGERS: And the information that you get is metadata. Does it contain PII in that metadata? Do you store the PII?

ADM. ROGERS: You could - well, it goes - again, I'd have to talk to a lawyer. But you could argue, I guess, that a phone number is PII. Of course the challenge is - not the challenge. We get the number, not a name.

REP. ROGERS: Yes. So there's no names and no addresses -

ADM. ROGERS: No addresses.

REP. ROGERS: -- the information of which you collect, and you use that as an analytical tool. Do you believe that that information is valuable in any counterterrorism effort that the United States undertakes?

ADM. ROGERS: Yes, I do.

REP. ROGERS: And do you have personal knowledge that that information has led or assisted in any counterterrorism investigation to help defend the United States?

ADM. ROGERS: Yes. I mean, I definitely think it has been of value and assistance to our efforts.

REP. ROGERS: All right. So just to make sure. This is really important to me. No content is collected on any of those phone calls under Section 215. You get a review by the court every 90 days, meaning you have to go back every 90 days with what you've done with it and how you've processed it and how you've handled it. And if you want to go for another 90 days, you have to make the case on why you do that.

ADM. ROGERS: Right. We have to make the case for the next 90 days.

REP. ROGERS: All right. So, you know, there's some notion that we shouldn't be participating in this, I think was a bit confusing here. I think we've tried to get this right by the ending of the bulk metadata collection by the government putting it all in one place. Even though those protections were in place, I think the general conscience of America said, yes, it was legal, it was constitutional but maybe that's not the way to do it. You've adjusted to that, is that correct?

ADM. ROGERS: Yes.

REP. ROGERS: You've adjusted to the new requirements. There are two, I think, competing bills that are trying to get this right. But I would be cautious about shedding that before there's any legislative direction on fixing that, would be my caution, and I know some others have called for something different. And secondly, on the PII from companies, don't you have the capability to strip PII from information? The NSA? Don't you do that today? You do that in any case.

ADM. ROGERS: Right. I would think we could do that in an automated fashion. Again, it's one of those things that, one of the reasons why I would want to have a discussion about exactly what kind of information we're talking about. And I can also build in the protections in terms of the technical -

REP. ROGERS: And I think this is - that was an important part missed in that conversation, that even if a company doesn't have the capability today but says, hey, I have this malicious source code that looks like this. I'm going to give it to you. You would have the ability to strip out PII before it ever got into your analytical database, is that correct?

ADM. ROGERS: I think -- I think we could do that.

REP. ROGERS: Yeah. In past conversations, that's at least what the NSA has told us; I believe that's accurate. My only fear is -- and again, this was the biggest debate; you want companies to participate -- because this is voluntary, we need to make sure that the liability standards are right if they are in fact in good faith trying to provide malicious source code without PII that these companies aren't held to some different standard when accidentally -- and it could happen -- that PII gets through.

So you'd want the companies making some effort. You'd want the NSA to have a system to strip that PII before it got into the analytical database, which is easier for you to do, I would argue, than the multitude -- thousands of companies trying to share malicious source code that may have originated in Russia or China or Iran or North Korea or some international organized crime element.

I just want to make sure we have that full and open discussion about what that looks like and why there are concerns about limiting the number of companies that could participate. It just adds more vulnerability to the whole system.

ADM. ROGERS: Right.

REP. ROGERS: So I just want to make sure we've made that clear and it was on our record.

ADM. ROGERS: Yes, sir.

REP. ROGERS: Admiral, you are saved by the bell. The vote -- the vote clock shows zero. But again, I want to thank you for your service to the country. Thanks for stepping in at a difficult time. Thanks for improving the morale of the NSA folks. And I hope that you'll take back -- as a committee that in a bipartisan way does pretty tough oversight -- I think you've seen that already --

ADM. ROGERS: Yes, sir.

REP. ROGERS: -- that we have the utmost respect for the work that they're doing and thanks for their patriotism and staying on mission despite what they might read in the newspapers.

So thank you, sir. And thanks to the men and women of the National Security Agency.

ADM. ROGERS: Thank you, sir.

REP. ROGERS: Thanks.

(END)