

***Fordham University's Fifth International Conference on Cyber Security
(ICCS 2015)
January 8, 2015
New York, New York***

Special Keynote Address

By

ADM Michael S. Rogers

Commander, U.S. Cyber Command, Director, National Security Agency, Chief, Central Security Service

Moderator: Joseph M. McShane, S.J.

President, Fordham University

Excerpt from the introduction by Joseph M. McShane, S.J./President of Fordham University:

The admiral, a native of Chicago, of Welsh extraction, he has been a flag officer since 2007. He served as a director of intelligence for both the Joint Chiefs of Staff, United States Pacific Command, and most recently as commander of the United States Fleet Cyber Command, United States 10th Fleet.

While his naval background assures us that he knows his way on the seas, his education, from Auburn University, a graduate with distinction of the Naval War College, and a holder of a masters of science in national security strategy, shows he knows his way around the cyber airways as well. He's a truly extraordinary man, and someone whom I do admire. I've only met him once, today.

But he's a man of great integrity. He's a man of great devotion to our country, and a man who thinks on his feet and is not afraid of a challenge. He is, after all, a man for whom character formation has been a part of his life from a very early age: a Cubs fan, a native of Chicago, but a man who serves our nation with great bravery, great tact, great wisdom, and great savvy.

I give you Admiral Rogers.

ADM MICHAEL ROGERS: I don't think I've ever had the expectation set so high for me in a public environment ever.

Well, father, for the team here at Fordham to the FBI to all of you who put this on, this is the fifth conference, I thank you for doing that. And I thank you for what you have created: an opportunity for a broad spectrum to come together on an incredibly complex and difficult set of issues.

You good?

All right. This is kind of neat.

(LAUGHTER)

I apologize if I play with this a little for the course of the discussion.

(LAUGHTER)

Yeah there you go.

I've never been in a big city before.

Yeah, if I could, I'd like to make this a little interactive, so what I intend to do is I'll talk to you for a little bit, but I'm much more interested on what is on your mind.

I would be interested, first: how many of you come from the academic arena?

So, probably maybe a little less than 10 percent.

How many of you come from private industry?

A pretty broad swathe. Not surprising in New York.

How many of you come from the government in some function?

How many of you come from the media?

All right. OK.

How many of you have a law enforcement background that brings you here today?

Look at that. Do not violate the law in the next 50 minutes. That would be bad.

The reason I asked that is the first point I would make to all of you is this conference is a vivid example of a fact that cyber is the ultimate teen sport to me. In the 33 years that I have been a commissioned officer in the United States Navy, I have never worked a problem set that had greater complexity and at the same time, the success of every one of us is so driven by the behaviors and actions of others. That is a great challenge.

Our ability to succeed here is going to be largely predicated, I believe, on our ability to create strong teams: teams that bridge a lot of traditional divides. I'm talking here today: I'm a uniformed guy from the Department of Defense.

My primary responsibility as the commander of U.S. Cyber Command really are three-fold: it's to defend the department's networks, so like many of you here in the private sector, I'm tasked with defending the networks of a large global organization that is both fixed in mobile locations, that works in both permanent and rather expeditionary kinds of things, that works at multiple classifications levels and in multiple formats and multiple forms.

Secondly, as U.S. Cyber Command, we are tasked with generating the cyber mission force that the department is going to use to execute its cyber operations from the defensive to the offensive side.

And thirdly, U.S. Cyber Command's final mission, to, if directed by the president or the secretary of defense, to defend critical U.S. infrastructure.

That last one is a very interesting one, given where we are right now. We have traditionally defined critical infrastructure for governmental purposes, 16 different segments that address those areas that damage to would potentially result in significant implications for our nation's security.

So think about power, think about water, think about aviation, think about the financial network. There's 16 different segments. We clearly did not put the motion picture entertainment industry in one of those 16 segments.

(LAUGHTER)

And yet we find ourselves in a situation where we've had, for the first time, offensive, malicious act by a nation-state specifically designed to achieve a coercive effect. In this case, stop the release of a film with a particular viewpoint or characterization of a leader. There's a lot of question, there's a lot of implications in that for us as a nation.

So, what is the role of government? Is it beyond this 16 segments, so to speak? Is it, we're going to treat cyber purely as a law enforcement issue? Is it -- is this a broader national security issue for us? I'm going to talk about that a little bit more in a minute or two.

The second job that I have, and the one that generally, to be honest, tends to get the most attention, is the director of the National Security Agency.

NSA has two primary missions. One gets a good deal of attention: our foreign intelligence mission. The one that perhaps in some ways is more critical to our discussion today is the fact that the National Security Agency is charged with an information assurance mission.

In that information assurance mission, we develop the cryptographics and security standards for the Department of Defense, we partner with other elements of the U.S. government to do the same thing for the U.S. government writ large. We provide analytic capability to develop insights to help defend against cyber activity, developing the signatures that we use to identify so we can load those into our systems, as well as we share that with the private sector, so you recognize the activity that's being directed against your networks.

We develop the countermeasures, if you will, to major viruses. So, if it's Heartbleed, if it's fill in the blank, if it's the specific malware, for example, that we saw used in the Sony scenario: we're partnering with others, using our technical expertise to write the programs that will counteract the ability of the malware to be effective.

Those are pretty significant roles for the nation, and we do it partnering with others. We, too, are part of a partnership, a team. That team from the -- from the U.S. government, the Department of Homeland Security generally in the lead, and (OFF-MIC) partnering with the Federal Bureau of Investigation and the law enforcement role here.

And I would compliment -- I always try to compliment my FBI teammates. You had the opportunity to hear from many of them over the last few days. They are a true asset to the nation, and I'm very honored to be able to partner with them.

So, two different jobs, slightly different roles. But in some way, all very much focused on this idea of so, how are we going to defend our systems? How are we going to generate capabilities that give us options to not just sit here and respond passively, or after an event to something that's happened? And harnessing the power of the government, the Department of Defense, in this case, in its broader mission of defending the nation. And so how are we going to do that?

I think there's a couple principles to how we're going to do that. The first is this idea of a team. We have got to create partnerships that bridge the divide between the private and the government. One of cyber's biggest challenges, I think, for all of us is that it forces us to look at problems in very non-traditional ways.

I'm a uniform. I come from the Department of Defense. One of the ways we often bin problems, if you will, at DOD is by geography. That's why we have a Central Command that deals with the Middle East, we have a Pacific Command that deals with the Pacific. Cyber doesn't recognize geography. If you just look at recent events, pick almost any significant hack, you watch the way it moved almost literally around the world to achieve the desired effect here in the United States, the idea that we're just going to treat this as some very regionalized or local problem is just not going to work.

Because of that, one other category for you guys. How many of you are international or from outside the United States? Another comment that I would make: this is not a U.S.-only problem. And the solution to these challenges are not going to be U.S.-only.

For many of you in the private sector, you live this challenge every day. You are a part of globally-based, transnational organizations that have either components, partners, subsidiaries that span the globe. And we've got to come up with a structure that enables us to do this in an international way.

The second challenge, I think, and we talked about this whole idea of partnerships, is I need your help in trying to send a broader message about why and how important that partnership is. It can't be just the government saying, you know, we really need to work together. I need you saying the exact same thing.

What I think I should be tasked to provide is -- so help me understand what's going to be coming at me, what is it going to look like, what are the kind of precursors of activity that I can expect before that

malware shows up, because all of us who know who work in the defensive cycle, there's a multitude of steps that an attacker goes through before we finally get to the end-state where the malware has been activated and has gone destructive. There's a whole host of steps that you have to go through.

Those of us in the profession, we understand that to make this work, again, I think we need the private sector articulating, "look, we have got to work this together." So, what I think I'm going to provide is insights as to here's what I think is coming at you, here's what I think it's going to look like, here's the characteristics of the malware, here's the tactics, techniques, and procedures I think that these groups, nations, individuals are going to be using, and here's what I think you should look for.

What I think I need from you to really be effective here is, so, is what you saw what we indicated?

Hey, have you seen something we have no clue about?

How did you configure your networks? What was effective? What worked? What didn't work?

What kind of precursor activity did you see that in hindsight, you say to yourself, I didn't realize it at the time, but these were really the first indicators that something was coming at me?

And invariably, on almost every million (ph) penetration I have ever dealt with, in the post factor analysis, there were always indicators. But normally, oftentimes we just don't pick up on them. And that's not a criticism against anybody. Like I said, I've defended networks, and I have, myself, at times, failed to achieve my objective. That is a terrible feeling.

Nothing quite like being an individual and having to tell your boss, whether you're a CIO, whether you're a CEO, and you're having to tell your boss, shareholders, "I've failed. They got in. And here's what's happened."

I don't like those, all right? Those days when that happens.

But we're going to need to work together on that. And so I think there's value that each of us can provide to help the other. Because if we think, I believe, that the private sector can withstand the efforts of nation-states who are determined to gain access to potentially steal intellectual property, to protect -- to potentially damage or destroy, as we saw in the case of Sony, some of you are infrastructure. I don't think it's realistic to expect the private sector to forestall that or deal with that totally by themselves.

Likewise, I don't think it's realistic to say, "Well, that's a government responsibility. They'll take care of that. I have no responsibility to defend my information. I have no responsibility to defend my networks. I'll count on the government to do that for me."

I don't think that's realistic either.

You know, we have got to bridge this divide. And, let's be honest with ourselves. This is all occurring at a time when the trust is not as high as it needs to be. I think that every day in some ways as the director of the National Security Agency, if I'm honest with ourselves.

We have got to decide as a society, as a nation, how are we gonna move beyond that, because I think, when I look at cyber, to me this is a national security challenge. It's not a private sector issue; it's not a government issue, it's a national security issue for us.

That requires us to think more broadly and to ask ourselves collectively as a society and a nation and partnering with those of other nations, how are we gonna deal with this. Because this is not a short-term phenomena, it's not a phenomenon that's gonna lessen in its intensity, I believe, in the near term.

What we've seen in the last six to nine months in general to me is just, when you look at some of the major intrusions in the financial sector, in the commercial sector, when you look at the destructive action we saw with respect to Sony, the trends are going in the wrong direction.

So doing more of the same and expecting different results, my military experience tells me is not a particularly effective strategy.

I'm interested in what can we try to do differently. Among the things I think we try to -- we need to try to do differently is building that partnership between the private sector and the public sector, the important role that I think legislation could play here.

You know, I think there is value in the Congress enacting legislation that helps to facilitate the sharing of information between the private sector and the government. I think a legal framework that provides a measure of protection in the liability arena is important to us.

You know, many of the individuals, the leaders that I partner with in the government, often have senior roles outside the government in the private sector. Many of them were general counsels for some of the largest companies in the United States. And I'll often asked them, so, tell me, when you were the general counsel of a large brokerage firm, when you were the general counsel of a large defense contractor, what advice did you give your board of directors, what advice did you give your C-suite (ph) when it came to what should we share with the government, what should we acknowledge, what should we provide to others?

And they're very quick to say, hey, look, liability is always a significant concern. Be very careful about engaging actions that open you up to the potential of suit. We've got to try to overcome that.

The voluntary role that -- approach that we have tried to date, while it has certainly gotten better over time, it is not gonna get us where we need to go.

There's just too much activity, there's too much going on, and the scope of it just keeps increasing.

I don't think it's in our best interest to just sit here and take it (inaudible).

Another point I would make is a strategy that is predicated purely on a defensive or post-facto response, probably not gonna get us where we need to go.

The whole idea of deterrence, trying to ensure nation-states, groups and individuals understand you don't want to engage in this behavior, either because -- there's two ways to deter in my experience: Either you lead an individual, group or a nation-state to believe that they don't be successful in doing so or in trying to do so, and there are steps that we've all taken to try to do that, or the second component is,

you try to convince those same individuals that the cost isn't worth it, that while you may be successful, the price you'll pay for doing it is not one that you want to go through.

Either we incur -- we reduce their ability to achieve their desired outcome, or we impose such a cost that they don't want to do it.

We've got to get to an idea of deterrence, because when I look around the world right now, my conclusion is that nation-states, groups and individuals seem to have come in large measure to the conclusion that there is little price to pay when engaging in these behaviors that are leading to among the greatest transfers of intellectual property and knowledge we have ever seen, the outright destructive activity we've seen in the Sony issue, for example. Those are all bad trends for us.

We have got to create the idea of deterrence. We have got to create the idea of norms about what is acceptable and what is not acceptable. And we need to do that on a broad, international basis.

Now, we'll continue to try to work our way through that as a nation, but I think the immediate challenge for all of us in this room is, you know, that's great, but what can we do right now? What's within my span of control? What's within my set of authorities? What can I try to do, today?

The thing is -- as a, you know military leader, my culture tells me, and I am constantly telling the team, both at Cyber Command and the National Security Agency, is stop focusing on what we can't do and let's talk about what we can do to try to help our nation within the constraints we have. Let's try to be creative here.

And we always obey the rule of law. We always remain accountable to the citizens of the nation we defend. When we make mistakes, we're very public and we acknowledge those mistakes. And we don't ever cut corners. Those are the four touchstones, for example, that I always remind the workforce at the U.S. Cyber Command and the National Security Agency, don't ever forget you obey the rule of law, you remain accountable to the citizens that we defend, we don't cut corners, and when we make mistakes, we stand up and we acknowledge that we made a mistake and we ask ourselves what have we got to do to make sure we don't make that mistake again.

Within that, I then challenge the team to tell me what's in the realm of the possible, what do we think we can do. Because I'm always much more interested in don't talk to me about what we can't do, talk to me about what we can.

I think when I look at the environment here in New York City, when I look at the ability to bring together such a large group, international, domestic, government, private, academic, business, that's a pretty powerful combination. New York City is a great laboratory to me. You know, what are some of the things that we can do within the realm of the possible to (inaudible)?

Now, I'm just one part of that team. You know, the Department of Homeland Security has the overall lead in the federal government for our interaction more broadly in terms of cyber across the nation. The Federal Bureau of Investigation has the lead in cyber in terms of law enforcement. They're not the only law enforcement entity, the Secret Service also has a role to play.

You know, I'm the lead within the Department of Defense, so to speak, at the operational level about how do we make this work, as the director of the National Security Agency, how can we generate

insights that help us understand what people and groups and nations are doing in this environment. And how do we apply NSA's technical capabilities to help generate the solutions that overcome some of these, develop the signatures that help us identify the activity, to develop the software that we can write that tells us how we're gonna defeat this malware.

And, with that, what I thought I'd do is I'm much more interested in what's on your minds. So what I'd like to do then is just take whatever questions that you all have for me.

(CROSSTALK)

MODERATOR: OK, Admiral, we have three questions.

ROGERS: And I'll take -- I'll take more from the audience (inaudible).

MODERATOR: OK.

Where do you see the cyber-world in the next five years and then the next 10 years?

ROGERS: So, in the next five years, let me look at it from a challenge perspective. The challenge that concerns -- the challenges that concern me in the next five years is does the line between actions by nation-states, groups and individuals start to blur, and do you start to see, for example, nation-states turning to criminal actors, turning to surrogates, turning to others as a vehicle to, number one, try to complicate our ability to do attribution, identify who conducted the act, number one.

Number two, the mobile side, is an area that I would tell you, man, just scares the heck out of me. You think about how that hand-held, mobile, digital device has become so integrated into everything we do. I mean, literally, is there anyone in this room who doesn't have a personal digital device with them?

These have become so integrated into what we do, not just in our day-to-day, everyday private and personal lives, but I carry a digital device for work with me wherever I am. Many of you do the exact same thing. We have become so dependent on these. And that's - so the second thing I articulate when I look at challenges in the next five years is how we're gonna deal with the mobile and the hand-held, you know, digital devices.

The next challenge in my mind is how do we move from where we are right now in the whole idea of trust and partnership to a point where we can get beyond, hey, I'm good and you're bad, and so a much more, hey, can't we have a dialogue about some substantial things, like what does -- as a nation, what does privacy in the digital age really mean?

Because if you think that the use of big data to understand personal behavior is a phenomena associated with intelligence, I would ask you, what world have you been living in for the last 10 or 15 years.

It is so foundational in both the business sector, in many ways, as well as in the world I live in, that I think we really need to have a broader dialogue as a nation about just what does privacy mean in the digital age, and what are we comfortable with as a nation.

Because, in the end, to me, it's all about striking that right balance. It's not either/or. We've got to do both. We need to understand that at its fundamental structure as a nation, we are about privacy and the rights of the individual. It is the cornerstone of our entire construct as a nation.

At the same time, we've got to recognize there are very valid concerns about how are we gonna ensure the security of our nation and our citizens and those of our key allies.

How are we gonna do it in a world where increasingly where illegitimate, where illegally minded individuals, as well as those terrorists and those nation-states, are all on the same coms paths, using the exact same software, using the same applications?

You're a different -- when I first started this business, when I joined and started as a signals intelligence kind of guy, 30 years ago, boy, it was easy to tell those nation-states and groups. They used unique communication paths, often developed by nation-states that were very separate from the infrastructure that -- what we used as private citizens.

I'm using the same software at work that I use at home in my personal life, and that ain't unique to the National Security Agency or the Department of Defense or the United States cyber-community.

So how do we deal with the fact that the coms infrastructure that we all rely on has fundamentally changed; it has now become one huge path that a wide variety of actors, some doing very legitimate, very valuable things -- I count on my ability to talk to my family wherever I am. I count on my ability to have a private and secure conversation with my children and my wife wherever I am. I count on the ability to engage in banking and do the other things that I want to be able to do in my life wherever I am.

At the same time, how do we deal with the fact that we are living -- the events of the last 24 hours in Paris, before Paris, you look at Sydney, you look at Ottawa, you look at London, you look at Madrid, you look at Washington, D.C., you look at Shanksville, Pennsylvania, and you look at New York City.

Every single one of those instances, we will find -- the other cases, we know, but I suspect we'll find in the Paris situation -- there was some measure of coordination using the same exact paths that all the rest of us use.

So how are we gonna deal with this?

The way to deal with it is not to say, well, they're inherently bad, and I'm good. Or, hey, you NSA guys are all bad and the rest of us are all good.

It's about as a nation, as a world, how do we strike that balance? How do we ensure the security of our cyber-systems that we're all counting on? How do we do it in a way that ensures the security and the privacy of our citizens and those of others around the world?

That's a hard question, but it's an important question for us as a nation. And, as I remind the workforce that I'm responsible for, be grateful that you live in a nation that is willing to engage in that kind of dialogue, because there's a lot of nations around the world where, quite frankly, the oversight of what intelligence structures do, the kinds of discussions that I've argued that we need to have, they would never happen.

They would never be discussed. You'd never even question. The government would just do it.

That's not what we're about. I think it's a real strength for us as a nation.

But for those who would argue, well, you don't have to worry about that stuff. The security piece, this threat piece is all overblown, I would say, what world are you living in?

Now, you're not gonna see me running around arguing that because of the real demands we have to achieve a level of security in the world we're living in, that that means we ought to override our freedoms. You will never hear me say that, because I don't believe that. I believe that we can strike that balance, that we can do it in a proactive, transparent way, that our society and those of our allies and friends can feel comfortable with.

But it is a challenge, because we're all good and bad, we're all out there using the exact same communication paths, the exact same softwares, the exact same social media. We're all out there together in this.

You saw that if you -- excuse me -- some of the forensics that we observed in the Sony situation, for example, you saw that same public infrastructure.

The other concern I have when I look at this potential -- to go to your question, back to your question, Jeremy (ph), about -- the third major trend that worries me is we're gonna go much more destructive.

To date, the destructive acts directed against U.S. infrastructure have been relatively limited. Sony's the most visible. It's not the only one, but the numbers have been very small.

But the trend's going the wrong way and so, in five years, my concern would be this is only gonna increase.

Again, if you don't change the dynamic, this is only going to increase.

What concerns me about that is a couple things. Number one, if we don't collaboratively work together to address how we're gonna deal with this, I'm concerned that many in the private sector will say, hey, look, if the government's not going to be there to help me here, then I'm gonna do what I need to do to protect my networks.

And then we'll start to get into hack-back (ph), we'll start to get into the offensive side in the private domain. And my concern there would be be really careful about going down that road. We will fratricide each other in the cyber environment. We will get into second and third-order effects.

And you tell me as a private business entity, what are you going to do when you decide you want to hack back, some nation state or group sees that and then decides that they're going to take the fight to somebody else.

And then somebody else says, "Hey, wait. I'm only dealing with this because of what you did. Now I'm going to sue you. I'm going to try to hold you accountable."

This is a really complicated, really slippery slope. So it's another reason to me why I think we have to deal with this phenomenon that I think we'll increase in the next five years, an outright destructive action directly against networks.

The other thing that concerns me in that regard, also to be quite honest, is Sony was important to me because the argument I made was the entire world is watching how we as a nation are going to respond to this, and if we don't acknowledge this, if we don't name names here, it will only, I am concerned, encourage others to decide, "Well, this must not be a red line for the United States; this must be something that they're comfortable and willing to accept."

That couldn't be further from reality, I think, for all of us; it's unacceptable behavior.

We need to develop those ideas of deterrence, those norms that clearly communicate to the world that those are unacceptable behaviors and if you engage in those behaviors, there will be a cost that you will have to pay, a cost designed to lead you to, "You don't want to do this," and designed to lead others to come to the same conclusion. You don't want to go down this road. You don't want to engage in destructive behaviors. It's an important dialogue we're going to have work our way through.

The other thing, then, I think, that flows out of this is, so, what's the role of the government in all this? Are we going to treat it as a criminal act? It'll just be law enforcement? FBI, for example, Secret Service, others deal with that.

Is it an attack against any U.S. company, or pick the criteria you want to use? Will it be, well, the damage has to arise to a certain level. Pick a dollar amount.

Is it the damage has to cross a certain threshold, for example, the first -- violation of the First Amendment, our ability to -- artistic freedom or our ability to express our opinions as citizens? What's the threshold that we want to set?

But we need to have that dialogue. What is the threshold? I think we need to clearly articulate to others what that threshold is. People understand what's in the "acceptable," what's in the "not acceptable" area.

It is complicated hard work, and it takes much longer than you'd ever like, as it is so complicated.

And you, as citizens, as members of the business community, as the academic world, you need to help us work our way through. So what -- how do you do it? What makes sense? What doesn't make sense? It can't be just guys like me, others in the government just deciding, well, here's the right answer.

The dialogue, the discussion's got to be much broader than that. That's one of the reasons why I think forums like this become so important.

The last part of your question was 10 years, right? So what if I look out 10 years?

Well, the first thing I would tell you as an intelligence officer, I have not had a great rate of success predicting activity 10 years out.

I once worked for -- as you heard in the introduction, I was the director of intelligence for the Joint Chiefs of Staff, so I was the intel officer for the secretary of defense and the chairman of the Joint Chiefs.

During my time in that job, Arab Spring kicked off. My former chairman boss loves to remind me, "So, how about this Arab Spring you didn't tell me about, Rogers"? So I'm always a little leery about trying to predict 10 years down the road.

What I hope happens 10 years down the road is we had managed to develop a set of norms for behavior in a cyber environment, but we have managed to create this idea of deterrence, that we have created well-established and well-moving partnerships back and forth and the flow of information is ongoing and regular.

Another thing my military experience teaches me is you can't show up in the middle of a crisis and suddenly decide, "OK, hey, I'm here to help you. So could you tell me how you're structured? What's your network look like? Hey, what do you need from us? What's important to you? What do you care about"?

My military experience teaches me you train and you exercise, and you do it on a regular basis, so when you get into that crisis situation, all the participants understand who's going to do what. You understand how you're going to do it. You understand how you're going to communicate. You understand how you're going to pass information. You're going to understand what information you're expecting from each other in what format via what means.

That's what the military culture is. You always train and exercise, and you do it over and over again, so when it's game day, you are ready to go and not discovering or -- as a military guy, discovering, learning, moving to contact is an incredibly costly way to learn. I don't want to learn that way. I would argue that I don't think we collectively want to learn that way.

So that would be my hope for 10 years. What's the next question?

(UNKNOWN): OK. (OFF-MIC)

What are the great opportunities -- for example, social media, big data, network mapping -- for enhancing intelligence support to cyber space operations?

ROGERS: So, the ability to harness the power of big data analytics probably is number (inaudible).

I always remind my team, look, data is interesting, but what we really value is knowledge and insight. Data is a vehicle to generate knowledge and insight, but in and of itself, data isn't what this is all about. We got to use data as a tool to get to something else. We got to figure out what's the best way for us to do that.

Big data analytics are a very powerful tool. When I look at what we're able -- the insights we're able to generate today through the ability to harness and analyze and look for patterns in tremendously large masses of data versus the way it was when I first started in this business 30 years go, it's just mindnumbing to me at times.

I think that's one of the key (inaudible).

I think as an intelligence individual, harnessing the power of open source I think is very powerful.

If you just take what happened in the Ukraine, you know, I've got a nation state arguing, "Hey, we're not pushing weapons into the Ukraine," and we're going, "Well, let me show you a poster from an individual and fill in the blank (ph) location, and these are -- this is your equipment crossing the border.

"Remember, it's got a GPS flag, got a location, got a time. I didn't do that as a government. A private individual did that and made it a matter of public record open to the world."

That becomes a very powerful tool to attempt to generate insights as to what is happening very remote -- on a global basis.

Now, there's a flipside to that, and I'd be the first to admit, we're trying to come to grips as an intelligence community about, "Well, what's the right -- what's the right balance"? Is it, hey, anything that anybody posts in social media should be open anybody, to include the intelligence arena (ph)? We're walking our way through that.

Overlay that in the current dynamic that -- that we're in right now, that is a little complicated. But we're trying to work our way through it.

What was the third one, George? I apologize (ph).

Network mapping and then the ability to -- in addition to network mapping, I think another big thing that's going to help us all collectively is visualization tools.

The reason I say that is man is a visual animal. It's the way we're genetically engineered. In my experience, it tends to be what we tend to respond to. It tends to facilitate decision-making. It tends to enhance understanding.

We have got to come with -- and it's certainly something that I'm pushing our team about -- how do you generate a visual map of -- of the challenges we're talking about?

Put another way, you tell me how -- how you defend something you can't see?

I mean, as a military commander, I'm used to the idea of walking into this nice, dark space with a series of screens that overlay symbology on geography and enable me to very quickly assimilate who's out, what are they doing, and it helps me to start pretty quickly assimilating some pretty complex scenarios and to start thinking about what are the decisions, what are some of the choices that I need to make.

We've got to get to that in the cyber arena. We've got to be able to visualize the activity and this domain, because there is a whole lot of activity, some of it, very valid -- most of it, very valid, and the last thing we want to do fratricide each other when we're attempting to defend ourselves.

(UNKNOWN): OK. Last question: What kind of skills are in demand for Cyber Command, and how can we apply, and do you only hire entry-level or experienced security people? (inaudible) recruiting.

ROGERS: So, Cyber Command has both civilian employees and military employees.

At NSA, conversely, the ratios are a little different. U.S. Cyber Command, we're largely a military organization.

As such, you got to join the military. You got to meet the same -- if you want to go the uniform route at U.S. Cyber Command, you got to meet the same standards of anybody else in the military.

That's an interesting question that we're trying to come to grips with. Is that the right model over time?

And by using that model -- and I'm sure it's the same for all of you, because one thing that unites us here -- and I have this discussion out in Silicon Valley all the time -- we're all going after the same people for our workforce. We're all interested in the same fundamental talent, and we're all interested, in many ways, in the same fundamental skill sets and experiences.

For me, our model in the department is I will generally get very young people. They'll have a baseline of education and -- and not unlike many of you -- then we'll provide them the additional training and experience they need to get them to the level that -- that we find we need.

Our model in the uniform world is I don't bring somebody in who's got 10 years experience, 15 years experience and multiple other businesses. That's not the uniform model.

But that is a question for us. We're trying to ask ourselves, so what is the right model for the uniform cyber workforce of the future?

The positive side for us right now is we have been able to meet every one of our targets in terms of assessing or recruiting people, and we're retaining people at a very high level right now within the cyber workforce.

Now, that's because the argument I make is it will never be about money. The Department of Defense is not going to be able to compete when it comes to salaries with many of our private partners, teammates, counterparts.

Where are we going to be able to compete?

Number one, the idea of serving something bigger than yourself.

Number two, the idea of doing something that directly contributes to the defense of the nation and its citizens and allies around the world.

Number three, doing stuff that is really neat, quite literally at times, you know, you shouldn't be doing anywhere else.

We're going to be giving you the opportunity to travel. We're a global organization just like many of you. So, if you like moving around, if you like seeing lots of parts of the world, we can do that for you.

And then perhaps another edge for us, we're going to give you responsibility at a very young age. We'll train you and we're going to put you in both technical and leadership roles and we're going to give you the opportunity to push yourselves. That's our edge. It's never going to be money. It's -- it's never

going to be, "Hey, we guarantee you you're going to work on that very latest, most cutting-edge tech knowledge. That's not how we're going to work through (ph) or how we're going to retain the workforce.

Well, if you want to be part of that workforce, you know, I'd be glad to sit down and talk to you afterwards. But we need motivated young men and women, just like everybody else. The (inaudible).

Now, any questions from the audience? Please, the least I can do.

Sir in the sweater. And I'll repeat -- oh. Go, you, sir, in the sweater. Then we'll switch over. And I'll repeat the question.

QUESTION: (OFF-MIC) (inaudible)...

ROGERS: So, the question, what do you think about -- and you tell me if I've -- if I've failed to paraphrase it. So, what do you think about the idea of border control in the cyber domain? And what should the role be in that regard? And the example was, "Hey, look, when I'm looking at malicious IPs, trying to figure (ph), would I be filtering these?"

You know, depending on the port settings you want to, "Hey, should my ISP doing this? Hey, should government be doing this?"

You know, my first comment would be a hard concept to really -- to really implement, just given the nature of the structure of the net and the flow of communications.

I certainly urge -- one of the things that we generally will share with people when we go look at companies when we're talking with others, and what we ourselves -- I very much pay attention to IPs and where they originate. And I aggressively use that as a criteria. I use -- when I decide what traffic do I want entering our networks, and from where, I use that criteria all the time. I want to urge others to consider using that as a defense.

Now, you just got to realize there's tradeoffs. So, you got to ask yourself, is it valid traffic? Is it not? How does that fit into a broader strategy? Because in and of itself, it doesn't get -- guarantee you. But if that's the only thing you're going to do, then, hey, congratulations. You've assured the defense of your network.

But it would be a little difficult, I think, in some ways to act irrationally (ph). There is something that we -- sir?

QUESTION: (OFF-MIC) (inaudible) hedge funds feel like they're monkeys -- feel like they're a monkey in the middle when it comes to business internationally. Data collection, data protection. Their U.S.-domiciled. They have offices in London, in Paris, in Cairo, In Hong Kong, in -- in France. And they are petrified -- and we get this question every day -- what happens if we have a breach in London or in Germany? And we're a public company. We need to fix it and we need to fix it fast.

Do you foresee -- or would you foresee in the future some sort of international norm or standard of -- of cyber security and business continuity, as opposed to U.S. companies being hamstrung -- I'm not saying this in a bad way -- having -- having to deal with privacy issues at the same time. Because the

converse to U.S. companies is loss of enterprise value, loss of shareholder value. And maybe enterprise death, if we can't fix the problem.

ROGERS: Well, the first comment I would make is, now we're really into some deep legal territory. And asking a serving -- asking a Navy guy, "Hey, you're -- you're not a lawyer, but you stayed at a Holiday Inn. Hey, what do you think about" -- I'm not the one most qualified to give an answer. I'll give you an opinion. But I predicate that with the idea, I'm not a lawyer. And this really, in its heart, is a question about the law and policy.

What I would hope over time is, this would be part of that idea about how do you generate or develop those seven norms? Because this is not a short-term phenomenon. It's been this way for a while, and it's only going to get more complicated.

So, the idea that you can somehow segment off portions of the network, for example -- I don't think, broadly, that's in everybody's best interests. You want to be able to quickly move ideas, information services across that network. And you want to do it on a global basis, I think, as a citizen. I think that's in all of our collective domestic interest.

Going up all the way in the back, sir?

QUESTION: (OFF-MIC) First, Admiral Rogers, I would like you to speak -- I'm sure you (ph) must have opinions on (ph) (inaudible). And hopefully, Father (ph) (inaudible) won't begrudge you for doing that. But thank you for your service to this nation and -- and for what you're doing for us.

I wanted to comment briefly just on the Sony situation. You know, there's been a lot of talking over the day -- the last couple of days about who actually perpetrated it. But let's assume, for the sake of argument, we all agree that North Korea played a role. You talked about making the cost not worth it. You talked about, you know, there's much more destructive things to come.

What, in your opinion, should be the response of the United States to discourage other nations from doing more destructive things? Because as private entities, we will never be able to -- to take any kind of actions in that particular regard.

ROGERS: Jack's (ph) out (ph). First of all, I very much agree -- and, you know, as part of those discussions, was very -- believed strongly, we must publicly acknowledge what has happened, and we must publicly attribute what has happened to the nation state in this case that did it. And we need to do that as a nation. And if we don't do that, there's lots of other nations, lots of other groups, lots of individual actors out there watching to see what we're going to do. And if we don't do anything -- if we don't acknowledge this, I'm concerned it would have the unintended consequence of potentially leading others to believe, "Well, this must be acceptable behavior."

The second thing I think is important was, I very much agree with the idea of not only publicly acknowledging that it happened, publicly attributing it to who did it.

Again, as you have heard, I have very high confidence -- I remain very confident -- this was North Korea.

The next thing that I think was important was a reminder -- merely because it happens to us in the cyber realm -- I mean that our response has to be focused in the cyber. If we're going to deter, for example, then we got to think much more broadly. And we got to ask ourselves, what are the full range of capabilities that we can bring to bear to help convince people, you don't want to -- and nations -- you don't want to engage in this behavior. So, the economic lever is -- in this case, as you're aware, the U.S. government announced a series of sanctions against two entities and 10 individuals within North Korea.

Secondly, I -- or thirdly, I thought the thing was important here that we also talked about, that this would be something that we would -- a series of actions that we would take over time in a proportional manner at the time and place of our choosing. But, hey, merely because something happens today doesn't mean we have to immediately tomorrow respond, and we have to immediately respond in the exact same manner. I don't think that that is the -- potentially the most effective. I think we need to look at a broader set of options.

And so, I -- I was very happy to see what ultimately, we as a nation decided to do. We'll see how this plays out over time.

I'd (ph) only remind you, North Korea is a nation that has sunk a sovereign warship of South Korea. Has engaged -- has detonated multiple nuclear weapons and has launched multiple intercontinental ballistic missiles. This kind of provocative behavior is not inconsistent with a pattern that we have observed over time.

(UNKNOWN): OK, last one. One more.

ROGERS: They're ruthlessly efficient.

QUESTION: Hi. Noshak -- Noshak (ph) with The Daily Beast.

I'm wondering -- we've heard a lot about the FBI's role and the Justice Department's role in the Sony hack. I'm hoping you can talk a little bit about what NSA's role was, particularly the I.A. Division, if at all. That's...

ROGERS: So, I would only say in broad terms, we partner with the Department of the Homeland Security, the FBI in many scenarios. This is one scenario where we specifically did. We were asked to provide our technical expertise. We were asked to take a look at the malware. We were asked to take a look at not just the data that was being generated from Sony, but also what -- what data could we bring to the table here. "Here's other activity and patterns we've observed from this actor over time."

So, yes, we were a part of a broad inter-agency effort. Not in legal. The Federal Bureau of Investigation had the overall lead in terms of interacting with Sony. But yes, we were part of a broader government attempt to understand exactly what happened.

And with that, I thank you all very, very much for your willingness to wait (ph). And...

(APPLAUSE)

Let me just conclude, if I could, by thanking you.

First of all, I remind people, you don't have to wear a uniform to serve. It took me a long time in my military experience to teach me that. To remind me of that. You don't have to wear a uniform to serve.

Many of you serve the nation in broad ways. And I thank you for your willingness to do that. I thank you for your willingness to spend time on a cold day in New York in the winter here, to come together and spend some time thinking about how are we as a nation going to come together and as -- with a set of international partners, how are we going to come to grips with one of the most complex issues facing us today? How do we achieve security in the cyber domain in this complex world we're living in with this technology that constantly changes, with a blurring of lines between the private sector and the public sector increasingly, from a technology standpoint, are really blurring? And how do we do it in a way that ensures we both achieve a level of security that's acceptable to the nation, and we do it in a way that is consistent with our values with respect to privacy and our civil rights?

That's not a -- an easy challenge. And it's one I think that's important to all of us. So, I thank you for your willingness to be part of that dialogue. And in the end, (inaudible) all of us, the key to success will be our ability to operate as a team. And you cannot operate as a team when you start from a position that vilifies each other. We have got to work together. And it can't be, "Hey, one of us is good and one of us is bad. One of us is focused on money, one of us is focused on service."

We're each part of a broader team. We've each got a role to play, but we each bring capabilities that, when brought together, can achieve greater good for the nation. And that's what matters to me.

So, I thank you very, very much for your time.

#####