

National Security Agency

Reagan National Defense Forum: Building Peace Through Strength for American Security

Panel Session 6: “Cyberwar: The Role of Cyber in the 21st Century Warfare”

**Moderator:
Thom Shanker,
The New York Times**

**Speakers:
Senator Roy Blunt (R-MO)**

**National Security Agency Director and U.S. Cyber Command Commander
Admiral Michael Rogers**

**Wes Bush,
CEO and President, Northrop Grumman**

**Michael Allen,
Managing Director, Beacon Global Strategies**

**Time: 1:45 p.m. PST
Date: Saturday, November 15, 2014**

*Transcript by
Federal News Service
Washington, D.C.*

ANNOUNCER: Ladies and gentlemen, welcome to Panel Session Number 6,
“Cyberwar: The Role of Cyber in the 21st Century Warfare.” Please welcome our moderator,

Assistant Washington editor, Washington Weekend editor for the New York Times, Mr. Thom Shanker. (Applause.)

SENATOR ROY BLUNT (R-MO): You're the only one that gets the voice.

THOM SHANKER: Exactly. Right. (Laughter.) Yes, I have the floor at least for an hour.

Thanks, and welcome to all of you to this panel discussion. The cyber issue is far more broad than cyberwar. It's an honor to be asked back for a second time, and I think we have a terrific panel discussion in store for you today. Clearly, this topic is one of the very most important on the national security agenda. Look at the size of the audience today, standing room only for this discussion. And it is interesting because cyber is, in so many ways, understood and misunderstood.

It's a new domain, to be sure, but it also operates in each of the traditional military domains, and some are even now describing it as operating in the space between – Assistant Secretary of Defense Eric Rosenbach has taken to using this phrase about cyber – he said it operates in the space between the traditional foreign policy tools – diplomacy, sanctions and all of that – and then traditional, kinetic military attacks. I personally like the phrase “the space between” because it allows you to channel both Clausewitz and the Dave Matthews Band. (Laughter.)

We will – you know, a wonderful tradition of the Reagan Library in these discussions is rather than have the whole time filtered through me and through your questions, we like to give each of our distinguished guests a couple of minutes to discuss their perspective on the issue, sort of prepare the battle space for our future discussion. I'll then guide part of the conversation. And of course I'm looking forward to hearing questions from the floor toward the end.

To my right is Senator Roy Blunt of Missouri, a member of the Senator Armed Services Committee. Next to him of course is Admiral Michael Rogers, commander, U.S. Cyber Command and director of the NSA. Beyond him is Mr. Wes Bush, CEO and president of Northrop Grumman. And then on the end is Michael Allen, who currently is managing director of Beacon Global Strategies. We're also looking forward to hearing his perspective from his tenure as staff director for the House Permanent Select Committee on Intelligence.

So with that, Senator, the floor is yours, sir.

SEN. BLUNT: Well, thank you, Thom. I actually think this is one of those issues that at some point people will be engaged in at a level that we currently can't even imagine. This is one

of those things, until we find out how bad it could be, nobody is prepared to deal with it or as concerned about it as they will be.

A cyberattack is constant. We think we have different levels of security in the cyber world, and generally it's been sort of the idea that the military cyber was the most secure, the government was the next most secure, and the critical infrastructure not quite as secure as either one of those. But in any of those areas, a successful attack could have such impact and be so concerning to people that if the government hasn't figured out better ways to deal with this before that happens, in all likelihood there will be a huge over-reaction when it does happen.

But it's – I guess in the – actually, as part of what happens in actual combat, probably the Russians in Georgia in 2008 was the first time that, simultaneous to military action, there were other actions going on that totally disrupted the way the attacked country could respond. And this has got to be part of all our considerations in every part of what we do in every defense community. At some point we're going to have to figure out a way that we can encourage the critical infrastructure community to get there as well. And I'm sure that's one of the topics we'll talk about later, why people are so reluctant to share information and what it may take to get them to share that information.

But I would just say, even in the last week, thinking that the government was pretty good at fighting this off and the military was even better at fighting this off – I think I read three stories last week while I was thinking about this panel. Anyway, maybe I was just more actively looking for stories, but one in the – in a Pittsburgh paper was about the Russians with black energy, trying to put malware into critical infrastructure that would be there in a way that could disrupt everything that relates to energy. And when you really think about what that can mean to a community, particularly a community in a moment of crisis, it's a terrifying thing.

And then the Washington Post last week had two different stories, one suggesting in the Post that the Chinese, in September – the Post said the Chinese; I don't know if it was the Chinese or not – got into the personnel file for the post office, which is potentially 800,000 people that they have that – that they got that information, plus the likelihood that there's some infiltration into a private company that does most of the vetting, the security vetting for the government, and then later in the week that a – again, according to the Post – a Chinese-associated group got into the NOAA system, the weather system, which is the weather system, the disaster response system and quite a bit of aviation.

And this is a constant – we know that we've constantly been pushing back. What we're now seeing is that there are more apparent penetrations. And of course that's why Mike, as he talks next – Admiral Rogers is in such a critical place to talk about what we can and will do to prevent that from happening.

MR. SHANKER: Thanks. I'll overlook the fact you didn't cite the New York Times in any of your recent reading. (Laughter.)

SEN. BLUNT: If I can get that in a follow up, I'll get that in a follow up.

MR. SHANKER: Yeah, of course.

Admiral, please, sir.

ADMIRAL MICHAEL ROGERS: So for me first, as commander of United States Cyber Command, three primary missions: defend the department's networks, generate the department's cyber capacity for the future and then employ it, and thirdly, when directed by the president or the secretary of defense, provide our capability from a cyber perspective to defend critical U.S. infrastructure. The federal government had identified 16 different segments as critical national security areas. Think power, water, fuel, financial. There's 16.

As the director of the National Security Agency, we use our foreign intelligence mission to generate insights as to what nations, states, groups and individuals are doing in the cyber arena directed against the U.S. We also use our information assurance mission to use our cyber expertise to help defend the department's and the broader U.S. government's systems, as well as, increasingly, provide capacity, partnering with Homeland Security as well as the FBI, to try to support the private sector, if you will. So that's kind of the, so what does Rogers do and why is he here?

The kind of touchstones I would just point out are a few things. So my primary focus is at the operation level: How are we going to make this work? How do we defend it? And how are we going to use this operationally from a warfare perspective?

The takeaways I would share with you are, number one, this is the ultimate team sport. There is no single sector, there is no single element of this population, there is no single element within the government that has the total answer here. It will take all of us working together to make this work. And that is a huge challenge for us because cyber blurs what traditionally we considered what was a private sector function, what's the role of the government, and how does this national security piece fit into this? And cyber tends to blur all three of these lines.

You can see that reflected in the panel that you have before you today, from legislative to business to military. It's just going to take a broad partnership to make it work. And I guess that's what I'll start with for a broad opening statement, and I look forward to your questions.

MR. SHANKER: Thank you.

And Wes?

WES BUSH: Thanks. I'd like to start by thanking the forum organizers for putting me on a panel where we don't have to talk about sequester. (Laughter.) So we might end up talking about it.

MR. SHANKER: That's right.

MR. BUSH: You know, we all, each of us, have our set of actions we have to take around cyber, from a company perspective, from a – if you want to think about it, any enterprise. And clearly Admiral Rogers has probably the biggest scope, along with DHS, of thinking about what needs to be done organizationally and within their field of control. But I think there are several things that we all need to be working on together, and to really build on the comment that the admiral made regarding a partnership approach. And I think there's four sort of big over-arching things that perhaps can form a little bit of the basis for some of our conversation.

Senator Blunt talked about the legislative side of it, and I think that is critically important that we get that right, especially when we think about the threat profile to the critical infrastructure. And there are a variety of issues that are going to have to get addressed there, ranging from how do we actually get the critical infrastructure industries to work with everyone to get this done, to liability protection that goes with it, to actually what the incentives are for making all this happen. So the legislative side of it I think is a big piece of it.

Technology is another area that I think we need to stay ahead on. And I want to make sure that as we have our discussion today we don't leave the technology side of it out. Oftentimes many of us have the perspective that there are so many other things we've got to work on, whether it's legislative or many of the other issues. We often actually find ourselves saying, well, technology isn't the issue; we need to go fix these other areas.

Technology is going to remain an issue, and it's going to be a big issue in cyber for a long time, particularly as we think about the expanding areas of the threat profile. We need to make sure that we're embedding the protection into the platforms and capabilities that we're all delivering. And we also need to make sure that we're thinking several steps ahead to what it's really going to take to have resilient networks and platform capabilities, and to have things where we're not just constantly thinking about building the wall around everything that we create.

The third area I would mention is workforce. This is another area for partnership. None of us alone are going to solve that problem. And we need to make sure that we're building on

many of the emerging partnerships between government and industry and universities to really create the workforce we're going to need for this rapidly growing area.

And the fourth element that I would mention is one that I don't think we talk very much about but I think is fundamental, is international. If ever there were a domain that has no borders, it's cyber. And every one of our enterprises has some connection into an international domain, whether you're a multinational company or you're thinking simply about the networks that connect to all of our critical infrastructure. There is a huge aspect of vulnerability and opportunity that goes with thinking about this beyond our borders, if you will, that I think is going to frame much of the progress we need to make on cyber.

So those are some key areas that I think are important, just an over-arching thought. We're not going to solve all of this all at one time. Most of the solutions are going to be inherently incremental, and we need to be OK with that, whether it's legislative – bite off a bit of this at a time – or it's technology, but we need to get on with it, and we can.

MR. SHANKER: Thank you.

Michael, please.

MICHAEL ALLEN: Thank you, Thom, and thanks to the Reagan Foundation for the invitation. It's great to be in Reagan country. I think we – when Senator Blunt mentions, how do we motivate legislative action or how do we increase awareness about cybersecurity, so often I think the buzzword that we've used to try and motivate action has been "cyber Pearl Harbor." I think that's important, and if that helps to motivate action I believe we need to, you know, continue to use it.

However, I think it sort of obscures what might be the true nature of the threat as we face it today. Now, it may be that ISIL and others, and other substate actors are tremendously successful in the medium term, but for now I think we need to focus on the economic theft of intellectual property that's going on across our country today.

We see, of course, examples in the defense industry, but we've also – when you go through the indictment of the three PLA Chinese military officials, you see that they're attacking Alcoa in western Pennsylvania; they're attacking a solar company in Oregon. This is the sustained economic pilferage of our intellectual property. I think maybe we need to start to talk about it as a jobs issue.

I think we're really at an inflection point with cyber. We are at the point where Congress is in dire need of, as Mr. Bush said, acting and setting a framework for information sharing. I

think we are at a period of tremendous stress with the private sector in cybersecurity. We always talk about how the private sector owns the majority of the networks, except, thanks to Edward Snowden, I think there is, at the very least, a perception problem on the part of many an industry for working with the U.S. government.

And finally, I think that there are issues with respect to NSA as an intelligence-gathering organization, or NSA – or Cyber Command as a – perhaps a combatant command in the future that we'll need to address as we try and prepare for what is going to be a long struggle against a persistent cyberthreat.

MR. SHANKER: Thank you very much. That was a wonderfully clear and concise sketch of the landscape for the cyber discussion.

I'd like to start with some questions for Admiral Rogers. But before I do, sir, I do want to express a very sincere thanks for you coming out today. The relationship between the military and the media, it's like a marriage. Now, it's as dysfunctional marriage – (laughter) – but we stay together for the kids.

DIR. ROGERS: But I love you. (Laughter.)

MR. SHANKER: And so it's great that we're here for a little counseling today. (Laughter.) And sincerely, thank you for coming out to discuss these very important issues at the four-star level with us.

There was a panel that preceded ours, hosted by my friend and colleague Barbara Starr of CNN, that talked about the question of strategy. And even though as CYBERCOM commander you described your role as at the operational level, I know that you're looking at this strategically.

And I guess my first question, Admiral, is, you know, does our nation have a real cyber strategy today? Does it even need one in time when there isn't even a national security strategy? And then as part of that, talk about the offensive piece, how it fits into strategy, the difficulties of, and why there hasn't been a lot of discussion about offensive cyber.

DIR. ROGERS: So just the small number of questions. (Laughter.)

MR. SHANKER: Just a small number of questions.

DIR. ROGERS: Let's see, first, I think we have a broad consensus of what the elements are that we need to address in a strategy. The challenge has been in gaining the consensus to come to an agreement on some of the specific aspects of it.

In terms of from a Department of Defense perspective, I'm very comfortable with the vision we have in terms of how do we create capability, what skillsets should it have, how should it be employed operationally, how should it be integrated? Cyber has got to be integrated with a much broader effort. I'm not a big fan of looking at cyber kind of in isolation. I think you've got to view it more broadly.

The bigger challenges, in my mind, really start to morph into the policy arena. So how do we get to a set of norms or expectations for behavior in this environment, because right now seemingly if you are a nation state, you are a group, you are an individual, there seems to be little sense that you run risk by engaging in attempts to penetrate inner systems, steal information. My concern there is if we're not careful and this trend continues, this will encourage nations, states, groups or individuals potentially to start to engage in ever-more escalatory and riskier behavior.

And that's not a good thing for us as a nation because, don't ever forget, once you gain access to a system, then the big challenge becomes what's the intent? Is it, I'm trying to steal intellectual property? Is it, I'm a criminal entity and I'm trying to steal data, account information, things that I can generate resources with, I can make money from? Is it, I'm trying to do reconnaissance for follow-on military activities? Is it, I'm using this access because I want to engage in manipulation of your data? Is it because I want to use this access to potentially engage in destructive behaviors? Intent is everything here, because once you get in, there's a lot of options open to you as the attacker, so to speak.

In terms – what was the second part, Thom, to make sure I answer your questions?

MR. SHANKER: Well, sort of the public discussion of the offensive question.

DIR. ROGERS: Oh, the offensive question.

MR. SHANKER: How does one engage with the public in cyber? You know, even with highly classification, during the Cold War there was a robust public debate about nuclear weapons and their offensive use. We don't really see that now with cyber.

DIR. ROGERS: Right, because I think it's still in the early days, in some ways, of offensive capability. I believe that you will see that. I mean, I'm spending some time in the academic world and in the policy world trying to argue, hey, look, this needs to be a much broader discussion than just the uniform world. There's a whole lot of other implications for

this. We want to make sure there's a broad set of parties involved in the discussion. But, you know, clearly from a DOD perspective, we have talked about it is our intent to generate the full range of cyber capability to provide policymakers and our operational commanders with a greater spectrum of options, should they choose to use them.

MR. SHANKER: Right. You mentioned your time in academia. I know that this week as well you've been up in Silicon Valley talking to people. You know, as you reach out to partners in the private sector, I'm just very curious about what you're hearing from and saying to people like at Apple and Google and Microsoft that are moving towards the kinds of encryption that make your job very, very difficult but has a legitimate and credible business need, because without the confidence in what America sells in software and software, they simply can't do business in the world. So is there a medium there or is this something that you're going to have to disagree about, or are you doing things that you can't talk about?

DIR. ROGERS: No, I mean, one of the reasons that I'm spending time in the valley – I'm generally up there, to be honest, every six months. I have been the commander for seven months. I have been there twice already in the seven months I have been the commander of U.S. Cyber Command, the director of NSA, because I am trying to have a discussion about, look, we have got to – number one, we have got to understand each other. And I'm watching two cultures that are largely just talking past each other, not because one is good and one is bad, but because they're two very different cultures with very different views of the world around them, lack of familiarity with the other side.

And the people that I lead are every bit – have the same challenge. They don't come from the corporate sector. They don't understand the imperatives that tend to shape decision-making – very valid concerns if you're running a business segment. Likewise, when I talk to my business partners, as it were, you know, my sense is I tell them is I don't think you really understand as the way you think you do. And so I'm trying to engage in a dialogue to help us walk our way through that so that we can actually sit down and walk our way through what is an incredibly difficult issue. What is the balance that we need to strike here?

And my argument is I don't think it's an either/or proposition. Can we find the middle ground? You've heard the director of the FBI talking about concerns – which I agree with, I agree with Jim very strongly: Hey, look. Can't we come up with a framework with a legal architecture to it so you don't want to do something arbitrary that will enable us to harness the power of technology and the legal framework we use as a nation to address issues that a court believes that represent a valid concern of potential threat to us as a nation or society? We use a legal framework as a nation to do that. I don't think cyber should be any different.

So, you know, my view is we're getting to the point where the emotion is starting to come out of this a little bit, which is good because another point I try to make is look, if we are each going to vilify each other, we will get nowhere. It cannot be that one of us is good and one of us is bad. It's got to be we come from two different perspectives, we each have a valid concern, and what's the way that we can work together to make this work, realizing that neither one of us is just good or bad?

MR. SHANKER: I'm sure other panel members have thoughts on that, but before I do, I have one sort of news question for you. It's always interesting when we hear about the war games that Cyber Command runs. I know that you recently had, last couple days, I guess, a large-scale cyber flag exercise. I'm sure the scenario was classified, but can you talk about some lessons learned, some gaps that maybe you identified and also, of course, what went right?

DIR. ROGERS: So part of it goes to something Wes said. So every year, U.S. Cyber Command hosts a major exercise. We do multiple exercises, but we host the largest one every year. We call it Cyber Flag. We just finished it up about a week ago. It's about a three-week exercise. It involves U.S. Cyber Command, its subordinate elements as well as other elements in the U.S. government – Department of Homeland Security, FBI is there to participate. We bring in corporate. We also brought in coalition partners this time, because again, as you heard Wes say, I'm a big fan of, look, we cannot just approach this from a U.S.-only perspective. We have got to figure out how can we mesh with our allies and friends around the world and how are we going to work our way through this because we are all going through this journey. Cyber is so foundational to each of us as individuals, to us as a nation and, I would argue, to the world around us.

And as the senator said, we're going to be dealing with this in ways we don't even understand right now. I mean, this is probably the most revolutionary invention that man has ever generated. Think of the impact that this has had in terms of generation of knowledge, the sharing of ideas and information, the ability to rapidly coalesce like-minded individuals who have no connection other than this means to bring them together to work particular issues or topics of concerns, the economic power that this has generated. Those are great things for the world. They're great things for us as a nation. We've got to figure out, even as we're trying to address the challenges inherent in cyber, how do we still build around the things that have made it what it is, that have generated those good outcomes?

This exercise, Cyber Flag, was designed to focus how are we going to – how are we going to fight, how are we going to defend our networks, how are we going to partner with other nations, how potentially are we going to look at the application of offensive capability, what are the rules of engagement we need to develop, what are the holes we have right now that we don't have answers but we need to get answers to, what are the things we feel very comfortable with,

what are the challenges in defending our networks so that the network, the exercise is really designed to put us in a high-stress environment and really push ourselves to get down to work those kinds of issues.

MR. SHANKER: Any gaps or shortcomings (they ?) identified?

DIR. ROGERS: There is always plenty of challenges, none I'm really going to get into quickly. I generally don't try to tell the other guy – (laughter) – exactly where he should focus his efforts.

MR. SHANKER: Senator, please.

SEN. BLUNT: Yeah, on that front, Thom, I think one of the interesting things probably Admiral's doing at Cyber Command and – is looking at what did we think we were going to be pushing back against last year or two years ago compared to what we're actually witnessing now. You know, one of the legislative problems with this, and generally the problems of trying to deal with it, is that all of these things have developed so much more quickly than we thought, and you're having so many more things come in so many more directions – and, you know, back to something as basic as like the telecom bill a decade ago, five years later, when it came time to do the telecom bill, not a single thing that we debated that was supposedly critically important five years earlier mattered any more. And so this is a rapidly changing environment.

One of the things will be difficult to deal with in terms of offensive cyber is how do you where the attack is coming from and how do you know to respond to. You know, you knew an earlier time where that weapon might be coming from – at least we thought we'd always know where the weapon was coming from, and that's where your retaliation is. In this, you might now know, and you might not even know if you think you know because somebody's got so good at this that they're able to hide where they're coming from, which is back to the conversation – (inaudible) – couple times about essentially back doors, why this is such a collective responsibility as there are so many different ways into everything, and so you may – you know, you may have gotten into – look at how people get into the various financial information they get into now through a retailer. It's seldom by getting directly into the information one step to the retailer; it's you get here, and then you get here, and then suddenly – so you may start somewhere that you – nobody ever even thought you needed to protect, just like the offensive cyberattack is going to be, how do we recognize that, and then how do we retaliate, and who determines that that level of retaliation to somebody else's financial network or their electricity network or their transportation network, who decides that, OK, this is – this is at the point that yes, we need to retaliate, and we need to do it right now – that's the – a different discussion than we've ever had to have before because this could be so potentially mask (ph) in how you figure what's happened and where it's coming from.

MR. SHANKER: Right. Since you mention the legislative piece, I'm curious to get your handicap (ph) for the Cybersecurity Information Sharing Act and related legislation. Any chances in a lame-duck Congress? And if it goes to the new Congress, what sort of compromises and changes might be needed?

SEN. BLUNT: Well, I think it's a little early to tell how long the lame-duck Congress would last. My guess is no because I've been working on these issues now for about four years with various efforts to try to figure out how you – how you get everybody to buy in. And I don't know that we're there yet. There is – there is more bipartisan cooperation here legislatively than there is cooperation in who you believe you're trying to help. You know, how do you create that liability protection that is attractive enough that somebody in the critical infrastructure network is willing to be more open about the attacks that they're getting, how they're responding to them, what do you put on the table that encourages them to be willing to tell you that because everybody has – so many people have some sense that their position at the marketplace is jeopardized by being too open about problems that they're dealing with, and how do you make that worthwhile.

You know, my view is, if there is ever – when we get to the point where there is a serious problem, what critical infrastructure folks need to understand is how much liability they may very well have if people's health and welfare is damaged because they couldn't properly secure their system. At least that's the case we made in court, unless there is some protection that you've done everything you could to be able to claim that cloak of having done your best, and that means that your liability is different because of that.

MR. SHANKER: I want to ask about your own Cybersecurity Public Awareness Act, and partly as a journalist but also as a – as a citizen, you talk about the prospects for that. And also, what is the role that the American public should play and should get to play in cyberpolicy?

SEN. BLUNT: Well, this is – actually, this is something that Senator Whitehouse and I have worked on. We were talking to leadership staff, both leaders, this week to see if there is any chance to move forward. But that is sort of at the crux of the – all we really would like people to do is be more open with the people that are impacted when there is an intrusion in the information and willing to do some things, like I said, that provide some liability assistance. But there is – we haven't gotten to the point where the people that this – we believe that we are – we are helping in the long run quite perceive maybe the vulnerability that they have. So I will say from our discussions last week I think we're going to continue to work on this, but I would not expect it to happen this year.

MR. SHANKER: Right.

Wes, I'd love to hear a little bit more of the corporate perspective. And in particular, what does industry need right now from the government? And can you also answer this question about the rub between obvious national security needs but your desire and need to have confidence with your investors and business partners?

MR. BUSH: So let me give you two perspectives on that, one being in the defense industrial base, we actually have a little bit of a leg up. On the one hand, we are perhaps more targeted than some industries because of the sensitivity of the information that we all manage in our networks, but on the other hand we've been working in this environment for so long that collectively, this is something we have been doing, not only for ourselves but for customers. So from a technology standpoint, we do actually in many cases have quite a leg up on other critical infrastructure industries.

But the other part that I would mention is an activity that was started a number of years ago, the DIB pilot, the defense industrial base pilot, that actually was the forerunner to where I think we need to go broadly with the critical infrastructure industries that actually figure out how we could share information. And I will tell you, you would think that the ability between defense companies and the Department of Defense and other related federal agencies to share security-related information should be a slam dunk. It took us over a year to clear all of the legal hurdles, if you will, that were identified and put in place for us to actually get the pilot started. And this is an industry that all the time is sharing security information with each other and with our customer community.

And from my perspective, that was the first big flag that went up for the rest of industry that's collectively referred to as the critical infrastructure industries, how hard this is going to be unless we clear some of these roadblocks. If the defense industry takes over a year just to be able to share information between itself and the Department of Defense, we know we have a real issue.

And so as I've gotten out and interacted with others who are in the other critical infrastructure industries, they really are dealing with all of these problems, one that on the technology front, most of these companies are spending a lot of money already just to operate their IT networks and to keep pace with technology and operating their IT networks and downloading, you know, all of the sort of the pro forma set of protection software that they possibly can. They are not yet able to move to that next level that we collectively believe they need to be at because to start with, they've got to build that intellectual capacity in that ability within their own organizations. But beyond that, the ability to share information so that Admiral Rogers is seeing something coming right at him, he can actually share that with them and enable them to take the protective steps that they need to take and that they can share what they're

seeing in their networks back into the federal government without the risk that, you know, five months later in hindsight, yes, there was maybe perhaps one little piece of personal identifying information that someone could be upset about that we have systems that actually enable us to manage this in the real time we have to manage it to deal with the cyber threat.

So we have, I think, across many of the critical infrastructure industries basically a stand-back-and-wait approach because the last thing you want to do is to run out, invest a huge amount of your shareholders' capital in what you think is a fix without an overlay either legislatively or technologically that says, yeah, that's actually the right fix – because inevitably, you'll get it wrong, you'll write that off, and then you'll try and do it again.

So I see across many of the industries a little bit of a wait-and-see. Let's wait and see what happens here. And unfortunately, wait-and-see can produce calamities, if we wait too long and – then we see what really can happen. So from a – from a defense industrial base perspective, as I said, I think we have a little bit of a leg up on this, fortunately, but I am quite concerned about what I see across the critical infrastructure industries.

MR. SHANKER: And what about the sharing of information with those that you don't want to be sharing it with who are getting into your critical systems? Companies like yours have some of America's most vital secrets. Putting aside sort of the consumer and public service hacks that the senator talked about, how are you going to regain the public trust by saying, yes, we can keep these things secure in your name?

MR. BUSH: Yes. And as we all deal with this every day, we are ratcheting the game up, you know, from a protection standpoint and from an investment standpoint. We're careful not to say publicly how much we're investing in this. As the admiral said, you don't want to necessarily give all of your anniversaries all of that information. But across our industry, the collective investment in securing networks is very high. And it goes into the cost of providing the goods and services that we provide. And ultimately, our customers have to decide if they see us at the right balance point on that.

But your point is exactly right. At the end of the day, you don't want to be looking backwards and saying, gee, if we had thrown another 50 million at this, we could have saved a critical piece of technology from being understood by our adversaries. And it is a constant risk-and-return assessment that we're doing.

MR. SHANKER: When our nation is attacked, when the military is attacked, there are clear rules governing the behavior, the laws of armed conflict. Those don't really exist in cyber for the private sector. Do you ever see the possibility of corporate (hackback ?) unilaterally?

MR. BUSH: Well, here again I think we will need to find our way through a legislative arena. None of us want to be the first company, you know, charged with doing something that isn't appropriate, OK?

So ultimately, I think all of us understand that a purely defensive strategy is probably not a successful strategy. You know, in the history of any form of security, if you're not able to impose a cost on the adversary, you rarely succeed. So from a corporate perspective, that's probably sometime in front of us, you know, before we can all get our arms around how that would really work and how that would work within a legal context. But today we're fighting the battle defensively.

MR. SHANKER: Right. I'll note for the record that Admiral Rogers was smiling during that question and –

DIR. ROGERS: Well, I was just thinking, I think that's where that whole idea of deterrence and norms becomes so critical because if we're not careful, this will become one of the ultimate cost (sums ?). We will just pour more and more resources, and we will always be reacting, and that's just not a good –

MR. : It's a losing strategy.

DIR. ROGERS: – a good place to be. It's not going to get us where we need to be. It will be a highly – it's a high-cost, high-attrition strategy. It's not generally successful.

MR. SHANKER: Michael, I'd like to turn to you. I would love your perspective from your work on the intelligence committee about some of the rub and friction when it comes to intelligence and cyber. You know, law enforcement, the intelligence community loves cyber because of what it can learn about an adversary, but there is – there is tensions that have been reported with the military that they needed to take a kinetic action against a cyberentity that they saw as presenting a clear and present danger to America's deployed troops. I was just curious what you think about that problem and whether they're being arbitrated effectively and in the government today.

MR. ALLEN: Well, that may have been what Admiral Rogers was referring to when we talk about how we need to have a lot of policy attention to try and resolve some of these fundamental issues – I think these are going back even to the Bush administration – and that's sort of the inherent conflict of if you consider that we might have electronic accesses around the world and we have the age-old question of do we want to continue to use that access for intelligence or monitoring purposes, or do we want to be able to use it for a kinetic purpose to achieve a battlefield effect? Now, you may say, well, we want to use it for both. But I think we

have to sort through this dichotomy of cyber – perhaps if Cyber Command is elevated now to a unified command, we've got to be able to reconcile the decision-making process through which we may use one of these accesses for a battlefield purpose and what harm that might do to the intelligence mission, which, after all, operates on stealth while the military, of course, operates, at least in a kinetic sense, on achieving sort of a loud, noisy physical effect on the ground. So I think there is a lot of policy issues here and in information-sharing in the Congress that we need to be able to sort through and quickly.

I mean, by the way, just to close out on the legislation, I mean, when you consider the breadth of the divide between Republicans and Democrats on everything from sequestration to entitlements to taxes, I think cyber legislation is sort of low- to medium-hanging fruit. I think there is general consensus out there that we need to be able have an information-sharing system that allows not only the NSA or the government to share classified threat signatures with the private sector but also the – maybe the more important part of that is what the private sector is allowed to share back with the government or among itself.

And so when we went through this issue in the House, it really came down to two issues. On the vertical information-sharing with the U.S. government, were we going to use the Department of Homeland Security, or were we going to use a pre-existing relationship you might have with the National Security Agency or the FBI? Ultimately, I think because of Edward Snowden and the rest, we came down to a system where the Department of Homeland Security would be the portal, but you would mandate that it would be immediately shared with who we believe to have the most cyber confidence in – competence in the federal government, which is of course National Security Agency.

And then finally, the other issue is the privacy and civil liberties issue of personally identifiable information. We all agree that it shouldn't be shared, where possible, if it's not part of the threat signature, but the question really came down to in the House of Representatives – and I think this is unresolved but solvable – is, if we're going to try and minimize or suppress personally identifiable information, who should do it? Should it be an individual company that has the charge to do that and maybe the Verizons and the AT&Ts of the world are equipped to do that, but is that an unfair mandate on a smaller company that we're trying to incentivize to participate in an information-sharing program, and should therefore the government be the one, maybe at the Department of Homeland Security level, to minimize the personally identifiable information.

When you look at the Rogers bill, Rogers-Ruppersberger that passed the House twice with bipartisan support, and you even look at the Feinstein-Chambliss bill, I think that – I think the solution is there. I think we just need some leadership from the executive branch, and I think

with the new Senate I think we, you know, maybe can get this done next year or at least in the next Congress.

MR. : Right. Just a historic footnote on the Title 10 versus Title 50 thing, when Mike and I were having our conversation, there's an incident that's been written about a little bit during the surge in Iraq when a terror organization called JRTN,, the Naqshbandia brotherhood – and by the way, they are now back and partnering with the Islamic State – they were hosting websites with information that was a danger to the surge. They were listing all the polling places for upcoming election. They were doing the military supply routes, all that. And the military commanders in Iraq wanted those websites taken down, which is a capability that this government has. But the intelligence community argued against it because they were learning so much about what the adversaries were doing. Finally, I went up to, I think, the principals level, and a decision was made to take it down during the elections because that was a period of time – it turned out, actually, that the website – that the servers hosting the site were not in Iraq but were in the United States, and so they were taken down not through military force but through a couple of people in white shirts and striped suits stopping by and asking for them to do that.

DIR. ROGERS: Tom, can I make one comment?

MR. SHANKER: Please, sir.

DIR. ROGERS: That's another reason why I think in the years subsequent to that event, that part of the decision to align U.S. Cyber Command and NSA under one individual. So you had one personal (ph) accountable, same – (inaudible) – both hats. Ultimately I work for the secretary of defense – both hats, one individual accountable. So, Rogers, if you made the wrong call and you felt that intel gain was the way to go, putting on your NSA hat, versus my U.S. Cyber Command operational commander hat, the reason that – one of the reasons we brought them together was to try to address just that. I am perfectly – for me, I don't think it's the issue that many have historically made it out to be because I don't feel conflicted at all. At times, my view is, hey, look, as a senior military individual, I'm held accountable for making choices and accepting risk, and partnering with others in doing that is not a decision I'm going to make in isolation. I think it's a strength of the current arrangement, personally.

MR. SHANKER: All right. Thank you. One last question for Michael before we move on. You were brave enough to use the S word, as in Snowden, so I'm going to ask you not so much your assessment of the damage he did – because we could all differ on that – but what do you think the impact of the Snowden affair is on legislation and its opportunities?

MR. ALLEN: I think the Snowden affair was definitely the approximate cause of no legislative action on cybersecurity in the last year and a half or so. I think that members of

Congress, rightfully so, heard a lot about the revelations, and it just wasn't in the cards to come up with a new legislative regime that was going to allow more private sector or personal information to go into the hands of the government, especially if perhaps it might be someone in the intelligence community behind the portal that would be able to analyze it. You know, I may regret saying this. I think and I hope – and maybe Glenn Greenwald will, you know, strike me down here with another article – but I think we're perhaps, maybe because of ISIL and just generally, time has passed that maybe we're coming out of the Snowden hangover effect. And with the continual march of JPMorgan, Home Depot, Target, et cetera, et cetera, I think we're going to be able to pull through that. That's not to say privacy and civil liberties will not be a huge issue. It will be. I think it's going to be a huge issue and it's something that will be fought very hard. But I think at the end of the day, a solution is doable, where, as Admiral Rogers said, both sides can feel comfortable that we have a system that works for the national security but also for the privacy and civil liberties of our citizens.

MR. SHANKER (?): Thank you.

DIR. ROGERS: And I could – I'd also highlight for the record, as the director of NSA, I've been very public about saying, look, I don't want personal information when we're talking about computer network defense. That slows me down because of the legal requirements associated with us handling – how we handle U.S. person data. That starts to really complicate, then, what I can do. I have to protect that data. It has to be put in a particular area. It's compartmented. I can't share it. It's controlled, how we use it. That's not what we need to do for computer network defense. I have zero interest in going down that road.

But I do think we need a dialogue between both the public sector, the private sector and those of us in the government, you know, tasked with trying to get down to the execution level. So when we say sharing information, just what do we mean? What are the specific elements of information that we want from each other? Because the answer is not, well, just send me everything you have. We can kill each other with volume in this arena. That's not what we need to generate the outcomes I think we're all looking for. You know, my view is, what I owe is, let me help you understand. Here's the malware that's going to be directed at you. Here's where it's coming from. These are the kinds of advanced indicators I think you're going to see that would suggest to you that this is coming. Here's how I think you, perhaps, can react to it. What I'm interested in from the private sector is, so, is what we told you what you saw? Did you see any advanced indicators that triggered you that something was coming that we didn't anticipate? What did you try in defending your network that was effective and worked that we can share with others? What did you try that didn't work that we can suggest to others, hey, you don't want to try this, you don't want to go down this path. This has got to be a two-way street, I think. And we have got to spend time defining exactly what we want each other's perspective and then how are we going to pass it.

MR. BUSH: Let me answer that. You know, I think there is a false perspective, oftentimes, that there is somehow a tradeoff between protection of personal information and cybersecurity, and the view that somehow any time some personal information finds its way into the government, that it's inherently bad. You know, last I checked, every year when I fill out my tax return, I provide the government a heck a lot of very personal information. Anyone who's – participates in Medicare or any other government-sponsored form of insurance is providing the government a heck of a lot of personal information. Yet we have reached a point where we all seem to figure out how to make that work.

We can do the same thing with cyber. And in fact, the technology available to help sort through that and make sure that the right sets of information go to the right places, that's with us today. This is not something we have to go and invent. So I think there is a very false argument, oftentimes, that there is somehow a block on our ability to do cybersecurity right because of this personal information. Do we need the systems to make sure it works right? Yes. Do we need the legislation to make sure it's performed correctly? Absolutely. But I think we can all be very candid about the fact that, yes, there will probably be cases where in the speed that's necessary to protect networks, some of that information may find its way through, but we can build the processes and use the technology to make sure it's secured in the right manner. And there should not be a tradeoff here.

SEN. BLUNT: But from the last two comments were made, don't you really have two very separate discussions going on here? One is an NSA discussion of what information the government wants to be able to have general access to if they determine some kind of pattern that has really not much to do with trying to secure a network. And the more you can separate those two things so that they don't become linked unnecessarily, I think is the better way to look at this, where, at the end of the day, we're probably never going to be able to secure as we – you – as people actually, if they knew how vulnerable their own network was, you're not going to get people to have different passwords for everything they do and change them occasionally and all those sorts of things, but the kinds of things that they could become a portal into, that's where, you know, you want to have that network more secure. I think we have to be really careful here. If we ever want to get anything done, either legislatively or practically, that as much as possible we don't confuse these two things, that cybersecurity doesn't necessarily have to be part of this other discussion about who you're talking to on the phone.

DIR. ROGERS: Right. That's why, for me, as director of NSA, I very much differentiate between what is a (foreign ?) intelligence –

SEN. BLUNT: Or who you're emailing or – yeah.

DIR. ROGERS: Right – what is a (four inch ?) intelligence mission we're doing under specified authorities and what is our information assurance computer network defense mission. And those are two very different things.

SEN. BLUNT: I guess my point would be either of them are hard enough to get done no matter how well you're doing. If you – if you – if you confuse them if it's not – if you don't have to – if you combine them if you don't have to, it makes either one of them infinitely more difficult to deal with.

MR. SHANKER: But it also seems there hasn't been a Darwinian evolution of the public perception because electronic information is somehow viewed differently. When any of us travel overseas and we come home, the customs inspector can go through our most intimate personal belongings in our suitcase and nobody says no. So how can you help the public understand that, in this new era, perhaps they need to change their thinking about information? Or is there something about electronic information that is even more private than your personal belongings?

DIR. ROGERS: For me, it goes to we need to have a broader discussion as a nation about just what does privacy mean in the digital age of the 21st century? Because if you think this is a phenomena that only involves the government, I would ask, what world have you been living in? The power of big data, whether it's the government, the private sector to generate insights about our behaviors as individuals and some of the choices we make, whether it's a foreign intelligence associated kind of threat choice or whether it's how you spend your money, where you spend it, when you spend it – big data's being used to generate insights for all of that and we shouldn't say to ourselves, oh my god, that's terrible. What we ought to say to ourselves, I think, is, so what are we comfortable with as a society? What's the right balance for us? But I – to Thom, it goes to your point – I just think this is so foundational to the future that this idea about well, we just suddenly characterize everything as, oh that's just – that's the government doing this or that and I'm thinking this – we need to make this discussion a whole lot broader. What are we comfortable with as a society?

SEN. BLUNT: I think (your needs ?) develop some greater sense of consequence, too, when people have information. So if you – last Christmas, there was a retail data breach that just – people were outraged. Similar things happened in the last 60 days and not much of a response. It's like well, OK that's already happened, the world didn't end and nothing happened to me – which, for most of us, would be the case – I'm sure some things happened to some people but until people have a greater sense of the consequences of information widely shared or what could happen to their utility – source of utilities or what could happen to their financial network, you know – and I had – I have had some people lately say, well, if you're in a data breach – I've heard retailers concerned that if so many people don't have access to their credit card for a week while they're getting their new card between now and Christmas, what does that do to retail

world? Now, that's beginning to get a little more of a discussion of what this could mean but I was just surprised that what we saw lately was no different than what we saw a year ago except the response was almost totally different. No discussion of not – you know, all the discussions we heard after the Target problem a year ago; we didn't hear anything like that eight months later when the same thing happened to other retailers and, you know, what are the consequences here?

MR. SHANKER: Right. A question about consequences and risk: Secretary Panetta, who's on a panel later this afternoon, famously warned of a looming cyber Pearl Harbor. This sort of digital attack has been discussed almost since the beginning of the internet yet, fortunately, it hasn't happened. So some critics say that the threat really isn't that serious and that this is all about money for the military and private sector contracts and all that. So I guess the question is, seriously, how serious is the threat and if we are at such risk, why has there been no cyberattack yet that's included real loss of life or (skata ?) failure? Each of you, please.

MR. BUSH: Can I offer just one perspective on that? You know, if I were an adversary and I were – basically had my pick of any network in the U.S. that I wanted to find my way into – perhaps other than some government networks and some very, very secure private networks – and I could go in and steal the intellectual property that I needed from time to time, mess around with things, maybe plant some things, why would I choose to do a Pearl Harbor? I'm getting exactly what I want.

MR. SHANKER: So you're among those who say that the sort of catastrophic loss of life attack is not the likely scenario?

MR. BUSH: It concerns me that, if we only hinge our strategy around, gee, if there's a calamitous event, we're all going to do something, we're being very, very shortsighted. The calamitous events are happening. For those who think that their networks are truly, truly secure, that all of that information is somehow getting protected; they're kidding themselves. So I actually think, you know, depending on what you want to call a Pearl Harbor, we've got the calamitous events underway right now and we need to be thinking of it in that context.

MR. SHANKER: Anybody else on that topic?

DIR. ROGERS: I would agree that there's plenty from destructive behavior out there – globally – if you look at this challenge set globally – multiple instances of destructive behavior, manipulative behavior, theft. To me, this is – if you still think, well, we're OK, we'll just wait for something really big to happen, I just think, wow. What a losing strategy. And as a nation, is that really the approach we want to take? Well, we'll wait until things get really horrendous. When we all, I think, intuitively realize, wow, this is a complex mission or area that's going to

require us to come to a broad consensus from both a legal and authorities piece, the corporate sector, government, the private sector and we're going to wait until some form of, you know, disaster to drive us to do it? Oh, man. That is not what we're about as a nation. We're willing to take on tough problems and this is a tough problem we have got to be willing to take on.

MR. SHANKER: Well, as you look at the hierarchy of potential adversaries – and I'm sure this will be e) all of the above – but do walk us through: I'd be interested to hear from each of you sort of the Russia, China threat, the patriotic hacker threat and also what we were discussing earlier, the sort of availability on the black market of malware in a way that simply has been unknown in past years. When you look at the landscape from each of your perspectives – legislative, corporate, military, intel – what do you see as the – as the hierarchy of risk?

SEN. BLUNT: Well, I think the – there are lots of risks. Hard to create, in my mind, the hierarchy of those risks but clearly this becoming a tool of nation states as well as a tool of terror groups and you've got sort of the curious individual element that is probably the least concern but at some point may actually be the group that actually pulls the trigger that people are more aware of because they're not – they're not thinking about anything, saying, I just wonder if I can do this. But you know, what I saw, particularly from the vantage point of several years on the intel committee, was a couple of our adversaries not only were not – they were just – they were constantly there but they were also constantly willing for you to know they were there. It's sort of like the person that breaks into your house and immediately finds what they need but they still dump all the dressers drawers just to be absolutely sure you knew that they were there and they could be there, I think we see this – their – see some intimidation, a willingness to use this as a – just constantly reminding us that they are not our friends.

MR. SHANKER: Michael, what was your sense when you were doing House intel work?

MR. ALLEN: Well, just to stay safe, I'll quote what General Clapper said in public at a intelligence conference in Austin, Texas last month, which is that – and I don't think this is a surprise to anybody in the room – it's the Russians and the Chinese. Director Clapper said he believed the Chinese were noisier but they throw mass at the problem. We saw a little bit of that in the indictments, when you see how many people at the third PLA are targeting everything from herbicides to a variety of different common household goods across the country, but that the Russians were in many cases more sophisticated and it's more complicated there because there's the suggestion that maybe the Russians are working on behalf – maybe some of the organized crime entities have connections back to the Kremlin. So I'd probably leave it there to say – keep it safe and quote Director Clapper.

MR. SHANKER: Right. (Laughter.) On these – on the new malware threats, can you – can one of you talk about sort of what they are appearing to be, what you're seeing, what their capabilities are?

DIR. ROGERS: For me?

MR. SHANKER: Please.

DIR. ROGERS: Apologize. Well, to be honest, I'm not going to get into the specifics of nation state or group behavior. I would say this, though: The concern I have increasingly is what if the lines are starting to blur and what if nation-states are turning to surrogates – whether they be criminal actors, whether they be groups or individuals? What if groups, individuals are starting to create partnerships with others that traditionally we hadn't looked at because we had the initially very clean, monolithic approach? Hey, we got, like, four different types of entities.

The biggest thing that concerns me in some ways in the immediate near term is we're taking capabilities – whether they be nation-states, groups or individuals – and I'm watching some of these blur and create partnerships that make attribution more difficult, that clearly are intended to try to stymie attribution as well as policy decisions on our part. That's probably the biggest thing that I'm watching right now that I'm going, wow, this is going to require us to think a little differently here.

MR. SHANKER: This is the new convergence that people are talking about.

MR. : Right.

MR. BUSH: I think it's both convergence and proliferation. The malware threat today continues to grow, not just because we're – we have a small number of adversaries who are increasingly technologically competent and focused on this. It's also growing because, just to put it bluntly, it's easy. And this is – this is a – if you want to call it a weapon or a toy or a tool or whatever – it is something that is propagating around the world in terms of individuals and small groups of individuals and networked groups of individuals creating capabilities on large scale. So I would worry not just about the convergence. I'd worry about proliferation.

MR. SHANKER: Mmm hmm. Thank you very much. This is the dynamic part of the program where I turn to the audience. And I'm eager for your questions. I think they'll be setting up some microphones for us. If you would just please introduce yourself. And I know lots of people will want to have questions. While they're setting those up, I'll end on sort of a lighter note.

This is a question for the military and the corporate representative. After lunch I was chatting with – there's a – there's a bunch of high school and college students here. And several of them were coming to this panel trying to decide their career paths. Both of you have talked about the need to develop math and science skills in a country that is falling behind.

So putting aside what can we do in that area, Admiral, what would you say to a high school student who says: I don't know whether I want to come to Cyber Command because of military culture? And, Wes, what would you say to somebody who said: I'm not sure corporate America's my place either. So make your pitch to the students who I know what to hear their career future.

DIR. ROGERS: So, not just Cyber Command, but I work out of the NSA side. I always tell people, look, we are not going to compete on the basis of money. I'm the first to acknowledge that. If the metric for you – and that is a choice you must make as an individual – if the metric for you is the financial side, then we're probably not your first choice. But if you care about a culture and an ethos of service to others, we're for you. If you want to be part of a mission that matters to this nation, we're for you. If you are into an ethos of service, we're for you. If you want to do some neat things that, quite frankly, legally you can't do anywhere else, we're for you. (Laughter, applause.)

MR. : I think you got them on the last one.

MR. SHANKER: OK, that was the sound bite for the recruitment poster, I'm sure.

MR. : Exactly right.

MR. SHANKER: All right. So, Wes, over to you, sir.

MR. BUSH: Let me just answer it more broadly. And I'll say the same thing that I say to the university students that I have the pleasure of interacting with so frequently because we're, like many companies in our industry, now working with so many universities on their cybersecurity programs. Now, you're going to have almost unlimited opportunities in this field. And I know it's a tough field. It is one that is demanding because it's not only a lot of mathematics and computer science and engineering that really have to converge in a – in this field of study to make someone proficient. It's tough, but it's worth it. Stick with it.

We're out trying to hire all of – all of you that we can possibly get. I know Admiral Rogers is as well. And as the recognition of the importance of this field continues to grow across industries, whether it's financial services or it's transportation or anything you can imagine, the demand for this skill set, I believe, is just going to continue to grow very, very rapidly. So as I

mentioned in my opening remarks, this is an area – an important area for great and in-depth cooperation between industry and government and the universities.

And I should mention, because I don't think we've said too much about what universities are doing in this regard, there are a lot of universities across our country that are working hard on this partnership, recognizing that this field is moving so fast that a university in isolation or even universities working together can't possibly keep up with it from an educational perspective. And they've reached out to government. They've reached out to industry. And we've formed some fabulous partnerships.

And my opportunity to get out and interact with the students that are – that are becoming a part of that curriculum, I'm blown away. The talent basis there is incredible. So stick with it. It's going to pay off for you.

MR. SHANKER: Thank you very much. First question here, please.

Q: Sydney Freedberg from Breaking Defense. There's a lot of talk about, you know, this is a domain. It's been elevated to that level. There is talk in the Navy about electromagnetic maneuver warfare that includes both cyber and more traditional jamming and spoofing. Talk in the Army about, you know, using this as an instrument – as a form of fires, for example.

But one thing that strikes me is when we try to apply these traditional military frameworks of maneuver or fires or domain, that nobody can just unplug large parts of the ocean while you're trying to send ships through it. You know, the private sector can't say, you know, you can't fly through the air here, we're going to block everything coming from your IP.

You know, how does the military – trying to operationalize this, trying to see this as more than a tech problem, but as a tactical and operational/strategic problem – you know, how do those old ideas get in your way because this domain is entirely artificial and, to a large extent, its existence, it – you know, it can flash on and off depending on what people in the private sector decide to do with the off button?

DIR. ROGERS: So, Sydney, I – you didn't use my name but I'm going to guess that this was directed at the military guy. (Laughter.)

Q: Sorry. I am looking straight at you, Admiral.

DIR. ROGERS: OK. And it was Sydney, right?

Q: Yes.

DIR. ROGERS: So, first comment I would make is if you think you can truly isolate yourself today in the interconnected world in which we're living, I don't think that's particularly realistic. I mean, I will often have people tell me, well, we'll just turn everything off. And I'm thinking, do you truly understand how complex your infrastructure is, and how many backdoors and how many connections that you've built into your framework that you probably don't even realize?

So the argument I made is, yes, I do believe cyber is an operational domain in which we conduct a variety of very traditional military evolutions. We maneuver. We reconnaissance, we do fires. I have no problem applying those, I think in part because it helps people understand what are you doing and why and what are you trying to achieve and what are some of the constraints – whether they be legal, rules of engagement, authorities. They help us also to better understand what are some of the constraints that we need to be mindful of.

MR. SHANKER: Thanks. Yes, please.

Q: Good afternoon, gentlemen. My name is Robert Nichols. I lead the government contracts group at Covington & Burling. I think everybody is familiar with USIS and what's happened in the last few months. They were breached by Iranians. They reported the breach to the government and they lost contracts as a result.

We talk a lot about cooperation between industry and government, but it strikes me that there are business consequences and financial consequences and legal consequences from third-party attacks on contractors, which are largely happening because contractors, unlike Home Depot or JP Morgan and Target – the reason they're attacked is because they're working for the government, they hold government secrets. Is your sense that there is a sober conversation going on between government and industry about the right allocation of risk between the two?

MR. BUSH: I'll take that one.

MR. SHANKER: Wes.

MR. BUSH: I think is an improving conversation. As with many other aspects of security when you are defense contractor or a government contractor, you have a certain set of obligations to ensure that you're doing the right things to protect that security. In physical security, they're far better defined. And you know, there are decades of ways of getting things done and standards. And many of them are actually in the contracts that you sign up to.

In cybersecurity they're less mature. They are maturing, though. And much of the work that the DOD has been focusing on is along those – (audio break) – best practices, how to create a set of standards that we all need to meet to make sure that we're doing the right things and to make sure that we're in the right place on risk and return. That's going to be the hardest part of this, the cost-benefit trade, because we can go way, way over on the side of spend a heck of a lot of money on this and may not have found the right balance and cost-benefit.

So I think that's probably the toughest part of the discussion right now. Now, I will tell you generally when an issue arises, the immediate response right now is spend what it takes to fix it. And we're all doing that. We're making sure we get everything fixed. As we gain more maturity in this and as we think about the better use of technology to have more resilient capability from a security perspective, I think we'll be able to find a better place in that trade between cost and benefit. So it is nowhere near as mature as physical security, for example, but it is an area of great focus. If you ask Frank Kendall this question, he will tell you that he and his team are spending a lot of time in progressing the maturity of the cybersecurity aspect for defense contractors.

Q: Thank you.

MR. SHANKER: Please.

Q: I'm David Craig (sp), a student at a local institution. This one's for you, Admiral. I don't know how much of it you'll be able to answer. Looking at –

DIR. ROGERS: That's the best kind of question. (Laughter.)

Q: Looking at, say, a 5(-year) or 10-year horizon, if an enemy nation state made an attack upon one of our critical infrastructures, what kind, or even what magnitude, of a retaliatory response would we be able to return, or would there be much of one at all?

DIR. ROGERS: Well, everything – that's such a broad – it was David, right?

Q: Yes.

DIR. ROGERS: I apologize. So David, that was such a broad scenario, let me say this. In cyber, I fully expect the same law that we use in terms of response in any other domain from a military perspective will apply: proportionality, you know, our ability to specifically discriminate. I don't expect cyber to be any different in that regard. And anything beyond that is just – the scenario you gave me was so broad, I don't know how to really answer it, other than –

you said you were in a local institution. This is not a prison, is it? (Laughter.) OK. I just want to make sure. You have guards here – (laughter).

MR. SHANKER: Thank you. Yes, please.

Q: My name is Meredith Walker. I'm an economist from Dallas and a member of the North Texas Crime Commission, and also a participant in the East-West Institute Cyberspace Cooperation Summits. So my question, for Admiral Rogers: You talked about the blur between private/public/government/national security. One blur I'm particularly concerned with is that between citizen and law enforcement and citizen and soldier. In my mind, we've all become boots on the ground in cyberspace. We're talking about are we going to have a cyber Pearl Harbor. But I'm remembering the worst death penalty in Imperial China was death by a thousand cuts.

What kind of recommendations do you have for our business community now that the battlefield extends to boardrooms?

ADM. ROGER: Well, first, I apologize to my panel mates. This reminds me a little bit of my confirmation hearing, where I kept saying to myself, you do realize the other guy next to me is a four-star who's going to be a combatant commander. (Laughter.)

MR. : Ask him something.

DIR. ROGERS: (Laughs.) That's right; ask him something.

Well, I think there's a couple things. First, what I always tell groups, businesses, the first step in solving any problem is recognition of the problem and accepting responsibility. So, A, if you're in a leadership position, whether it's a corporate sector, whether it's in government, it's acknowledging that we got an issue here that we all need to be a part of the solution, as opposed to, well, this isn't my problem, this is somebody else's problem, because I think there's a role for all of us.

I think the sector construct that the Department of Homeland Security has been putting together is a very powerful one for us. It's a great place for us to start, where like-minded businesses, like-minded elements of the same sector can pool their expertise, can share information with each other, can share insights with each other. I think that's a very powerful model. Because one of the things that concerns me – and I'm riffing a little bit off your question, but, you know, large corporations, as you heard Wes say, hey, they will apply the resources necessary to fix this, but what sometimes is it's the small and the mid-guy who says, look, I don't have that kind of money, I don't have those resources. Or if you're in the power segment,

for example: Hey, we're a regulated industry, I have to go – the only way for me to generate resources to address this problem is through rate hikes; I have to go to a regulatory board to get permission to do that. Nobody's really keen on hiking power rates or getting a regulatory board to say yes to the idea of, hey, I need resources for cyberdefense.

So I think the partnering and the sharing and the sector piece, whether that be in government, I think that's really the way to start, even as we're trying to work, you know, on the Congress and other things, the much more foundational legal, information, legislative kinds of things.

I apologize –

MR. SHANKER: Please.

MR. BUSH: If I could add to that, this framework that is now out, I would commend to any company that's just getting started on this. I think it is a very logical framework to use across an enterprise to think about how to provide the beginning levels of protection. So if a company is looking for a framework to start with, that's a good one.

DIR. ROGERS: I agree. I think that's a really good point.

MR. SHANKER: Well, I wish we could take more questions, but we have less than one minute left. And the Reagan Library chose me because I lived five years in Moscow and I run these meetings with Stalinist efficiency. (Laughter.)

MR. : Politburo!

MR. SHANKER: But I can't end the day without thanking our esteemed panel for very illuminating comments. I thank all of you for being such an attentive audience, and, of course, the Reagan Library for being our host today. Thank you all. (Applause.)

(END)