MARCH 12, 2013

OVERSIGHT: U.S. STRATEGIC COMMAND AND U.S. CYBER COMMAND

U.S. SENATE, COMMITTEE ON ARMED SERVICES

ONE HUNDRED AND THIRTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

WEBCAST: [*view*]

FULL TRANSCRIPT: [*view*]

WITNESSES:

General C. Robert Kehler [*view pdf*]
Commander, U.S. Strategic Command

General Keith B. Alexander, USA [*view pdf*]
Commander, U.S. Cyber Command

COMPILED FROM:
http://www.armed-services.senate.gov/hearings/event.cfm?eventid=0daf354e2970a9db3a6d0023abe58a27

HEARING TO RECEIVE TESTIMONY ON U.S. STRATEGIC COMMAND AND U.S. CYBER COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

TUESDAY, MARCH 12, 2013

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:35 a.m. in room SD–G50, Dirksen Senate Office Building, Senator Carl Levin (chairman) presiding.

Committee members present: Senators Levin, Reed, Nelson, Udall, Blumenthal, Donnelly, Hirono, Kaine, King, Inhofe, McCain, Sessions, Wicker, Ayotte, Fischer, Graham, Blunt, and Lee.

Committee staff members present: Peter K. Levine, staff director; and Leah C. Brewer, nominations and hearings clerk.

Majority staff members present: Joseph M. Bryan, professional staff member; Jonathan S. Epstein, counsel; Richard W. Fieldhouse, professional staff member; Creighton Greene, professional staff member; and Thomas K. McConnell, professional staff member.

Minority staff members present: Steven M. Barney, minority counsel; Ambrose R. Hock, professional staff member; Daniel A. Lerner, professional staff member; and Robert M. Soofer, professional staff member.

Staff assistants present: Kathleen A. Kulenkampff, Bradley S. Watson, and Lauren M. Gillis.

Committee members' assistants present: Carolyn Chuhta, assistant to Senator Reed; Jeff Fatora, assistant to Senator Nelson; Casey Howard, assistant to Senator Udall; Marta McLellan Ross, assistant to Senator Donnelly; Nick Ikeda, assistant to Senator Hirono; Karen Courington, assistant to Senator Kaine; Steve Smith, assistant to Senator King; Christian Brose, Paul C. Hutton IV, and Elizabeth Lopez, assistants to Senator McCain; Lenwood Landrum, assistant to Senator Sessions; Brandon Bell, assistant to Senator Chambliss; Joseph Lai, assistant to Senator Wicker; Brad Bowman, assistant to Senator Ayotte; Peter Schirtzinger, assistant to Senator Fischer; Craig Abele, assistant to Senator Graham; Charles Prosch, assistant to Senator Blunt; and Robert Moore, assistant to Senator Lee.

OPENING STATEMENT OF SENATOR CARL LEVIN, CHAIRMAN

Chairman LEVIN. Good morning, everybody. Today's hearing continues a series of posture hearings that the Armed Services Committee is conducting on our combatant commands. Today we receive testimony from the U.S. Strategic Command and the U.S. Cyber Command, a sub-unified command of the U.S. Strategic Command.

Let us welcome General Robert Kehler, the Commander of the U.S. Strategic Command, and General Keith Alexander, the Commander of the U.S. Cyber Command, wearing one of his hats, and I thank them both. We thank you for your great work. We thank you. If you would pass along our thanks to those who work with you for their service, we would greatly appreciate it.

This hearing comes at a time when the Department of Defense and other Federal agencies face the twin threat of sequestration and an expiring continuing resolution and we will want to hear from our witnesses what impact budget restrictions and uncertainty are likely to have on their programs and their operations over the coming months.

First, General Kehler, here are some of the issues that I hope you'll address this morning: First, are you satisfied with the status of our nuclear deterrence?

Second, are you satisfied with the National Nuclear Security Administration's ability to maintain our nuclear stockpile so we can ensure without testing that the stockpile remains safe and meets military requirements?

Third, do you believe we have the ability to protect our space assets and to reconstitute them if necessary, given the growing congested and contested nature of space?

Fourth, the Department of Defense is allocated a block of the electromagnetic spectrum that connects our space, cyber, and electronic warfare assets to our forces. STRATCOM is the lead combatant command for synchronizing spectrum operations. How concerned are you about preserving the Department of Defense's access to this block of spectrum, given the competing pressure to allocate more spectrum towards commercial use?

And finally, what is your view on the links between the space and cyber domains and the potential for integration of capabilities and operations in both domains?

Now, relative to the Cyber Command: For years and especially since the Department proposed to establish a Cyber Command, the Armed Services Committee has emphasized the lack of an effective, mature policy, strategy, rules of engagement, doctrine, roles and missions, and command and control arrangements that are so critical to managing this vital but complex new domain. Progress in this area has been slower than we desired, but appears to be picking up some steam.

After Congress failed to pass comprehensive cyber security legislation, the President developed and issued an executive order aimed at improving the security of critical infrastructure and to better share cyber threat information. The President has also recently issued a classified presidential policy directive governing cyber operations. The Department of Defense, working through the interagency planning process, has developed a set of emergency ac-

tion procedures for cyber crisis situations similar to the processes in place and regularly exercised for nuclear and ballistic missile defense operations. The Joint Staff is ready to issue is first-ever document covering cyber doctrine. Finally, we understand that the Joint Staff states that it will soon issue rules of engagement for military commanders.

The fact that these foundational policy frameworks and planning actions are now just taking shape serves as a stark illustration of how immature and complex this warfare domain remains.

The National Defense Authorization Act for Fiscal Year 2013 included a sense of Congress provision that raised serious concerns about the complications that could be caused by making Cyber Command a full unified command. The NDAA also included a provision that requires the Secretary of Defense to create a process for designated defense contractors to report to the Department when networks containing DOD information are successfully penetrated, and we'd be interested in hearing the views of our witnesses on our recent important addition to the law in that regard.

Meanwhile, China's massive campaign to steal technology, business practices, intellectual property, and business strategies through cyber space continues and it continues relentlessly. Last year's report by the National Counterintelligence Executive, plus the recent report by Mandiant Corporation and the very recent Cyber National Intelligence Estimate, all leave little doubt that China's actions are a serious threat to our Nation's economic wellbeing and to our security.

It's long past time when the United States and our allies, who are also being attacked in this way, should be imposing costs and penalties on China for their behavior. The Defense Science Board released a study in January that provides a grim assessment of the ability of the Defense Department and the owners of critical infrastructure to defend vital systems and networks against capable adversaries. In light of vulnerabilities highlighted in that report, the Defense Science Board suggests building resilience into our forces and infrastructure in addition to trying to improve defenses.

We look forward to hearing from General Alexander on the extent to which Cyber Command is capable of preventing adversaries from seriously damaging our critical infrastructure.

We have a long way to go to protect our vital infrastructure and services from damaging cyber attacks. That's why I supported the Lieberman-Collins bill that the Senate failed to act on last year. That's the reason why the President issued his recent executive order. And that's the reason why all of us are deeply concerned about this issue and look to working together to try to address the threat that exists particularly from China in that area.

Senator Inhofe.

STATEMENT OF SENATOR JAMES M. INHOFE

Senator INHOFE. Thank you, Mr. Chairman. I agree with all of your statements and I am very concerned. I think it's a very significant hearing with both Generals Kehler and Alexander. I want to thank both of you for the time that you've given me personally to help me along, particularly you, General Alexander, because it's

a tough issue that not many of us understand, certainly not as well as you do.

The importance of our nuclear forces for the security of the Nation and that of our allies was made clear by Deputy Secretary of Defense Carter before this committee just last month. Even in the face of the drastic budget cuts and all of this brought about by the sequestration, he said: "We in the Department of Defense will try to protect our nuclear capabilities to the maximum extent possible," and that "The nuclear deterrence is the last thing that you want to do serious damage to." While we all agree with that in this room, there are a lot of people out there who really don't, because it's not as well understood as the conventional threats that face us.

It's troubling, General Kehler, the statement that you made to the House Armed Services Committee last week. As the sequestration impacts continued to grow, you said: "Reduced readiness and curtailed modernization will damage the perceived credibility of our capabilities, increasing the risk to achieve our primary deterrence and assurance objectives." You're exactly right and I'm glad you made that very bold statement. In other words, if we don't consistently demonstrate a commitment to modernizing our nuclear deterrent both in words and in funding, our allies might lose confidence in the U.S. nuclear umbrella, while potential adversaries could be led to believe that they hold a nuclear advantage over the United States, which I think that gap is closing. It disturbs me.

While the President has been AWOL on the issue, I was pleased to hear him acknowledge in his State of the Union message the need to strengthen our own missile defense capabilities.

Now, on the cyber end of it, I do agree—and I'm skipping a lot of my opening statement because some of the contents made references to China, because that is a fact and it would be redundant. But this administration has thus far failed to implement an effective cyber deterrence strategy that dissuades those seeking to hold our economic and national security interests at risk in cyber space. Not a day goes by where it is not reported that our national security is being exploited in the cyber domain. Nation states such as Iran and China have been exposed publicly for attempting to gain access to national secrets and undermine our defense and economic interests. Criminal and terrorist organizations continue to actively pursue and exploit malicious capabilities, with little resistance or consequences.

Despite my concern on White House policy, progress is being made within the Department of Defense. Organizations and structure are maturing and the Department is beginning to rise above the inter-agency gridlock that's sought to undermine the Pentagon's reach.

I'm happy to welcome General Alexander and applaud him and his team for the progress that they have made in just the last year in developing the foundation, the foundations necessary to start developing an offensive cyber capability. I will confess to them the conversation that you and I had. My concern over your future is to make sure you're there long enough to we can find somebody who understands this very complicated issue and can deal with it as effectively as you have.

Certainly more must be done and the resources must be allocated. However, progress is being made and I'm pleased to see the Department is moving past the defense-only mind set. I think we need to get beyond that so that we can understand that there's an offensive angle to this that's going to have to be pursued.

So under the sequester every Department of Defense account will be subject to the highest level of scrutiny. The threats we face, however, are blind to our fiscal woes and are emboldened by our dysfunction. Every dollar we spend has got to be maximized, and those going toward nuclear deterrence, missile defense, and cyber should be placed at a premium. That's nuclear deterrence, missile defense, and cyber; that's what is the most significant part, I believe, of the hearing that we're having today.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you so much, Senator Inhofe.

General Kehler.

STATEMENT OF GEN. C. ROBERT KEHLER, USAF, COMMANDER, U.S. STRATEGIC COMMAND

General KEHLER. Good morning, sir. With your permission, I'd like to make my full statement a part of the record, please.

Chairman LEVIN. It will be.

General KEHLER. Good morning, sir, and Senator Inhofe, distinguished members of the committee: I am honored to join you today. It's a privilege to begin my third year leading the outstanding men and women of United States Strategic Command.

I'm also pleased to be here with General Keith Alexander, whose responsibilities as the Commander of U.S. Cyber Command and Director of the National Security Agency cover some of the most critically important national security subjects. General Alexander and I and our staffs are in constant contact and I greatly value his leadership, his vision, and his counsel.

Uncertainty and complexity continue to dominate the national security landscape, even as the United States transitions from a decade of active conflict in Southwest Asia. Uncertainty and complexity make this transition unlike any we have experienced in the past. Many regions of the world remain volatile and increasing economic and infrastructure connections mean regional issues can quickly have global consequences. Events over the past year validate this perspective.

Since my last appearance before the committee, we have seen violent extremists continue to act against or threaten U.S. interests, citizens, allies, partners, and our Homeland. Cyber activities increased in both quantity and intensity, with the potential for greater exploitation of U.S. intellectual property, institutions, and critical infrastructure.

Iran's nuclear ambitions remain concerning. North Korea conducted a missile launch in violation of its obligations under multiple U.N. Security Council resolutions and announced last month it conducted another nuclear test. Civil war continues in Syria. Russia and China continue to improve and demonstrate their strategic capabilities.

Fiscal uncertainty is adding unique challenges. Not only are the additional sequestration reductions steep, but the law allows little

flexibility in how to apply them, and we're working from a continuing resolution while the services are transitioning contingency needs to the base budget—all of this during a time when continued readiness is essential, modernization is overdue, violent extremists remain active, threats in space and cyber space are increasing, and the possibility of nuclear and ballistic missile proliferation persists.

As we confront these challenges, our enemies and potential enemies are watching. In this uncertain and complex world, STRATCOM remains focused on conducting the missions that are most critical to protect our core national security interests, and my priorities support this focus. Our fundamental purpose remains constant: With the other combatant commands, we must deter, detect, and prevent attacks against the United States, assure our friends and allies of our security commitments to them, and, if directed, employ appropriate force to achieve national objectives should deterrence fail.

To do this, our men and women wield a range of complementary capabilities to create the tailored effects the Nation needs. Our primary objective is to prevent conflict by influencing in advance the perceptions, assessments, and decisions of those who would consider threatening our vital national interests. Ultimately this requires the continuing credibility of America's military capabilities, brought to bear in concert with other elements of national power.

While our heritage in Strategic Command is nuclear and our nuclear vigilance will never waver as long as those weapons exist, today's STRATCOM is far more diverse and versatile than ever before. Mr. Chairman, I am pleased to report that STRATCOM is capable of executing its assigned missions today. However, given the potential impact fiscal uncertainty and declining resources could have on STRATCOM, I am concerned that I may not be able to say the same in 6 months or a year.

I'm most concerned with the impact financial uncertainty is having on our people. Uniformed and nonuniformed members alike have managed the effects of sustained high-stress combat deployment and operational tempos. They willingly take personal risks for their country, but they are fearful of taking financial risks for their families. Hiring restrictions, salary freezes, and the likelihood of unpaid furloughs are especially troubling to our civilians. And by the way, civilians comprise about 60 percent of the STRATCOM headquarters staff. They hold key leadership positions. They represent critical expertise and they make up much of the essential workforce which provides crucial functions like intelligence, maintenance, and sustainment.

Because they are such dedicated patriots, I believe our military and civilian members will cope with the effects of financial uncertainty in the near term. But I worry that over time our most experienced professionals will retire early and our best young people will leave to pursue more stable opportunities elsewhere. We are detecting hints of that now. Beyond the human dimension, sequestration will eventually impact the command's readiness and curtail growth in new areas like cyber and cyber defense.

Now, even though the services are trying to give STRATCOM's missions as much priority treatment as possible within the law—and you heard that from Deputy Secretary Carter last month—we

could not remain immune. So while the immediate impact will vary by command, overall in STRATCOM the effect is a bit like an avalanche. Seemingly small initial impacts are going to grow. As time passes, we will see greater impacts and potential impacts to things as Senator Inhofe mentioned, like the nuclear deterrent, to Global Strike, to missile warning and missile defense, the situational awareness in both space and cyber space, and to our support to warfighters around the globe.

In the longer term, continuing in this financial path will affect STRATCOM's modernization and long-term sustainment needs, potentially eliminating or jeopardizing a number of important recapitalization efforts. And of course, ultimately such reductions could impact our ability to deter and assure.

Mr. Chairman, STRATCOM's responsibilities have not changed, but the strategic and fiscal environment in which we must carry them out is much different than a year ago. I remain enormously proud of the superb men and women I am privileged to lead and potential adversaries must know that we can meet our mission responsibilities today. But the pathway we're on is creating growing risk to our defense strategy and our ability to execute it.

I look forward to working with this committee and Congress on these difficult and complex challenges. I will certainly carry back your message of appreciation for the men and women who we are privileged to be associated with, and I look forward to your questions. Thank you.

[The prepared statement of General Kehler follows:]

Chairman LEVIN. Thank you very much, General Kehler.

General Alexander.

STATEMENT OF GEN. KEITH B. ALEXANDER, USA, COMMANDER, U.S. CYBER COMMAND

General ALEXANDER. Thank you, Chairman Levin, Ranking Member Inhofe, and distinguished members of the committee. It's an honor to lead the men and women of Cyber Command. It's also a tremendous honor to work with and for General Bob Kehler. He has been truly supportive of everything that we're trying to do in Cyber Command, and he's the only one that's nice to me, and as an intelligence officer that's unique. [Laughter.]

You know, it does give me great pleasure to come here today and talk to you about the great things that we're doing at Cyber Command, but also to address some of the questions that you've put on the table and I think some of the questions that have troubled the committee in the past. I will try to answer some of those. I cannot answer all of those today.

First, the role of the Defense Department. As you know, it takes a team to operate in cyber space and we've talked about this team approach. But at times I think in talking about the team approach we're not clear on who's in charge when. For defending the Nation in cyber space or in any way when the Nation is under attack, that's a Defense Department mission and that falls to STRATCOM and U.S. Cyber Command in cyber space. We are also responsible for supporting the combatant commands in their cyber space operations and for defending the Defense Department networks, as well as supporting DHS and defending critical infrastructure. We must

also gather important threat information to protect, prevent, and mitigate and recover from cyber incidents in support of DHS and FBI.

As I said, no single public or private entity has all the required authorities, resources, or capabilities to respond to or prevent a serious cyber attack. I work closely with Secretary Napolitano and Deputy Secretary Lew at DHS and with Director Bob Mueller at FBI. We all see eye to eye on the importance of cyber, of supporting each other in these cyber missions. FBI's role in domestic space is absolutely critical to disrupting cyber criminals and stopping cyber attacks and leading investigation in those areas. DHS' work to defend the government and to strengthen the security posture of critical infrastructure is essential. They are the lead for domestic cyber security and help protect Federal networks and critical infrastructure.

To act quickly, we must have clear lanes of responsibility and rules of engagement. We all recognize the private sector plays a key role in this area and having the ability to work with the private sector is important to us and one of the key reasons we need cyber legislation. The EO issued last month, as you noted, Chairman, is a step in the right direction, but it does not take away the need for cyber legislation.

I'd like to point out before I go forward that civil liberties, oversight, and compliance are key for both Cyber Command and NSA in operating in this space, and we take that requirement sincerely and to heart and ensure that we do every part of this properly. I would also point out that we can do both. You can protect civil liberties and privacy and protect our Nation in cyber space. I think that's one of the things that we need to educate the American people on, how do we do that, how do we work with industry to do this.

If you look at the strategic landscape—you've hit on much of that, Chairman. When you look at the strategic landscape from our perspective, it's getting worse. Cyber effects are growing. We've seen the attacks on Wall Street over the last 6 months grow significantly, over 140 of those attacks over the last 6 months. Last summer in August we saw a destructive attack on Saudi Aramco where the data on over 30,000 systems were destroyed. If you look at industry, especially the antivirus community and others, they believe it's going to grow more in 2013, and there's a lot that we need to do to prepare for this.

Let me just talk a little bit about what we're doing to prepare for it from our perspective. As many of you know, we are already developing the teams that we need, the tactics, techniques, procedures, and the doctrine for how these teams would be employed, with a focus on defending the Nation in cyber space.

I would like to be clear that this team, this defend the Nation team, is not a defensive team; this is an offensive team that the Defense Department would use to defend the Nation if it were attacked in cyber space. 13 of the teams that we are creating are for that mission set alone. We're also creating 27 teams that would support combatant commands and their planning process for offensive cyber capabilities. Then we have a series of teams that would defend our networks in cyber space. Those three sets of teams are

the core construct for what we're working with and the services to develop our cyber cadre.

As you noted, the key here is training our folks to the highest standard possible. I think that's the most important thing that we are on the road to and it's the most important partnership that we have with NSA and others, is ensuring that the training standards that we have for our folks is at the highest level.

I'd just like to hit on a few key points that we're doing to develop this cyber strategy. You mentioned command and control. General Kehler, the combatant commands, the service chiefs and I are all looking at the command and control, how we work this with the other combatant commands. That's a key issue. We have done a lot of work on that and we've ironed out how the joint cyber centers at each combatant command would work with Cyber Command and how we push information back and forth and how we'd have operational control and direct support of teams operating in their area. More to do in this as the teams come on line.

One of the key things that we have to address is situational awareness, how do you see an attack in cyber space. Today seeing that attack is almost impossible for the Defense Department. Specifically, an attack on Wall Street would probably not be seen by us. It's going to be seen by the private sector first, and that's a key need for information-sharing. It has to be real-time to the Defense Department, Department of Homeland Security, and the FBI, all at the same time, one government team. If we're going to respond in time to make a difference, we have to see that in real time. And those companies that are sharing that information with us have to have liability protection.

We're also building the operational picture that we would share, Cyber Command would share, with the other combatant commands, with DHS, with FBI, and with other national leaders the operational picture that we would share, Cyber Command would share, with the other combatant commands, with DHS, with FBI, and with other national leaders.

We need a defensible architecture, and you've heard about the joint information environment, our cloud security. Not only is that more defensible, it was created by some of our folks to come up with the most defensible architecture we could make; it's also more secure. It's not perfect. No architecture is perfect in security, but it is better than where we are and it's cheaper, and it's something that we should push for.

Mr. Chairman, you mentioned authorities, policies, and SRO. We're working that hard, but, as you've already stated, this is a new area for many of our folks, especially within the administration, within Congress, and the American people. Setting those right, we're being cautious in ensuring that we're doing that exactly right and sharing the information we have with Congress.

So in conclusion, from my perspective no one actor is to blame for our current level of preparedness in cyber space. Many don't understand how serious the threat is, so we need to educate people on this threat. We must address this as a team, sharing unique insights across government and with the private sector. We must leverage the Nation's ingenuity through an exceptional cyber workforce and rapid technological innovation. The U.S. Government has

made significant strides in defining cyber doctrine, organizing cyber capabilities, and building cyber capacity. We must do much more to sustain our momentum in an environment where adversary capabilities continue to evolve as fast or faster than our own.

Mr. Chairman, that completes my statement.

[The prepared statement of General Alexander follows:]

Chairman LEVIN. Thank you so much, General Alexander.

We'll have an 8-minute first round.

General Kehler, let me start with you. The Defense Science Board released a report in January that has a number of noteworthy assertions and I'd like you to start with this assertion and comment on it. The report says that: "Our nuclear deterrent is regularly evaluated for reliability and readiness." But then it says: "However, must of the systems have not been assessed against a sophisticated cyber attack to understand possible weak spots."

Can you comment on that? And then, General Alexander, I'm going to ask you to comment on that as well.

General KEHLER. Mr. Chairman, in general terms I agree with the thrust of the DSB report. I think that they've pointed out a number of places that we need to do better. Let me hone in specifically on the nuclear command and control system for just a second. Much of the nuclear command and control system today is the legacy system that we've had. In some ways that helps us in terms of the cyber threat. In some cases it's point to point, hard-wired, which makes it very difficult for an external cyber threat to emerge.

However, we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves. We do evaluate that. I think, as the Defense Science Board pointed out, in terms of an end-to-end comprehensive review I think that's homework for us to go and accomplish.

In what we have done to date and the pieces that we have looked at to date, which has been going on for quite some time, I am confident today that the nuclear command and control system and the nuclear weapons platforms themselves do not have a significant vulnerability that would cause me to be concerned. We don't know what we don't know, and I think what the Defense Science Board pointed out is that we need a more comprehensive recurring way to evaluate such a threat. And on that I am in agreement with them.

But I don't want to leave you with the perception that I believe that there is some critical vulnerability today that would stop us from being able to perform our mission or, most importantly, would disconnect the President from the forces. I believe we have looked at that. I receive those reports. We've done a lot more over the last one to two years. But I think in general terms the Defense Science Board is right. We need to do better at exercising such threats and we need to do better working with Keith and his team to detect such threats, red teaming, as the DSB suggested. I think we have a way to go here until we put a punctuation mark at the end of the sentence.

Chairman LEVIN. Is that underway? Is those kinds of continuous reviews underway?

General KEHLER. Yes, sir, they are. In fact, the pace of those things has increased. We completed, for example, a review of the Minuteman intercontinental ballistic missile system not so very long ago. We have a little bit different problem, of course, with aircraft that are in flight and submarines that are under way. We're confident in the connectivity to those.

But I think that this is something we're going to need to increase the volume of the gain here on this whole issue.

Chairman LEVIN. Thank you.

General Alexander, do you want to add anything to that?

General ALEXANDER. Mr. Chairman, I would just add three key points. First, General Kehler has led a series of meetings on the nuclear command and control, working with both the NSA side and the Cyber Command side, to look at vulnerabilities and address those. I would tell you I think they've done a great job over the last 6 months in doing that and I think that's moved in the right direction and leads to the conclusion that General Kehler just gave.

I would also add that our infrastructure that we ride on, the power and the communications grid, are one of the things that is a source of concern, how you maintain that. Now, we can go to backup generators and we can have independent routes, but it complicates significantly our mission set. And it gets back to, in the cyber realm how the government and industry work together to ensure the viability of those key portions of our critical infrastructure.

Chairman LEVIN. General Alexander, there's a real, real theft going on of our technology and our business strategies, our intellectual property, by China particularly, not exclusively but by China. The question is, of course, what is it going to take to stop that practice? I will Reserve that question for later if there's time.

But I guess the real question I want to focus on right now is whether the intelligence community can determine not only which Chinese government organizations are stealing our intellectual property, but also what Chinese companies may be receiving that intellectual property and using it to compete against U.S. firms?

General ALEXANDER. Walking a fine line, Mr. Chairman, I would say that the intelligence community has increased its capabilities in this area significantly over the last 7 years, and I can give you specific examples in a classified setting.

Chairman LEVIN. Because it's really important that we act. I think there's a consensus here in Congress that this has got to stop and that we've got to find ways of preventing it, stopping it, responding to it in every way we can. This is a threat which is at the moment probably an economic threat, but some day could be a physical and a military threat as well. So we will take that in a classified setting.

General Alexander, you mentioned three teams that you're creating, I believe. Is there a timetable for those three teams?

General ALEXANDER. Chairman, we're working with the Services on that. The intent is to roughly stand up one- third of those, the first third, by the end of September of this year, the next third you September of the next year, 2014, and the final third you September 2015. The Services are on track. In fact, I would tell you great kudos to the Service Chiefs because they are pushing that

faster. The key part of that is training. I am extremely proud of the rate that they're pushing that on.

Chairman LEVIN. General Alexander, you mentioned the executive order. You've indicated that information-sharing is needed in real time. Give us your personal view as to why Congress needs to pass cyber legislation and what needs to be in there? What is missing now that needs to be in legislation which Congress hopefully will pass?

General ALEXANDER. Well, there's three key elements that I believe personally that needs to be in cyber legislation: first, the ability for industry to tell us in real time—and this is specifically the Internet service providers—when they see in their networks an attack starting. They can do that in real time. They have the technical capability, but they don't have the authority to share that information with us at network speed. And they need liability protection when we share information back and forth and they take actions.

The third part is more difficult and the Executive order in part addresses that. That's how do we get the networks to a more defensible state. It's like your own personal computers; how do we set the standards without being overly bureaucratic, but how do we set the standards so that the power grid, our communications infrastructure, banks and the government can withstand cyber exploits and attack? That resiliency needs to be built in.

I think what the executive order offers us is a way of discussing that with industry, led by Pat Gallagher, Dr. Pat Gallagher at NIST, would allow us to sit down with different sectors of industry and get their insights on the most efficient way of doing that and, coming back then from Congress, how do we incentivize them for moving forward and in some cases, for example the power companies, how do we help move there through regulatory processes.

Chairman LEVIN. Just to complete that point, you talk about the ability to communicate. You talk about the authority to share. Do we need legislation to authorize the sharing? That's the privacy piece of it?

General ALEXANDER. Chairman, it is the authority for them to share back information on the networks to the government. That's the part that needs to be in there.

Chairman LEVIN. All right. But that's essentially a privacy or a commercial protection of secrets, of proprietary information, issue?

General ALEXANDER. In combination, and I think it goes to some of the previous acts that have been there on computer and protection that's out there. I think what we have to do is tell them it's okay to share this level of information with the government. Specifically from our perspective, that information that we need to share is the fact of an exploit or an attack that's coming in.

We need to have it in real time. The complication, to really get to the point of your question here, is when the government shares back signatures it becomes more complicated because some of our capabilities are classified. So we have to have a way of giving them classified information that they would have to protect, and then if they see that classified information, think of this as going up to New York City on the New Jersey Turnpike. The EasyPass would see a car going by. What we're telling the Internet service provider

is if you see a red car tell us that you saw the red car, where you saw it, and where it's going.

In cyber space it would be they saw this significant event going from this Internet address to this target address, and they could tell us that at network speed and they could stop that traffic. It is important to recognize the role of industry because government could not easily scale to what the Internet service providers could do. It would be very costly, very inefficient. So we're asking industry to do that.

Chairman, that does not get into the content of those communications. I think it's absolutely important for people to understand we're not asking for content. We're asking for information about threats. Think of that as metadata.

Chairman LEVIN. And you're aware of the fact that I the last defense authorization bill we put in a requirement that industry that has classified—that has clearance for classified information is required to report threats to the government, and the regulations and rules for that are currently being written and I presume you're having an input in that; is that correct?

General ALEXANDER. That's correct. We're working with them. The issue would be with the defense industrial base, would be they don't see all the threats coming in all the time. Oftentimes the threats that we see have gotten in long before. So I think we need a total approach. I think that's a good step in the right direction.

Chairman LEVIN. What, the law that we wrote?

General ALEXANDER. Yes.

Chairman LEVIN. Okay. Thanks. Thank you.

Senator Inhofe.

Senator INHOFE. Thank you, Mr. Chairman.

I'm going to just ask for some brief answers to a couple of questions here. General Kehler, there seems to be unanimity in drawing the relationship between the nuclear reductions and nuclear modernization. It's been stated several times, and I will quote Secretary Gates, who said: "When we have more confidence in the long-term viability of our weapons system, then our ability to reduce the number of weapons that we must keep in the stockpile is enhanced." Do you agree with that and with the linkage in general that I'm referring to?

General KEHLER. Yes, sir, I do.

Senator INHOFE. Would you take that last statement, that says "When we have more confidence in the long-term viability of our weapons system," is there reason to believe that we do now have more confidence? Have we done what's necessary to have that, to earn that confidence in the existing system?

General KEHLER. Sir, I'm confident in the deployed weapons today. I am confident in the stockpile that provides the sustainment spares and the hedge against any technical failure that we might experience. I'm confident in that stockpile today. Every year my predecessors, the commanders of Strategic Command prior to me, and I are responsible to provide our assessment of the stockpile, and through this year I can certify.

Senator INHOFE. You feel you've had the resources necessary to do that to your expectations and to ours?

General KEHLER. Yes. Although the resources have increased over the last couple of years and that has helped us, I think that the resources were dwindling to an unacceptable point.

Senator INHOFE. Let me get into the homeland missile defense. You know, we've said for quite some time that there's more concentration—or less concentration on the homeland part of the missile defense. I'm referring to, of course, the number of ground-based interceptors going down under this administration from 44 to 30, but it's really more than that because there were 10 of them that would have been part of the Poland ground-based interceptor, which would have been more for protection of the eastern part of the United States.

It was kind of interesting because I had Vaclav Klaus in my office yesterday and we were talking about a conversation we had many years, not too many years ago, where I'd made the statement—or he made the statement to me, he said: Are you sure now, if we put our radar system in the Czech Republic and agree and do what's necessary in Poland for a ground-based interceptor for the Western Europe and Eastern United States, that you won't pull the rug out from under us? And of course I said yes. But we did anyway.

Now we're looking at where we are today and I would ask you, General Kehler, do you think we should—are you satisfied with the numbers that we've gone down to in terms of our ground-based interceptors and do you think that we should be—there are a lot of options I'll ask you about in a minute. Are you satisfied with the number of ground- based interceptors we have right now at 30?

General KEHLER. I am satisfied that we can defend against a limited attack from North Korea today with 30. I think——

Senator INHOFE. What about Iran?

General KEHLER. I am confident that we can defend against a limited attack from Iran, although we are not in the most optimum posture to do that today.

Senator INHOFE. Well, that's—yes, I think you're being a little too cautious—not cautious enough here when you say a "limited attack," when our intelligence has shown us that Iran is going to have the capability and a delivery system by 2015. And we're looking at what we have today with some options there. They're talking about possibly an option on the East Coast, an option on additional ground-based interceptors—I think you'd probably say it's not necessary—at Fort Greely, but to enhance our capability.

I'm concerned, as I always have been going all the way back to the Poland operation that was pulled out, with what was going to happen as far as the East Coast of the United States. I know you're somewhat cautiously confident. How would you characterize your level of confidence in the protection of the eastern part of this country with the capability that we have today?

General KEHLER. Again, cautious. And it doesn't provide total defense today.

Senator INHOFE. What about the idea of a third site in the United States?

General KEHLER. It is under consideration along with, as importantly, this sensors that will be important for the threat from Iran.

Senator INHOFE. Okay, I'm concerned when you talk about SM–3 Block 2A missiles. The date of that I believe currently that we could expect that would be 2018, is that correct?

General KEHLER. Around '18, yes, sir.

Senator INHOFE. And the capability that I've been concerned about with Iran is 2015. I would share with you and I'd like to have you send to me your level of confidence about what's going to happen, what our capability is in that three-year interim time.

General KEHLER. Yes, sir.

Senator INHOFE. That can be for the record, if you would do that for me.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator INHOFE. Let's see. Let's go to, if we could, to General Alexander. First of all, you've been very helpful to me in bringing to my attention some of the things that I—some of my shortfalls in knowledge, as I've confessed to you, on this whole issue. Yet I consider it to be so incredibly important. Right now, as you're well aware, the mainframe computers, while could be considered a relic of the 80s and the 90s, of the past, they are still integral to our core infrastructure and have unique security vulnerabilities that are not as well appreciated at this endpoint in security.

Do you agree that layered defenses are essential and that the efforts must be made to ensure our mainframes receive comparable attention on the vulnerability protection? It seems to me that most of the focus is on where all of the data is stored and all the new stuff that's coming on, and are we adequately protecting the mainstream, mainframe components of our systems?

General ALEXANDER. Senator, as we've discussed, I believe there's more work that needs to be done in protecting the mainframe computers and that portion of the total information infrastructure. It's not the only vulnerability and probably not the most frequent one that we see, but it's an important one to address because it is at the heart of many of our systems. As you've stated, it is one of the ones that we don't normally look at. But it is one that our information assurance folks are addressing and it's one, as you stated, that's key to a layered defense.

Senator INHOFE. I think that's important, because what you hear is the new systems coming on more than the mainframe. I'm glad to know that you'll be paying adequate attention to that relative to some of the new innovations that we see.

There was an article in the Wall Street Journal, I think it was yesterday, that talked a little bit about the banks are seeking help on Iran cyber attacks. It says "Financial firms have spent millions of dollars responding to the attacks, according to bank officials, who add that they can't be expected to fend off attacks from a foreign government."

Then further down in the article it says: "U.S. officials have been weighing options, including whether to retaliate against Iran. Officials say the topic was discussed at high-level White House meetings a few weeks ago, a U.S. official said, adding, 'All options are on the table.'"

Could you address this for me?

General ALEXANDER. Senator, what I can do is hit more theoretical and then in a closed session address that more specifically, that question. But I think this gets to the heart of, so how do we defend the country and when does the Defense Department step in to defend the country, and what are the actions that the Internet service providers can do, and what's the most logical approach to this? Why I say logical is that distributed denial of service attacks, those are what mainly today are hitting Wall Street. Those types of attacks are probably best today, if they're at the nuisance level, mitigated by the Internet service providers.

The issue that we're weighing is when does a nuisance become a real problem and when are you prepared to step in for that. That's the work that I think the administration is going through right now in highlighting that. In order to do that, it gets back to the question the chairman had asked about information sharing. For us to stop this at network speed, we've got to see it at network speed, and that's going to be key to helping the banks and others.

I do see this as a growing problem and I believe this is one of the problems that the antivirus community and others have brought forward to say, here's what you're going to see in 2013. What we're seeing with the banks today I am concerned is going to grow significantly throughout the year. We have to address it.

Senator INHOFE. I appreciate that.

Then lastly, just for the record, General Kehler, I have been concerned about our allies losing confidence in the strength of our umbrella that's out there, and I'd like to have you—we all remember during the New START Treaty, which I opposed, the President was very specific on the things that he was going to do. I look at these things and I see that they haven't, with specific reference to the B61 bomb, the warheads of 78 and 88 and the air-launched cruise missiles, the Los Alamos processing facility. These are all behind the schedule that was put out back during the New START Treaty.

So for the record, I'd like to have you evaluate what we have done that we should have done and were told was going to be done if that treaty would pass, if you would do that for the record.

General KEHLER. Yes, sir, I will.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator INHOFE. Thank you.

Chairman LEVIN. Thank you, Senator Inhofe.

Senator Reed.

Senator REED. Thank you very much, Mr. Chairman.

Thank you, gentlemen, for your service.

General Kehler, in your discussions with Senator Inhofe you talked about the capacity to withstand, I believe, a limited attack from a country like North Korea or Iran. I think it's important to sort of determine what that means. Their existing capabilities would allow them only to mount a limited attack or they could mount a limited attack and something more than that? I.e., are we capable of defending today against what they have, and at what point do you feel that they could go beyond a limited attack?

General KEHLER. Senator, let me split that into two different questions. There's a question for the theater and the theater-class ballistic missiles, where the numbers are large and we continue to

try to deploy capabilities to be able to blunt such a large ballistic missile attack in theater.

Senator REED. Which would not be against the United States. It would be against regional powers.

General KEHLER. Regional powers, our allies or forward forces, etcetera, and perhaps in some cases Guam and other U.S. territory.

Senator REED. But not the continental United States.

General KEHLER. Yes, sir.

Then the second question is about a limited threat to the United States, and the current ballistic missile defense system is limited in two important ways: number one, in terms of the size of raid, if you will, that it could deal with; and second in terms of the technological capability of it. So our system is limited. It is limited in terms of the size—and sir, before I say it's X number of ballistic missiles, what I can say is we are confident we could defeat a threat from North Korea today. But, given the potential progress we are seeing from them, we are considering right now whether we need to take additional steps.

Senator REED. That's a fair response. But today you feel confident you could protect the continent of the United States from an attack. And then the question is their technology, how fast it evolves.

General KEHLER. Yes, sir.

Senator REED. And you're considering that, as you must.

General KEHLER. And numbers and whether they evolve in terms of an intercontinental threat. And we're working with the Intelligence Community on that to see if we can't scope that. But that has our attention. Their activities have our attention and it has our concern.

Senator REED. Thank you.

Let me shift gears slightly, and that is the architecture of our nuclear deterrence has been the triad, sea, air, and land. One aspect is the replacement of the *Ohio*-class ballistic missile submarine. That's slipped a bit. Can you give us your assessment of can we allow additional slippage or that's something we have to get on with?

General KEHLER. I think we have to get on with the replacement for the *Ohio*-class submarine. I support the triad. I continue to support the triad. I think that what it brings to us still are the three big attributes: survivability, flexibility, and responsiveness. And that confounds an attacker.

I think that continues to serve us well, and of course the most survivable of the legs is the OHIO replacement. As far as we can see into the future, I think we're going to require a replacement for the *Ohio* class. Here's the interesting part. They will reach a date certain that they are no longer capable of going to sea and being used the way they're used today. The Navy is working very hard to make sure we understand that time with clarity. We intend to keep those submarines longer than any other submarines we've ever had before. So I think we will reach a point that we must have a replacement and I believe we understand where that point is, and the current program puts us right about there.

Senator REED. Thank you.

Let me ask a question to both of you which involves the triad. You made the point that the most invulnerable leg of the triad is the undersea, the submarine. There's been lots of discussion of the potential for disruption of the electric grid as one of the major ways to inflict damage on the United States. To what extent, General Kehler, are your land-based assets, the missile silos and the airfields, dependent critically on the local grid that could be taken down and therefore, either wittingly or incidentally, two legs of the triad could be knocked out without an explicit kinetic blow?

General KEHLER. Sir, the nuclear deterrent force was designed to operate through the most extreme circumstances we could possibly imagine. So I am not concerned that a disruption in the power grid, for example, would disrupt our ability to continue to use that force if the President ever chose to do that or needed to do that.

I am concerned, though, about some other facets of this. One, of course there's a continuing need to make sure that we are protected against electromagnetic pulse and any kind of electromagnetic interference. Sometimes we have debates over whether that's a Cold War relic and I would argue it is not. We need to be mindful of potential disruptions to that force. But I am not concerned about disruptions to the power grid, for example, or other critical infrastructure pieces impacting that force.

Senator REED. General Alexander, your comments about this, the potential threat?

General ALEXANDER. Sir, I agree with what General Kehler said with nuclear command and control and the way that we do that specifically. I think what it really impacts is, as you look at commands like TRANSCOM and others, our ability to communicate would be significantly reduced and it would complicate our governance, if you will, and our ability for the government to act.

I think what General Kehler has would be intact. So the consequence of that is, it's the cascading effect into operating in that kind of environment that concerns us, concerns me mostly.

Senator REED. General Alexander, let me raise an issue that, as Senator Lieberman indicated—excuse me—Senator Levin, the Collins-Lieberman legislation was not successful. I share his view it's very important because right now we have essentially a voluntary scheme. One of the arguments that's raised by the opponents is that it would impose too much cost on the business community, etcetera.

Your knowledge of the potential state and non-state ability to disrupt the economy of the United States, not our Strategic Command but ATM machines, etcetera, do you have—have you done a calculation of the potential cost to the economy if someone decided to conduct, not an intermittent attack on a banking system, but a concentrated attack?

General ALEXANDER. Senator, an attack on a bank, as you know, would be significant. It would have significant impacts. If people can't get to their money the impact of that is huge, and you've seen that and we've discussed that impact.

What I'm concerned about is a distributed denial of service attack could accomplish that. A significant distributed denial of service attack could make it very difficult for our people to do online banking, online trading, and others. The cost—so there's the cost

of losing that. If you think about Amazon, one hour of Amazon costs $7 million in profit to them if they were offline.

There's also a cost that complicates legislation in that each of our critical infrastructure portions of our industry have different levels of cyber readiness, if you will. So the banks and the Internet service providers are generally pretty good, the power companies not so good, and the government somewhere in between. So the cost for repairing, for fixing that, is significant.

I think the issue that I get talking to industry is their concern on creating an overbureaucratic regulatory process. So I do think that what the administration has put forward is, let's sit down and talk to them on the way to address this, is a great step forward. It really does allow us now to sit down with industry and say, so here's what we think needs to be done.

In my discussions with the power company specifically, their comment is: Look, we'd like to do that, but that's going to cost more; how do we do that?

Senator REED. But the point, my final point, is from your perspective right now if an attack, which is conceivable, took place the cost to that company would be many, many times the cost of preemptive action today. Yet they still object to that cost. Now, the probability of attack has to be weighed. If that probability today is one percent, that cost, that might be a reasonable judgment. But I think the impression I get from your testimony and consistently is that percentage or probability goes up and up and up each day, until we reach the point where, do the math and if they're not investing in protecting themselves, those financial institutions, then the cost they're likely, probably to shoulder, will be catastrophic. They don't seem to get that point, though.

General ALEXANDER. I think that's accurate. Just as you've said, it increases every day. That's the concern and I think you've seen that from industry stating the same thing. So I do think we have to have this public debate on that and get it right.

Senator REED. Thank you very much.

Chairman LEVIN. Thank you, Senator Reed.

Senator Ayotte.

Senator AYOTTE. Thank you, Mr. Chairman.

I want to thank both of our witnesses for your leadership and for your service to our country.

I wanted to follow up, General Kehler, on the issue of the intercontinental ballistic missile threat to the country that Senator Inhofe and Senator Reed asked you about. You used the term in terms of, I think you said "not optimum" in terms of some of the challenges we may face there. Just so it's clear to people, if now an ICBM were headed to the west coast we would get a shoot-look-shoot at it, correct, because of our missile defense system? But we don't have an East Coast missile defense system, so if Iran develops ballistic missile capability we don't have the same capacity, do we, on the East Coast of the country?

General KEHLER. While I hate to say it, the answer is it depends. It depends on what a country like Iran would do, where they would launch from, what the azimuths are, etcetera. The intent is that as time passes and additional features are added to the ballistic missile defense system that our capability to defend improves.

Senator AYOTTE. But just so we're clear, as of today am I not correct in saying that West Coast, North Korea, we get shoot-look-shoot? We don't get the same capacity on the East Coast if Iran—some analysts believe that they could develop this ICBM capability as soon as 2015. That may or may not be correct. But at this point our missile defense is—the capacity is different on the East Coast of the country versus the West Coast, isn't that true?

General KEHLER. I would tentatively say yes and provide you a better answer for the record.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator AYOTTE. I appreciate it, because the National Research Council actually this year recommended an additional ballistic missile site on the East Coast; isn't that right?

General KEHLER. Yes. They are one of the organizations that has looked at this, yes.

Senator AYOTTE. Well, I certainly would like to hear your view more specifically as to why an East Coast missile defense site would or would not enhance our capability to address an ICBM missile coming from Iran, particularly protecting the population base in the East Coast of the country.

General KEHLER. I'd be happy to provide that for the record.

Senator AYOTTE. Thank you, General.

I also wanted to follow up. As I understand it, last week you testified in the House Armed Services Committee that any potential future nuclear arms reductions with the Russians should be bilateral in nature; is that fair?

General KEHLER. That's fair.

Senator AYOTTE. So my follow-up question to that is, should they not be bilateral and verifiable? Is verifiable important if we were going to take arms reductions based on what we were going to count on a bilateral understanding with the Russians?

General KEHLER. I believe verifiable is important.

Senator AYOTTE. Why is verifiable critical or important when we think about entering these types of understandings with the Russians, or any other country for that matter, with regard to nuclear arms?

General KEHLER. Senator, from a military perspective I believe we have been on a successful and deliberate pathway with the Russians that has allowed us to reduce the threat to the American people and to our allies while at the same time being able to achieve our national security objectives, and we've done so in a way that's verifiable. I think that's a winning combination of things. Verification has proven to be important for us, I believe, from an assurance standpoint, and I think it's important. It has also provided second and third order benefits in terms of transparency and engagement with Russia which I think has been very valuable.

Senator AYOTTE. General, are the Russians in full compliance with all existing arms control agreements with the United States right now?

General KEHLER. The United States' view is that they are not in compliance with the Conventional Forces in Europe Treaty.

Senator AYOTTE. Are there any other treaty obligations they're not in compliance with?

General KEHLER. As I recall, and I'll provide the official answer for the record, as I recall there are a couple of other treaties where we have questions about the way they are going about it. I think the only one that we have said that we do not believe officially that they are complying with is Conventional Forces in Europe.

I can tell you that so far under New START all of the indications I have is that they are in fact complying.

Senator AYOTTE. I would actually like a follow-up for the record, just with the question of whether they are in full compliance with all existing arms control agreements with the United States.

General KEHLER. I'll provide that for the record.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator AYOTTE. Thank you, General.

I also wanted to ask you—you and I talked about this when you came to see me in my office yesterday, which I appreciated, to talk about these issues—an article that appeared in the Sunday New York Times titled "Cuts Give Obama Path to Leaner Military." In that article the article essentially said that it would give the administration—the sequestration cuts would allow the administration to call for deep reductions in programs long in President Obama's sights, and among those programs were an additional reduction in deployed nuclear weapons and stockpiles and a restructuring.

There's some other restructuring, but the issue I want to ask you about is an additional reduction in deployed nuclear weapons. Can you tell me right now—in the article it said that the Joint Chiefs had agreed that we could trim the number of active nuclear weapons in America's arsenal by nearly a third and make big cuts in stockpile of backup weapons. Is there any intention by the administration right now that you're aware of or any recommendation pending to significantly reduce our active nuclear weapon arsenal by a third or make big cuts in the stockpile of our backup weapons, as outlined in this article?

General KEHLER. Senator, I can't comment on the article. What I can say is that from the nuclear posture review forward certainly the administration has undertaken a study to look at what alternatives may exist beyond New START, for reductions beyond New START. We participated in that conversation and in parts of the study. In fact, we did parts of the study at STRATCOM. We were fully involved, and to my knowledge no decisions have been made.

Senator AYOTTE. Let me just say that, obviously, I think that preserving our nuclear deterrent is very, very important, and I think that making significant reductions right now, at a time with what's happening in North Korea, with the threat we face from Iran, and also from the situation where we find ourselves I think in the world, that obviously I hope that if there are any reductions that are made, for example, with the Russians, that will be done through the treaty process. The New START was done through the treaty process.

One of the things this article also says is that there could be reductions made with the Russians without a treaty. So I don't know whether you would weigh in on whether we should go through the

treaty process, but in my view I think that Congress should have an ability to weigh in on these issues.

As a follow-up, I wanted to ask you, General Alexander, the role of the Guard in cyber issues. Where do you see the Air National—excuse me—the Guard in general, not just the Air National Guard, but all of the Guard, playing what role they would play with regard to how we meet the challenges facing us with cyber attacks, and what role could the Guard play on a State basis working with your—obviously, you, General Kehler and General Alexander, and how can the Guard help in this?

General ALEXANDER. Thank you, Senator. I've sat down with the Guard leadership, all the adjutant generals from all the Guard, and talked about the role and responsibility of the Guard in cyber space. I think there's two key things that they can do: first by setting up protection platoons and teams and training them to the same standard as the active force, it gives us additional capacity that we may need in a cyber conflict.

The second part is it also provides us an ability to work with the States, with the Joint Terrorism Task Force and cyber forces that FBI has, and with DHS to provide additional technical capacity for resilience and recovery. I think those two areas the Guard can play a huge role in.

The key is training them to the same standards. We talked about the with all the Guard chiefs. They agree with that and we are working towards that objective.

Senator AYOTTE. Thank you both. I appreciate it.

Chairman LEVIN. Thank you, Senator Ayotte.

Senator Nelson.

Senator NELSON. Thank you, Mr. Chairman.

General Kehler, you spoke very crisply about us having the ability in our command and control to control our nuclear response. I appreciate that, and that is assuring, even though we might have a cyber attack that would take out electric grids and so forth and so on.

What about the Russians and the Chinese? Do they have the ability to stop some cyber attack from launching one of their nuclear ICBMs?

General KEHLER. Senator, I don't know. I do not know.

General KEHLER. Well, Mr. Chairman, I think that's a question that we ought to see to what degree we could answer. That reminds me, you know, in the disintegration of the Soviet Union it was the United States that took the initiative through Nunn-Lugar to go in and try to secure those nuclear weapons. That turned out to be a very successful program.

In this new world of cyber threats, we of course have to be responsible for ours, but we have to worry about those others on the planet that have a nuclear strike capability protecting theirs against some outside player coming in and suddenly taking over their command and control.

General Alexander, do you have any comment on that?

Chairman LEVIN. I wonder if you would yield before his answer.

Senator NELSON. Certainly.

Chairman LEVIN. That is, it's a very important question. I wonder for starters—and I didn't mean to, I shouldn't interrupt the an-

swer—is to whether for starters, Senator Nelson, we should ask the intelligence community writ large as to what we know about that.

Senator NELSON. Okay. If you want to save that—

Chairman LEVIN. No, no. We will do that. It's a great idea. It's an important point and we will take that on. We will ask. But let me not interrupt further the answer.

Senator NELSON. Okay. I know General Alexander is going to be constrained as to what he can say in this setting. So let me just defer that then for a classified setting.

Chairman LEVIN. Well, not just classified, but also a broader intelligence community assessment as well, if we could do that, Senator Nelson.

Senator NELSON. Well, General Alexander knows everything about everything.

General KEHLER. Senator, if I could add just one additional point, though. I would say that we know—I think because we've worked with the Russians over the years and we've had fairly decent transparency with the Russians over the years, I think we understand they are very careful about their nuclear command and control. They are very careful about the way they provide what we would call nuclear surety as well.

This is also one of the reasons for why we would like to see additional transparency with China, because we would like to be able to have these dialogues with them in a military-to-military kind of context. It's something that we have been trying to push now for quite some time.

Senator NELSON. Exactly. And as we go into the session that the chairman has recommended, let's just don't stop with China. What about the Brits? What about the French? Do they have the capabilities of stopping a cyber—a rogue cyber attack from coming in and suddenly messing up their command and control?

Okay. General Alexander, you must be one of the most frustrated people on the planet, because you know the threat in cyber and here the Congress can't get anything done because certain players won't allow the passage of the legislation. So let me ask you, what is it about liability protection that the private sector would feel comfortable about in order so that real-time, as you said, we have to have the private sector respond to an attack with the information in real time in order to be able to meet this present and increasingly dangerous threat?

General ALEXANDER. Senator, I'll give you my answer here and I'd ask to just take that for the record to get you a really accurate and detailed answer on it, because I do think this is important to lay this out.

The issues as I see it for liability protection are in two parts. When the Internet service providers and companies are acting as an agent of the government and make a mistake and are subject to lawsuits, the issue becomes they get sued so many times by so many different actors that they spend a lot of money and time and effort responding to those lawsuits when we've asked them to do something to defend the Nation. So there is that one set.

The other is, let's say theoretically that we send a signature that says stop this piece of traffic because it is that Wiper virus that hit Saudi Aramco, but we the government mischaracterize it and

when they stop it that stops some traffic that they didn't intend to nor did we. We make a mistake. Mistakes are going to happen because when you have real-time concerns, emergency concerns, some traffic may be impacted.

That traffic that is impacted, the Internet service providers would quickly fix by altering that signature to get it right. But some traffic has been delayed or disrupted by their actions because we've asked them to, which could cause them also subject to lawsuits.

So I think it's in that venue that we've got to give them immunity from those kinds of actions. I'm not talking about giving them broad general immunity and I don't think anyone is. It is when they're dealing with the government in good faith in these areas we should protect them for what we're asking them to do, and I think that's in the venue.

I'll get you a more specific answer from our legal folks on the technical side.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator NELSON. This should not be that hard, because we've been through this before with the metadata on all the question a few years ago of being able to intercept traffic in order to identify the terrorist wherever the terrorist was. Clearly, we've dealt with it before and liability protections, so we ought to be able to get this one.

General ALEXANDER. I think, Senator, if I may, I think there's broad consensus on information sharing and liability protection. Where it really gets uncomfortable, if you will, is regulations, standards, what the government does there. That's the really hard part, in part because all the industry sectors are so different.

I think that's one of the things that the administration has done that really puts the step forward, is the executive order now gives us an avenue to start discussing that. I think that's very useful. I think any legislation should point to that and look at incentives to get industry and others to having a more resilient infrastructure.

Senator NELSON. Thank you.

Thanks, Mr. Chairman.

Chairman LEVIN. Thank you. Thank you, Senator Nelson.

Now it is Senator Blunt.

Senator BLUNT. Thank you, chairman.

General Alexander, on the staffing of Cyber Command, it's been reported that you need to expand in a significant way. Do you want to talk a little about what you see as your staffing needs and also how you'd meet those staffing needs? How do you compete for the kind of people you need that are in the private sector now?

General ALEXANDER. Senator, thank you. There are two issues here and let me just pull them apart to accurately answer your question. We're not talking about significantly increasing the Cyber Command staff per se. We're actually asking the service components of Cyber Command to field teams that could do three missions: defend the Nation from an attack, support our combatant commanders, and defend our networks with cyber protection platoons.

Those sets of teams are what is the big growth that we're talking about and that the services are looking at. We are working closely with each of the services in setting standards, training standards for those.

The good news: So far the services have stood up and met every goal that we've put for them here. I just give my hats-off to the service chiefs and our components in doing that. So we are right now in line, on track for one-third of that force being completed by September and about one-third the next September, 2014, and the last third by 2015, that target range.

The good news is we are taking the most serious threats and addressing those first with the teams that have already stood up. They're already on line and actively working in this field. So we already have teams up and running, thanks to the Army, Air Force, and Navy for setting those teams up.

So what we're talking about is bringing those folks in. Now, doing that, there's two parts to it. One is training. So we can take kids, young adults, with great aptitude. They don't have to be cyber experts. We can help them get there. I will tell you, my experience is people who want to work in this area and have the desire—we have a machinist's mate from the Navy, a machinist's mate—you know, you thought—I talked to him and I said, well, how'd you get here? He goes: Well, I really wanted to do it. He is one of our best. So we've asked the Navy to give us all their machinist's mates. No, just kidding.

So when you look at it, there is great talent out there. The real key part is how do we keep them, how do we incentivize them, and what are the programs that we're doing? We're working on a program with the Services to do that, and setting up their career fields for the Services to have this common among the Services.

Senator BLUNT. A concept I'd like you to talk about if you want to and think about if you haven't thought about it. Senator Vitter, Senator Gillibrand from this committee, and I, along with Senator Coons and others, are looking at some legislation that would create more cyber warrior opportunities in the National Guard. Missouri's done some of this already, as I think you know. These are people who are actively in this work every day anyway, who would then be available to react or be available to train.

Do you have a sense of how that might be part of what you're looking at in the future?

General ALEXANDER. Senator, we have National Guard folks on our staff. We are actively working that with the Guard. A few weeks ago I sat down with all the adjutant generals from all the States and walked through how we could do this, how we train everybody to the same standard, active and Guard. Their roles, twofold. Just to quickly summarize, one would be how they work with the States, DHS, FBI, in resiliency and recovery and helping the investigative portion, and how they work with us in a cyber conflict to complement what we're trying to do. We will not have enough force on our side, so we'll depend on Reserve and National Guard just like the rest of our force structure.

Senator BLUNT. I think in this area that gives—for instance, your machinist's mate, if he decides, he or she decides, for some reason that they don't want to be in the full-time force, but they

have this great skill level that they've acquired, to take that to the Guard.

General.

General KEHLER. Senator, if I just might pile into the conversation for a moment. I think it's just as important for us to remind ourselves that, whether it's growth in cyber, whether it's investment in replacement for the *Ohio*-class submarine, no matter which piece of the future that we are looking at here, all of this is sensitive to the budget decisions.

Sequestration, for example, and those budget totals will in fact impact all of this. And while General Alexander is right, there is some growth that is underway—and I think the services have been very generous in that regard—there will be impacts across the board here. We just can't predict what those will look like today until the actual budgets are redone.

Senator BLUNT. General Kehler, have you talked about the sequestration and the continuing resolution component of that? We had people in here in the last few days that have talked about how important it is we update your spending request, and hopefully we're in the process of doing that. But would you visit with me a little bit about that?

General KEHLER. Yes, sir. I think we would be in favor of as much certainty as we can put back into the process. That is a way to help with certainty, and that will be very beneficial. I think, as I said earlier, the most immediate impact for us and the most concerning and troubling impact in Strategic Command is the impact that we will see on our civilians. That is not insignificant, and I think we've got to be very mindful of the potential damage that those impacts will have.

Beyond that, then there are the impacts on the readiness accounts that we will see. That's like a slow- motion movie. In STRATCOM this will be like watching something in slow motion. It will occur. It is happening now. It's just we do not see the effect yet. We will see that effect as the months progress.

Senator BLUNT. I think these two things come together here, where the failure to update the priorities by refusing to appropriate and debate those bills on the floor has come together with then cutting those old priorities on a line by line basis, and it's challenging.

General KEHLER. Yes, sir.

Senator BLUNT. General Alexander?

General ALEXANDER. Senator, I was just going to add that it impacts Cyber Command in a similar way, two parts. The continuing resolution holds us to the fiscal year 2012 budget, but, as you now know, we're standing up all these teams in fiscal year 2013 and the funding for that was in the fiscal year 2013 budget. So that's about 25 percent of our budget right now is held up. That's significant.

One-third of our workforce are Air Force civilians and they are going to be impacted by this furlough. When you think about it, here are the folks that we're asking to do this tremendous job and we're now going to furlough many of those. That's a wrong message to send people we want to stay in the military acting in these career fields.

Senator BLUNT. What's the impact of dividing your workforce between the uniformed personnel and the civilian personnel? What's the internal management challenge of that, General Alexander?

General ALEXANDER. Actually, it works well together.

Senator BLUNT. I know it works well, but when the civilian force takes a furlough—

General ALEXANDER. Right. It has a significant impact because they look at it and they say, well, why are we being targeted for this? And it is a smaller group, and when you look at it both sides agree that this is the wrong way to handle it.

I think I would add to what General Kehler said, is we need to give the service chiefs and the military the ability, the flexibility to look at where we take these cuts and do it in a smart way. Right now, just doing it by activity doesn't make sense. We would not do it if we ran this as an industry.

Senator BLUNT. I couldn't agree more.

General Kehler, when I was at Whiteman Air Force Base the other day the commanding general there on this topic said: The civilian force is an integral part of what we do and we don't need to send a message to them that somehow they're not as integral to what happens every day as the uniformed force is. He showed real, I thought, very good management concern about how you keep your team together when the law is dividing your team and part of your team's taking the hit that the other part's not taking.

Not suggesting, by the way, that we do anything to the uniformed force, but I think this is maybe one of those, the law of unintended consequences. You think you're protecting the uniformed force and in writing the law that way then all the personnel obligation goes onto the other side.

Do you have anything you want to say about that?

General KEHLER. Sir, I couldn't agree more. The role of our civilians has changed dramatically over the years that I've served. Today they are integral to everything we do. They are leaders in our organizations. They occupy senior leadership positions. And in many, many cases they represent the expertise and the experience that we do not have in the uniformed force.

So in a place like Strategic Command, in a place like Cyber Command, in a place like the nuclear enterprise, where our senior civilians really represent most of the experience that's left in these types of highly technical, highly complicated places—so certainly in the space part of our business, we have some senior civilians who are in very important parts of the DOD space organizations.

So I think that my concern with the sequestration begins with the intentional and then the unintentional intangible impacts that we might see on our workforce. It is the uncertainty that goes with that that concerns me the most.

If I could just add one more thing, we have had a very successful intern program to try to entice young college graduates to enter civil service so that they can have government careers. It's been very successful. So in Omaha we find that a number of these youngsters who are just beginning their careers in civil service with college degrees are looking around today and wondering if this is their future.

Senator BLUNT. Exactly.

Thank you, Generals.

Chairman LEVIN. Thank you, Senator Blunt.

Senator Donnelly.

Senator DONNELLY. Thank you, Mr. Chairman.

To General Kehler, General Alexander, thank you so much for your service.

General Alexander, does the private sector have the same skills that your team does in reacting to cyber security and to reacting to cyber attacks and being able to protect themselves?

General ALEXANDER. The private sector has some tremendous talent in this area, which we need to leverage and partner with. So I want to I think be clear. There are two parts to answering this question I think accurately. When you look back 70 years ago to Enigma and you look at the making and breaking of codes and doing some of the special work that the predecessors to NSA did, we have special capabilities both in Cyber Command and NSA. Hence that partnership. That gives us unique insights to vulnerabilities and other things that we can share back and forth.

It is that area that is perhaps most important in identifying those vulnerabilities and sharing it with industry, those things that could impact our industry. But industry has like skills and sees different things. So the antivirus community is very good in this area, and I don't want to underestimate them. What you're actually doing is saying, let's put the best of those two teams for our Nation together to defending us. I think that's in legislation one of the key things that we need to do.

Senator DONNELLY. When we look at what's going on, a huge, huge amount of this is efforts to try to steal America's intellectual property, from defense contractors, from private businesses, from our military. If you are a business and you're developing products and you're going to patent it, you may be concerned about your ability to protect against a cyber attack. You know how to develop a great product that may help cars run faster, on less fuel, etcetera, but cyber attacks are not your thing.

If you were that company, what would you recommend to them in terms of protecting themselves?

General ALEXANDER. I would recommend that they first talk to companies like McAfee, Symantec, Mandiant and others that have great experience in this and that can give them great advice. The defense industrial base also have companies that can do that. That takes them one step.

I think Senator Inhofe brought up a good point that needs to be brought in here and that is it needs to be a layered defense. So there are things that they can do to have a more resilient and more protected architecture, and those things they should do. It's like having Norton Antivirus in your home computer.

Senator DONNELLY. Sure.

General ALEXANDER. Those are the key things and we can help them with that. There's another part. We know things about the network that now we'll call classified information, that would be useful for us to share to protect those. But what we can't do is share those so widely that the adversary knows that we know them, or we lose that capability.

So that part of sharing has to be done properly, in a classified forum, that those Internet service providers and other companies can use to protect the networks. That's why I say it's almost two layers to this.

Senator DONNELLY. You had mentioned before, you talked about being on offense as well. Are there communications made to those countries, to those organizations, that have done cyber attacks against us that there are consequences in regards to what we can do as well?

General ALEXANDER. The President did make that statement publicly in 2011, that we'd respond to cyber attacks with all the broad range of options that he has before them. I think some companies have been talked to privately. I can't go into that here. I think that's the first logical step that we should take, is say if you do A it will really upset us. That's why they don't have me do it. They have people who can really put this in the right words. But I think we ought to have those demarches and other things with other countries and I know the inter- agency process does work that closely.

Senator DONNELLY. General Kehler, in regards to North Korea and what we have seen in the past few weeks, at this point what adjustments to our posture are needed, if any, to make sure that not only our friends in South Korea, but our own Nation and our other allies are protected?

General KEHLER. Senator, we're looking across our entire range of activities to see if any adjustments need to be made. What I would say is that deterring North Korea from acting irrationally is our number one priority, and that deterrence begins on the peninsula with our alliance with the ROK. It extends to our conventional forces that are forward on the peninsula. It extends to other forces that are available in the theater to Admiral Locklear and General Thurman. It extends ultimately all the way back to our nuclear deterrent.

Today my assessment of certainly Strategic Command's role in this is that we are capable of offering to the President the full range of options. Whatever he chooses to use in response to a North Korean act, I believe we can make available to him, and I'm confident in that today.

We are looking, though, at the pace of the North Korea threat to see whether or not the limited missile defense that we have in place, both in the theater and for the United States, is on the right pathway to deal with the threat. We're working that with the intelligence community to see if there's a more complete assessment that we need to put in place today and whether that will cause us to make any adjustments.

Senator DONNELLY. With some areas, some countries, you can in a way determine here's what we expect them to do next. Has North Korea—you talked about rational actors. Is it difficult at times to determine what they are going to do next and what steps they will take?

General KEHLER. I believe it's difficult. I believe that we all think that's difficult, especially with a new leader that, frankly, I think we're still getting to know. So I think that there are great debates about rational, irrational, etcetera. I think for us anyway it is a

question about readiness for us, and us being ready to respond in any way that might become appropriate. I am confident today that we can respond in appropriate ways.

We participate in exercises, of course, with Pacific Command and with our command on the peninsula, as they are participating with the ROK's in their exercise series. So I believe that we are demonstrating the credibility of our capabilities and that's important.

Senator DONNELLY. Do you see coordination between North Korea and Iran in Iran's efforts to develop further nuclear technologies and in Korea's efforts?

General KEHLER. Sir, I would prefer to have that conversation in a different setting.

Senator DONNELLY. That's fine.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Donnelly.

Senator Fischer is next.

Senator FISCHER. Thank you, Mr. Chairman.

Thank you, gentlemen, for being here today. General Kehler, it is a pleasure to see you again.

Earlier you said that we can protect the continental United States with the resources that we currently have. Is that correct?

General KEHLER. Against a limited threat, yes.

Senator FISCHER. Against a limited threat. Would you agree that that equation would rapidly change if others would be able to develop technology to detect our submarines, if governments would become more hostile to us, and if we don't maintain the systems that we have?

General KEHLER. Senator, I think that any time the threat changes that that certainly causes us to review and could cause us to make adjustments in all kinds of places, yes.

Senator FISCHER. Are we addressing those concerns now?

General KEHLER. Yes, we are.

Senator FISCHER. Are we maintaining our nuclear arsenal to the standards you would like to see?

General KEHLER. We are today and—however, with a caveat. And the caveat is that all along here over the last two years that I've been in command we have made a point of agreeing forcefully with the need to both modernize the deterrent and make sure that the enterprise is capable of sustaining it. So with those caveats, then yes, I am comfortable that we are capable of maintaining a safe, secure, and effective deterrent.

Senator FISCHER. And with those caveats, you can perform the mission that you are asked to do right now?

General KEHLER. Yes.

Senator FISCHER. Do you agree with the statement the more useable weapons are the more deterrent value they have and the less likely they will be used?

General KEHLER. I would generally agree with that. I typically say the more credible the deterrent is, and that of course includes that we are able to employ it if we were ever in the situation where the President asked for us to employ it.

Senator FISCHER. Do you believe that our conventional forces today would be able to execute a deterrence mission that's currently performed by our nuclear weapons?

General KEHLER. I think in some cases conventional forces are capable of executing—of producing a military result that would be similar to what a nuclear weapon could do. The question about deterrent effect I think is an interesting one, and in some cases yes, I believe that strong conventional forces clearly improve and increase our overall deterrent, just like a number of other factors do.

But I believe that nuclear weapons continue to occupy a unique places in our defense strategy, in our national security, and I think in global perceptions I think they continue to occupy a unique place.

Senator FISCHER. From your response I would assume that you would agree that we need to maintain the balance that we currently have, then, with our nuclear deterrent in balance with our conventional forces. Is that a good balance right now? Are we at a good point?

General KEHLER. I think an interesting thing has happened. I believe that we are. I think that they are complementary, I would say. What has happened, I believe, since the Cold War is that our increases in our conventional capabilities and in sort of the overwhelming conventional power projection that we can bring to bear around the world has made a difference in the role of our nuclear deterrent. I think that we've been able to narrow the role of that nuclear deterrent accordingly.

But I think as we go forward that will be an interesting question to watch, whether our conventional forces remain strong.

Senator FISCHER. But at current levels you believe that it is a good balance? If those levels would drop with conventional forces or with nuclear, but focusing on the conventional, if we see the nuclear side drop, if we don't maintain the arsenal that we have now or if we continue to limit it, can the conventional forces pick up the slack?

General KEHLER. I think in some cases the answer is yes. I don't think they can across the board. I don't think that they substitute for the effect of the nuclear deterrent. However, I do think that conventional forces do in fact make a difference in terms that we are no longer in a position where we have to threaten nuclear use in order to overcome a conventional deficiency. So that's made a difference.

I also think that we need—saying that they are in some kind of balance today doesn't mean in my view that there isn't some opportunity to perhaps go below New START levels.

Senator FISCHER. Would you like to elaborate on that?

General KEHLER. I think there are still—as I said earlier, from my military perspective, I think that we have in the deliberate pathway we have been on with the Russians over the years in reducing the number of weapons that can potentially threaten the United States or our allies, and we've done that in a way that's maintained stability and we've done that in a way that's been verifiable, I think that has provided benefit to us from a military perspective. And I think that if there are additional opportunities in the future we ought to explore those.

Senator FISCHER. Would you recommend going below the New START levels unilaterally?

General KEHLER. I would not. I would not. I think that again the formula for success has been that we have done this with the Russians and I think that's the formula for continued success. And I believe that certainly Secretary Panetta was very public about that. I've seen some correspondence from Secretary Hagel where he has agreed with that. The President mentioned in his State of the Union address that he wanted to work with the Russians. I think that's a consistent theme that we have seen across the board.

Senator FISCHER. It's been suggested by opponents to our nuclear program that the program's on a hair trigger. Do you believe that there is any risk that's caused by our readiness posture right now?

General KEHLER. We go to extraordinary lengths to make sure that our nuclear deterrent force is both safe and secure, and I believe that it is safe and I believe that it is secure. It is also under the positive control of the President of the United States.

Senator FISCHER. Do you believe that it makes our country safer?

General KEHLER. I believe that in today's global environment that having a portion of our force in a ready to use posture for the President meets our needs today. But we are always reviewing that to see whether that's the appropriate balance for tomorrow or the day after. I think that will vary as the world situation changes.

Senator FISCHER. Thank you.

General Alexander, if I could just ask you a brief question. The defense authorization bill said that Congress should be consulted about any changes to the UCP as it relates to Cyber Command. Would you commit to providing this committee, this panel, with justification for elevating to a U.S. Cyber Command?

General ALEXANDER. Absolutely. I think right now the Secretary and others are looking at that and I know that the intent is to share everything with this committee before they take any action and make sure the committee is comfortable with any actions. Right now it's just in the discussion phases. The new Secretary has to look at it and I think that will take some time, and they will bring it back.

Senator FISCHER. Thank you very much.

Thank you, Mr. Chairman.

Chairman LEVIN. Thank you very much, Senator Fisher.

Senator Blumenthal is next.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

Thank you both for your service, your extraordinary contribution to our defense readiness and our Nation.

Perhaps I could begin, General Alexander, by asking you a general question which perplexes me. We agree, I think all of us on this committee, agree with you that the threat of cyber attacks and cyber interference with key parts of our Nation's infrastructure, our private companies that are so vital to our national defense, is a clear and present danger to our Nation. Yet the Nation as a whole seems unaware, certainly unalarmed, by this threat.

I know that you've thought a lot about these issues, have spoken to us about them privately as well as publicly. And I wonder if you have some suggestions for us as to how we or you or the President can make the Nation more aware about them. Obviously, the President has spoken about them, but I wonder whether you have some thoughts for us——

I know it may seem as though it's in the political realm, but really in the educational task that I think we face together to make the country aware of the real threat physically and otherwise of cyber attack.

General ALEXANDER. Senator, thank you. What you bring out is the key, I think, to really moving the legislation and other things forward, and that's educating people on the threat, accurately educating them on the technical side—what does this mean, what's a cyber attack, and what are the effects, what's going on, what are we losing, and what should we do.

There are many reasons that industry and other players are concerned about legislation and other things. Part of it is the cost, the bureaucracy that comes in. Part of it is addressing a very complex issue that at times it's easier to ignore, and that's theft of intellectual property. The fact that they lose it is an issue, but for the country, for the Nation as a whole, this is our future. That intellectual property from an economic perspective represents future wealth and we're losing some of that.

Senator BLUMENTHAL. And you've referred to it, I think, as the greatest single transfer, illegal transfer of wealth in the history of the world.

General ALEXANDER. Illegal, yes, exactly. And I'm concerned that if we don't stop it it will hurt our Nation significantly. There's two parts to stopping it. One is fixing our infrastructure, working together with industry and government to stop these attacks. Then the second, as was brought out by Mr. Donnelly, perhaps our administration and others reaching out to those countries and stopping them.

I think the second part is ongoing right now. We have to step back to the first part and look at how we educate. I do believe that we have to be more public in some of this and we have to defuse the alarming stuff that comes out on civil liberties and privacy and have a candid set of discussions on what it means to protect in cyber space. I think that's often lost. Often it is just thrown out there as a way of stopping progress when what will happen, what I'm really concerned about, is a significant event happens and then we rush to legislation.

We have the time now to think our way through and get this right. We should educate people and do that. And we are pushing the same thing, and we'll help in any way we can, Senator.

Senator BLUMENTHAL. Thank you.

General Kehler, if I may ask you. You have stated that "It is essential to provide sufficient resources to replace our *Ohio*-class ballistic missile submarines." As you're aware, the fiscal year 2013 budget deferred procurement of the first *Ohio* replacement boat by 2 years. I'd like to—I'd like you to share with the committee to the extent that you can whether 12 submarines are still required—I assume that they are—and how in general terms a requirement like this is established, and what we're going to do to achieve that goal?

General KEHLER. Senator, we established the requirement by looking into the future and making a number of judgments about the future, which is what we do with every weapons system that we put on the books. In this case, though, I think we've started report the assessment that the value of a submarine-based deterrent

as we go to the future will remain as high as it is today. Then the question doesn't become if you need to do it; in my mind it becomes when do you need to do it.

So we've worked this very carefully with the Navy, and it is ultimately the Navy's assessment of the current performance of the existing submarines and their longevity that's driving the answer to this question. Much like any other military platform, the amount of use that gets put on it determines its lifetime. In the case of submarines, which I don't know much about, but a number of submariners who work for me remind me constantly that it's the cycles on a submarine. It's a harsh environment, first of all, and then you get the pressure, no pressure, pressure, reduced pressure, etcetera.

So that does things to metallurgy and it does things to fittings and it does things to sort of the internal workings of a submarine that ultimately cause them to question the continued safety of being able to cycle down and up. The Navy tells us that we're going to reach that. It's not going to be a bright line in the sand that on today they're all okay and tomorrow they're not. There's a zone that they're going to enter and sliding these an additional two years to the right puts them in the zone.

My view would be it's not prudent for us to slide them further, unless of course the Navy steps forward and says, no, we can go another couple of years. I don't know that they're going to say that. I don't expect that they will. But I think again it's not a bright line in the sand. I think the issue for us will be 12 looks like the right number as we go to the future. That can always be adjusted as we go to the future. It seems to be the right balance between capability and cost, and that's going to be important as we go to the future, no question about that.

So on balance my view is that we do need to go forward with that. We need to go forward with long-range strike aircraft as well, and we need to complete the analysis of alternatives on the future of the intercontinental ballistic missiles beyond 2030. That's not a decision we have to make today, but it is an analysis of alternatives that needs to go forward.

Senator BLUMENTHAL. But there's no question right now that 12 is the right number?

General KEHLER. I don't have a question that that's—I would say that that's a minimum number that we sit there looking at today. I don't know if the number gets larger than that, and that will depend, I believe, on a number of factors as we go forward.

Senator BLUMENTHAL. When you say that sliding to two years puts us in the zone, could you explain what you mean?

General KEHLER. The first of the OHIO-class submarines will begin to reach the end of their service lives at just about the time the first of the replacements comes on line. It's a dance that we're working. And by the way, we're working this with the United Kingdom as well because they are looking the piggyback, if you will, on this program for their own replacement. So this is a very delicate programmatic dance that the Navy is doing with the U.K. as well as with the needs that STRATCOM has put on them.

Senator BLUMENTHAL. Thank you.

My time has expired. Perhaps I can follow up with some questions and also to General Alexander, if we can explore perhaps fur-

ther the education of the public, which is so vital to the work really that you're doing and that we're seeking to assist you to do.

Thank you very much. Thank you both.

Chairman LEVIN. Thank you, Senator Blumenthal.

Senator Sessions.

Senator SESSIONS. Thank you, Mr. Chairman.

I thank both of you for your leadership in the important commands that you have, both of which are extremely important to America.

The Defense Department acknowledges, General Kehler, that Russia is increasing its reliance on nuclear weapons and that the pace and scope of China's nuclear programs, as well as the strategy behind their plans, raises questions about their future intentions and the number of weapons they intend to have. Likewise, India and Pakistan are modernizing their nuclear forces and the French president recently commented that nuclear weapons are essential for France. And of course, North Korea continues to expand its capabilities, while Iran is on the verge of acquiring nuclear weapons.

So I'm not aware of any country reducing their nuclear stockpiles, except perhaps us as we continue to look at that.

But let me ask you, what are the strategic implications of these trends of enhanced nuclear weapons around the world?

General KEHLER. Senator, they do have implications for us. I think first of all, when we look at assessing other nuclear arsenals around the world what we do is we look at intent and capability. I think none of us believe that the Russians intend to attack the United States. I think we don't believe the Chinese intend to attack the United States, etcetera. However, they have the capability to do so, and as long as they do then we have an obligation to deter against such an attack. And that means we've got to be mindful of the capabilities that they are bringing to bear.

We note their modernization and we certainly note their numbers. And I think, at least again from my military perspective, arms control and arms reductions have helped us in terms of limiting or reducing in some cases the threat that we face.

We get to a point here, though, where as we work toward a goal, if the eventual goal is zero, you get to a point where other arsenals I think begin to bear on this equation.

Senator SESSIONS. Well, I couldn't agree more about that. I think it's unimaginable that if we go to zero that every other country in the world would go to zero, and that would place us at a strategic disadvantage of great magnitude and cannot be allowed to happen.

Could the disparity in public vision of countries and their nuclear weapons, some or most of these I've mentioned more robust than the United States, could that make our allies nervous? I'm concerned about these discussions that we're having about further reducing our nuclear weapons to a level I think is dangerous, about what discussions—what impact they might be having on our allies around the world, like Japan and South Korea, that have relied on the U.S. nuclear umbrella for the past seven decades.

If our arsenal and therefore the nuclear umbrella we provide continues to shrink, I'm concerned that our partners will look to create their own, and this is the very definition of proliferation, it seems to me.

As you may have seen, the Sunday New York Times reported that following North Korea's third nuclear test some influential South Koreans are now beginning to openly call for the South to develop its own nuclear arsenal.

Do our allies—is this a factor that we should consider as we evaluate the level of nuclear weapons that we want to maintain?

General KEHLER. Yes, sir, I believe it is a factor you have to consider.

Senator SESSIONS. In a message to the United States Senate in February 2011, President Obama said: "I intend to, A, modernize or replace the triad of strategic nuclear delivery systems of heavy bomber, air-launched cruise missile, and ICBM, and nuclear-powered ballistic missile submarines and SLBM's, and maintain the United States' rocket motor industrial base."

Additionally, two days before the vote on the New START treaty in a letter to Senators Inouye, Feinstein, Cochran, and Alexander, President Obama reaffirmed this commitment to nuclear modernization, stating: "I recognize that nuclear modernization requires investment for the long term. That is my commitment to the Congress, that my administration will pursue these programs and capabilities for as long as I am President."

Can you tell us where we are on the efforts to modernize our triad and our nuclear infrastructure, and are we on pace to comply with the President's commitment?

General KEHLER. Sir, I can tell you that through the submission of the 2013 President's budget, with some exceptions that we talked about last year—there were still issues in the nuclear enterprise, the weapons part of the business. The program didn't close, if you recall that from last year. But the 2013 budget continued the modernization efforts across the board. Some were later than others, but it continued the modernization efforts.

The 2013 budget turned into a CR. I don't know what the remainder of the year is going to bring to us in terms of the 2013 piece of this.

The 2014 piece—we've worked pretty hard over the last year to try to structure the '14 piece so that it would also continue all of the things that you've mentioned here. I don't know what's going to happen to the '14 piece, given the additional investment reductions that will have to come with sequestration. So I can't tell you today what it looks like, sir. I can't tell you it's not going to happen. I just can't tell you what's going to happen yet, because we don't have a budget on the Hill yet that describes our position.

Senator SESSIONS. Do you believe financially we should follow through with the commitments that the President had and this is a reasonable defense posture and expenditure for the United States?

General KEHLER. I believe, as the advocate for the strategic force, that this continues to be a wise investment on our behalf, I do.

Senator SESSIONS. In the last National Defense Authorization Act, we articulated certain expectations of the National Nuclear Security Administration, which manages our nuclear weapons production, and the Nuclear Weapons Council, of which you're a member, with regard to the shaping and reviewing of NNSA's budget. You review the budget and through the Council have input into that.

Specifically, our report said: "The conferees expect that the Nuclear Weapons Council not only certify, as required by law, that the NNSA budget as it is submitted to Congress, but that the Nuclear Weapons Council also take an active role in shaping and reviewing the NNSA budget as it is prepared for submission to Congress and negotiated with the Office of Management and Budget during the budget review process."

Is the NWC, the Nuclear Weapons Council, which you and others sit on, taking an active role in shaping and reviewing NNSA's budget proposal? I ask that because it's really clear to me, colleagues, that the Nuclear Security Administration and the Department of Energy, their role is much like a defense contractor, a Boeing or a Lockheed. They're producing a weapons system that you have to have and utilize, and you should be involved in how they manage that and the amount of money that's spent on it, I believe. At least I think that's healthy for America.

So do you feel good about where NWC is and are we on track here to raise it up as we intended to, to give it more power?

General KEHLER. Senator, I do feel good about where we are today in terms of insight and influence. It isn't perfect, but I think that over the last year in particular there has been a dramatic change in the working relationship between the Department of Defense and the Department of Energy and NNSA in particular over visibility into the budget and over influence in shaping that budget.

So again, it's not perfect. I think we're learning a lot about how we can get better at this as we go forward. I think there's more to do. But I have seen a tremendous change in the way we go about working together through the Nuclear Weapons Council and I think it's a tremendous positive change.

Senator SESSIONS. Well, great.

Mr. Chairman, I would note that my understanding is that the Department of Defense has not yet certified the budget. They must have some concerns about it. But it is at the OMB level already and going forward. I do think it's healthy that the Defense Department have real input into the production of the budget for nuclear weapons.

Thank you.

Chairman LEVIN. Thank you, Senator Sessions.

Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman.

Thank you, General Kehler and General Alexander, for your service.

General Kehler, as you know, the men and women who are assigned to the Pacific Missile Range Facility on Hawaii are some of the best around. The capabilities provided at this facility are exceptional and the Missile Defense Agency, the MDA, uses it to test the systems that will protect our country and allies from missile attacks.

Currently under construction there is the Aegis Ashore facility, I'm sure you're familiar, which will enhance the capabilities available for MDA and the Navy. So if you have not visited PMRF recently, I certainly encourage you to go out there, and I would certainly want to join you in that visit so that you can chat with the

great team that we have out there and also the contractor personnel that keeps the whole place going.

I would welcome your thoughts on the facility as we go forward in these economically constrained times.

General KEHLER. Senator, I'll do that. I could hear my staff back here volunteering to get on the airplane and go visit out there.

I can tell you that the entire Pacific Range complex, that really starts on the West Coast of the United States, goes to PMRF in Hawaii—there are other range assets in Hawaii elsewhere as well, as I know you know—and then it extends all the way out toward Kwajalein—is very, very important to the United States.

Senator HIRONO. So I can expect your continuing support for the new construction that's happening for the Aegis Ashore?

General KEHLER. Yes, you can.

Senator HIRONO. Again, I note in your testimony the challenge that you're facing—I think you might have talked about this a little bit—to process and analyze all the data that our intelligence, surveillance, and reconnaissance platforms are providing. So it's one thing to collect all the data and we want to be sure that that data is accurate. It's another as to how you're going to use that data, all this tremendous amount of raw information that you're getting.

Given the challenging budget situation that we face and the limits on the number of analysts that you have, the costs of data storage, and the limits on the amount of intelligence products your consumers can effectively use, how do you solve this problem and find the balance while ensuring that we don't miss something big?

General KEHLER. Senator, let me start and then I'm going to defer to my intelligence community colleague sitting on my left, because over the last ten years I think we've learned something in combat in Southwest Asia, and that is that it isn't about the collectors as much as it is about collecting and processing. So the more processing power we've been able to throw at the collection to have the machines make sense out of what is being collected, the better we have gotten. And it has provided great insight for forward forces to be able to carry out their missions and act in ways I think that the adversaries did not think we could act.

The question now and the trick is to extend that globally for all of our combatant commands as we look to the future. That's something that we are looking at as we speak. So that's going to be really important, and I'll defer to Keith because his organization has really been in the forefront of how do you use computing power to help us in this collection business.

General ALEXANDER. Senator, I think one of the things—and I'll just go back to Iraq—was putting together a real-time regional gateway capability—think of this as the processing power that General Kehler talks about—and putting it forward with our combat troops so that they had the information they needed.

I think there's a few things that you have to put on the table: first, understanding the needs of the tactical commander, what do they need to do their job. So from the intelligence community perspective that means our folks going down and being in their environment, living in their environment, and understanding what their needs are, and then having access to all the data that the collectors do.

I think this committee and others and some of your staff have worked hard to ensure that the sensors that we have push their information into data stores that everybody could use. This is key, key to leveraging the power of our collectors, national, theater, and tactical, to impact the tactical commander's requirements. We've made great strides in that.

I know you've been up to NSA Hawaii, a wonderful facility, and I think some of the capabilities exist there, and our folks would love to walk you through those.

Senator HIRONO. So I take it that the research and development component of what you do is very critical and that we need to continue to provide resources for that in order to enable you to do what you need to do with all this massive data that you are needing to analyze.

I note, General Alexander, that you had talked a little bit about how important recruiting and retaining your key personnel would be. I note in your testimony that you wanted to increase the education of our future leaders by fully integrating cyber into our existing War College curricula. You noted that this will further the assimilation of cyber into the operational arena for every domain.

So I know that what you're working in is an area that needs to become fully integrated and assimilated. What are your thoughts on how long this is going to take to make sure that the curricula incorporates cyber and that cyber is at the forefront of what all of our generals should be thinking about?

General ALEXANDER. It should be absolutely the first thing they learn and the most important. That's my view, of course. I do think—

Senator HIRONO. I tend to share that view. This is a new area and I think that we are very, very vulnerable on the cyber front.

General ALEXANDER. So I speak at the war colleges. We have people at the war colleges on the NSA side that carry that message forward, and we are adding it into the curriculum and these courses are growing.

We are also working with the Defense Intelligence Agency on setting up a cyber, if you will, mid-grade course for field grade officers, the young O3s, 04s that we have. And we have a series of courses that we have for our folks and for staffs, for the combatant command staffs, not just ours but all of them, to understand cyber.

The interesting part here is we'll get that set up, but it's key to note that every day this area changes. So keeping on top of it and keeping those changes is what we really need to do, and keeping people aware of those changes and the impact those changes have. That's the key part.

One of the great parts about having Cyber Command at NSA is that we can leverage the academic capabilities of NSA with the military working together to ensure we have these courses that both our civilian and military people go through. We've made great strides in that and we have a whole series of courses that we can show you that we're giving to our folks.

Then when I talk publicly, I also give people insights to books that they should read. When I was a younger officer, I know I did not read all those books that people recommended, but there are

some great books out there on cyber space that we recommend that they read.

Senator HIRONO. So are you satisfied that this assimilation is going on fast enough and that it will continue? As you note, changes occur very rapidly in this area.

General ALEXANDER. It's growing. It's not fast enough. There's a lot that we have to do. But changing some of these courses takes time. We are pushing this very hard, with a focus on those folks that first have to operate in this area. I think that part is going well. And we do have the staff-level courses out, and we have opened it up for all the combatant commands, and we're hitting those key parts.

Finally, I'll tell you that the Chairman and others have worked with the combatant commands and had these discussions with all of us sitting around the table to talk about cyber in a classified environment, so everybody understands the threat of that. I'll tell you, the senior officers in our military do understand that.

Senator HIRONO. You noted just now that this is an area that changes very rapidly and you have to stay on top of these changes. So can you talk a little bit about how you would measure effectiveness in your cyber security efforts and what kind of metrics would you use to determine whether we're on the right track?

General ALEXANDER. There's two parts to measuring that. One is certifying individuals, so we are developing a certification program—think about getting a flying license—that our cyber operators would have to be certified to operate in cyber space for different functionalities. That's one part.

The other is in our defense, looking at what we see in going through our cyber readiness inspections to see where each of our commands in the military are in defending their networks. What we've seen is a constant improvement in the cyber readiness of those networks. It's not perfect, but it's growing and getting better.

Senator HIRONO. That's reassuring.

I recall that you testified about how important collaboration is with the private sector. Can you talk a little bit about what you see as the kind of collaboration? Are we talking about collaborating on information with the private sector, collaborating on technology? And then you also said that in order for all of this to happen that the private sector would need insulation from liability. So can you talk a little bit more specifically about what you mean and why the private sector needs liability protection?

General ALEXANDER. Senator, the key things that they need, that we need in sharing information, is the ability for those to understand the threats as we see them, perhaps in a classified environment, and what they're seeing in threats in their networks. They're going to be looking at different portions of our networks than the government looks at. So together we see more if we put those two facts together, and we can come up with a more defensible architecture.

So there's that sharing of information on the threats that we both see. Those threats could be just routine malicious software that's out there to nation-state capabilities. That's one set of threats, and sharing it.

The second part is, so what do you do to fix the networks and make them more defensible? Here industry and government have some great ideas, and implementing those, for example the joint information environment, is just such a path forward that gives us a more defensible architecture because it allows us to patch at a more rapid rate and see threats better than we've ever been able to in the past. So it's those kinds of things that we're working on to move forward.

The reason we need liability protection is when we share some of this information with industry or they share it back, the liability that they incur because they are acting perhaps as an agent of the government in letting us know a threat is significant. And allowing them to be sued in some of these areas, from my perspective, when we're asking them to do something and then they bear the brunt of that lawsuit, is not right, and we ought to fix that and address that. We ought to give them the authority to share their information with the government, which they don't have today.

Senator HIRONO. Thank you.

I apologize for going over my time. I didn't see the little blue note. But thank you so much, Mr. Chairman.

Chairman LEVIN. Thank you, Senator Hirono, and we will put these blue notes a little bit closer to the eye contact in the future. But you've always maintained your courtesy, so I'm sure our colleagues understand.

Senator LEE. Thank you, Mr. Chairman.

Thank you, General Kehler and General Alexander, for joining us today and for your service to our country. Both of those things are deeply appreciated.

General Kehler, in June of 2010 as the Senate was considering the New START treaty, your predecessor General Chilton testified before the Senate Foreign Relations Committee that the force level under that treaty, meaning 1,550 warheads on 700 delivery vehicles, was "exactly what is needed today to provide the deterrent."

Did I understand your answer to Senator Fischer's question as being inconsistent with that? I think I did. I thought I heard you say we could go lower than that. If that's exactly what we needed in 2010, what has changed between now and then?

General KEHLER. Senator, I think I'm not inconsistent with that, so let me explain. The way we determine the size of the force, we don't start with a number. What we start with is a set of national security objectives. Those objectives eventually wind up being military tasks. Those tasks require a certain number of weapons to achieve.

When General Chilton was asked that question, he took a look at the national objectives that he had at the time, the tasks that he was asked to perform, and he looked at the number of weapons that were going to be permissible under the New START Treaty, and he said all of those matched.

My point is that we may have opportunities to go below that, but it doesn't start with a number; it's got to start with national objectives and military tasks that would be associated with it.

Senator LEE. Okay. So you're not saying as of right now you're certain or you're confident that we could go below that. You're say-

ing it is possible, based on further assessments at some point in the future?

General KEHLER. Yes, sir, I think that's right. I think it's possible, based upon assessments, based upon national objectives, based upon the military tasks we would be asked to achieve. And I think it depends on the nature of any threat that's out there. So I think many factors go into the number.

My contention is, though, like the nuclear posture review said, I support this. I think we should explore whether further reductions are possible.

Senator LEE. One of the reasons why I think I was a little bit surprised to hear you say that, though, was in light of the ambitious ongoing modernization programs that we have going on in Russia and in China, and in light of the fact that we've got other countries like North Korea and Iran with aggressive nuclear ambitions. I would think that our risk and our threat would be on the increase and our need for those weapons would not necessarily be diminishing. Am I mistaken in that regard?

General KEHLER. I think all of those factors need to be considered. Primarily, though, yet today the arsenal that we have, that was built during the Cold War, and the arsenal that the Russians have represent the vast majority of the weapons that exist. So——

Senator LEE. Sure, I understand that. But you know, there are a lot of countries that rely, a lot of countries in addition to the United States, that rely on our nuclear arsenal.

General KEHLER. Most definitely.

Senator LEE. So that umbrella, if you will, extends over a number of our allies, some of which lie in close proximity to countries like Iran and countries like North Korea. What consequence do you think it might have if we diminish our nuclear forces even further, either through reductions or because of a failure to modernize adequately? What impact might that have on some of our allies who rely on our own nuclear capabilities to protect them? And couldn't that bring about additional nuclear proliferation?

General KEHLER. I think that's always a possibility. I think we would have to be mindful of that as we go forward and that needs to be one of the factors considered.

Senator LEE. Now, do you think that countries like Saudi Arabia, Turkey, or maybe other nations in the Middle East might feel compelled to develop nuclear weapons in the relatively near-term future if, for example, Iran is able to achieve status as a nuclear power?

General KEHLER. There have been some reports that some of those countries would consider it. Whether—I don't have a good feeling from my position about what our official view is of that, but I think that again any time that we are talking about extending our nuclear guarantee, which is what we have done for many, many, many years, that our allies, what they've told us when they come and visit my headquarters is that it concerns them as we consider making changes. So I think we need to be mindful of those concerns and address them accordingly.

Senator LEE. Right, right. That probably means that we ought to be cautious before reducing our nuclear arsenal, and we also ought to be very concerned about our failure to modernize adequately

those weapons systems, wouldn't it? Because again, it seems to me logical that, especially as we've got states like Iran and North Korea moving in that direction, that inevitably will have a huge impact on what other countries do and what other countries do will in turn most likely put more of a burden on us and further strain our ability to provide that assurance that we've provided in the past, would it not?

General KEHLER. I think, Senator, as we have always thought, ultimately our ability to deter, our ability to extend that deterrence and assure our allies with that is based on the credibility of our nuclear deterrent and our nuclear deterrent force. Increasingly, certainly over the last decade now, the presence and capability of our conventional capabilities has made a difference, and I think in some cases has set a different context for the way we view our nuclear forces. But they still remain critical, I believe, and complementary.

Senator LEE. Okay. In the minute and a half or so that I have left, I'd like to talk to you a little bit about China. What can you tell me about the Chinese nuclear arsenal, and in particular whether you believe that China will continue to increase its—the number of weapons in its arsenal, and whether it's going to try to seek a level of equivalency with the United States and Russia in terms of nuclear weapons?

General KEHLER. Senator, I think we need to have a more full conversation in a different setting than this. But just in this setting, what I would say is we watch China continuing to modernize portions of their nuclear force. In terms of numbers, I believe the number ranges that are intelligence community has assessed with that—I don't think I can state that here, but I tend to believe that they're in about the range that we are talking about.

I do not see, nor has the intelligence community reported to me, that they are seeking to have some kind of numeric parity with the United States or with Russia. But I would quickly say I think this is why we want more transparency with China. We'd like to know what their intentions are going forward and we'd like to be able to expand our dialogue with them so that we can prevent any misunderstandings.

Senator LEE. Thank you very much, General.

Thank you, Mr. Chairman. I see my time has expired.

Chairman LEVIN. Thank you very much, Senator Lee.

Senator Graham.

Senator GRAHAM. Thank you, Mr. Chairman.

I certainly want to associate myself with the line of questioning of Senator Lee. I think he's right on point. We've got to look at the world we live in when we make these decisions about numbers and capabilities.

General Kehler, am I pronouncing your name right?

General KEHLER. Yes.

Senator GRAHAM. Close enough?

Senator FISCHER. Yes, you and I are right.

Chairman LEVIN. We've been batting about 500 on the committee today.

Senator GRAHAM. Well, I'm a colonel. I don't want to get courtmartialed. [Laughter.]

Are we spending enough money to modernize our nuclear weapons force?

General KEHLER. I think we are coming out of a period where the answer was no. I think—

Senator GRAHAM. How does sequestration affect?

General KEHLER. It affects it. I can tell you it affects it in the near term in terms of the potential impact on readiness, as I mentioned earlier, which will come about over a period of months. I described this earlier as a slow-motion impact in STRATCOM, because the services are trying to protect——

Senator GRAHAM. Well, as part of the START Treaty negotiations was, those who voted for the treaty—I did not—there was a promise given we'd modernize our nuclear force.

General KEHLER. And part two of sequestration, of course, is the overall budget totals which are coming down.

Senator GRAHAM. So basically my view is we never honored the modernization commitment in terms of funding, and along comes sequestration. So you've been hit twice. We never gave the—we never made the commitment that was promised in terms of modernization funds, even though it was more than in the past. And now you have sequestration. It's sort of a double whammy. Would you agree?

General KEHLER. Well, I don't know yet, sir, what the sequestration investment impact is going to be on us. I don't know. The budget details have yet to be worked out.

Senator GRAHAM. Well, if it's across the board your account will be hit, right?

General KEHLER. Certainly if the rules stay the way they are, across the board.

Senator GRAHAM. Well, let's just assume that. Get back to me or the committee in writing: Assuming an across-the-board continuation over a ten-year period, what it would do to our nuclear modernization efforts. Could you do that?

General KEHLER. Yes, I can.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator GRAHAM. General Alexander, why isn't an attack on critical infrastructure in this Nation, a cyber attack by a government like China or Russia, why is that not considered an act of war?

General ALEXANDER. That's a great question and I think one that needs to be ironed out: What constitutes an act of war in cyber space? So let me give you my thoughts on that—

Senator GRAHAM. Please.

General ALEXANDER.—versus trying to bat this around.

Senator GRAHAM. There is no clear answer, I agree with you.

General ALEXANDER. Right. I think first I would look at the laws of armed conflict, the intent of the Nation, and what they're doing. I would say what we're seeing today from those countries, essentially espionage and theft of intellectual property, is not an act of war.

Senator GRAHAM. What about military modernization plans, stealing—a lot of their fighters tend to look like our fighters.

General ALEXANDER. That's right, and a lot, a lot across the board. So I think that's espionage. I think that's theft of intellec-

tual property. I would say that the intent is to steal secrets and you're into the espionage, criminal

If the intent is to disrupt or destroy our infrastructure, I think you've crossed a line. So somewhere in that zone——

Senator GRAHAM. Have you seen an intent, a planning process in place where enemies of the Nation would attack us through cyber space? Is that something we should be worried about?

General ALEXANDER. Yes, that's something we should be worried about, and I can give you more details in a closed setting.

Senator GRAHAM. All right. Now let's talk about outside Department of Defense. You can defend the defense infrastructures, but you're so connected to the private sector one cannot be disconnected from the other; is that correct?

General ALEXANDER. That's correct.

Senator GRAHAM. We don't have a little bubble that you can protect. If systems go down, if power systems go down, it affects you. If financial services are disrupted it would affect you. You can just go on and on with how an attack on critical infrastructure could affect our national security.

Have you talked to Senator Whitehouse about his proposed solution of dealing with critical infrastructure?

General ALEXANDER. I have not, not the latest one. I have talked to Senator Whitehouse in the past and found that he and I are essentially in sync on those discussions. But I haven't seen his latest.

Senator GRAHAM. I am with him. The concept is that we would identify critical infrastructure in the private sector, like power supply, financial services, things that every American depends on, and if they went down would hurt us as a Nation, hurt our economy, and could do harm to our citizens. I think his concept is that, let's identify our critical infrastructure and allow the industries in question, like the utilities, to come up with best business practices within their industry and submit their proposal to a collaborative body of government agencies, with Homeland Security certainly a key component of it.

And if these best business practices are in the minds of the government meaningful, we would grant liability protection to those who met those standards. It would be voluntary.

Does that sound like a reasonable way to proceed?

General ALEXANDER. Senator, I think in part that's reasonable. The issue that it leaves not addressed is the information-sharing part.

Senator GRAHAM. Right. That has to be done. That's a critical part of it.

Let's assume that we get the information-sharing right. We've got two ways to do this, through a regulatory regime—my belief is that regulations would be expensive and the threats move too fast for it to work. Do you agree with that?

General KEHLER. I do. In fact, I would say so if you separate the two and you have liability and information- sharing on one side and then you have liability and standards and regulation on the other side that work together, in essence that's essentially where the executive order is trying to go as well.

Senator GRAHAM. Right. So I would just want to encourage you. We'll meet with Senator Whitehouse and others and see if we can

find a pathway forward that would allow the private sector to set the standards in the critical infrastructure area, and the payoff would be liability protection, because this is an ever-changing threat.

Finally, what kind of damage could be done to our you through a cyber attack? Start with nation states, then criminal organizations. What kind of threat are we facing?

And finally, in South Carolina our database at the Department of Revenue was hacked into and every citizen's Social Security number and a lot of business information was stolen, causing the State of South Carolina a lot of chaos in trying to provide identity theft protection to our citizens. This was a massive intrusion into a State system where over 3 million Social Security numbers were seized.

Can you just quickly tell the committee the kind of threats we face, and if Congress doesn't get involved I think we will regret the day.

General ALEXANDER. Generally speaking, all our systems today, our power systems, our water systems, our governments, our industry, depend on computers, depend on computerized switches, depend on these networks, all are at risk. If an adversary were to get in, they could essentially destroy those components, make so that you either had to replace them or get somebody to come in and replace each part of that.

In the power grid as an example——

Senator GRAHAM. They could do as much or more damage than the attacks of 9–11?

General ALEXANDER. That's correct, I think it would. If you look at what happened in 2003 in the Northeast power disruption, that was caused by a software failure. That was not somebody attacking us. That was a software failure.

But now think about somebody imposing a software failure, not just in the Northeast, but across all of those and cascading that across the United States, and breaking some of the transformers, which would be very difficult to replace. We would have significant power outages for extended periods throughout the country.

Think about Wall Street if we were to go in and—I know Senator Blumenthal was asking questions on this earlier, about what happens if you attack Wall Street and you destroyed the data that they need to at the end of the day ensure all the books are right. If you can't close those books, which are done today by computers, you have a significant problem in our banking infrastructure, not just ours but global.

Senator GRAHAM. Since our time is up, if you could maybe just submit to the committee sort of a worst case scenario from a cyber attack, kind of a September 11 scenario.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator GRAHAM. Finally, the executive order I think is a result of Congress' inaction and I don't blame the President at all. Do you believe it would be prudent for the Congress to enhance the executive order, that we need legislation in this area beyond the executive order to make the Nation safe?

General ALEXANDER. I do.

Senator GRAHAM. Thank you.

Chairman LEVIN. We're expecting Senator Kaine back at any minute. Senator Inhofe has a question and then I'll have a question, and then we'll turn it over to Senator Kaine.

Senator INHOFE. General Kehler, in response to the question that was given to you by Senator Graham—he was talking about what's going to happen to you under sequestration, and then you qualified it and said, well, that is assuming it's going to be cut straight across the board. Of course that would be damaging, because that's done in my opinion without thought. It's just a cut across the board.

Now, I introduced legislation six weeks ago anticipating that maybe sequestration would happen. I didn't think it would, but I thought in case it does, to take the same top line as to how it's going to affect a whole division of bureaucracies and then say, in the case of you and of anything having to do with defense, take that and adhere to that top line, but allow the service chiefs underneath that to make those decisions, and would that be better?

And all the service chiefs, all five including the Guard chief—I contacted them, too—said yes, that would make a world of difference. The devastation is still there, but not as devastating.

Would you agree with that?

General KEHLER. Yes, sir, I would.

Senator INHOFE. Would you, General Alexander, too?

General ALEXANDER. I would, Senator.

Senator INHOFE. Thank you.

Chairman LEVIN. Thank you.

Now Senator Kaine.

Senator KAINE. Thank you, Mr. Chair.

Thank you, Generals Kehler and Alexander.

General Kehler, I just want to focus a little bit on some of your testimony that grabbed my attention. The opening comment that you made and that you repeated verbally today is uncertainty and complexity continue to dominate the national security landscape. I agree with that and I want to wrestle with questions that many of the colleagues here have asked about fiscal uncertainty.

We can't necessarily reduce the uncertainty in the broader world, but it is in our power as Congress to try to reduce some of the fiscal uncertainty that you're dealing with. One week ago yesterday, so the first weekday after the sequester cuts went into effect, I visited the Pentagon and spoke with Secretary Hagel and General Odierno, Deputy Secretary Carter. I spoke with General Welsh on that same day here in my office.

Then I went downstairs and didn't talk to the brass, but I went to the cafeteria and just went table to table. In three tables, just in the random three tables I went to, I've got active duty assigned to the Pentagon, veterans who were there having lunch with friends, DOD contractors, DOD civilians, and some Guard representatives who were there for planning meeting.

They were all sharing their concerns about sequester, CR, and the overall climate of uncertainty as it affects them and as it sends a message about our commitment to the mission, to the DOD mission. One affect of the uncertainty that I think just has really

dawned on me and increasingly in your testimony is the effect on personnel.

So a couple of the comments in your testimony. On page 2: "Fiscal uncertainty presents our people with an unprecedented combination of professional and personal concerns as well. The all-volunteer military and civilian team has performed beyond our greatest expectations and is the envy of the world. But some of the best young uniformed and non-uniformed people assigned to STRATCOM are questioning their future. The uncertainty surrounding civilian hiring restrictions, salary freezes, and the possibility of unpaid furloughs is especially troubling since," as you testified earlier, "60 percent of U.S. STRATCOM headquarters staff and much of the essential workforce which supports our missions and sustains our mission-critical platforms and systems are civilians."

Then with a specific reference to cyber, at the end of your testimony—and this is General Kehler's testimony, but I'm sure it's something that General Alexander resonates with as well: "Improving the DOD's ability to operate effectively in cyber space requires investment in five major areas." And then you go over the areas. "But of these, the most urgent intelligence is increasing the numbers, training, and readiness of our cyber forces."

Again, it's about personnel and the choices that people are making about their own future. It strikes me, and I just would like to hear you talk about this a bit more—I know that Senator Blunt raised it—it strikes me that you've got two issues of significant concern as you're trying to grow a cyber talent pool within DOD.

The first is the competition from the outside world, which from a salary and benefits standpoint I would imagine for these professionals can be pretty intense. The second is a fiscal uncertainty that people would have if they chose the path of public service. What would they face in terms of furloughs or pay cuts or pay freezes? What is the commitment that we have?

I would like to hear each of you just talk about how you deal with the sort of recruiting and retention in this environment when you not only have a global uncertainty, but tough economic competitors in the private sector and fiscal uncertainty as well.

General KEHLER. Senator, I would only add a couple of remarks. Number one, we have the most magnificent people anywhere. They're the envy of every other military in the world. They're like that for a reason. They're extraordinarily talented and they are very patriotic.

So normally I don't worry much about them other than to make sure that as a leader I'm doing everything that I can to take care of them and make sure that they're going to be there and that we're taking care of them and their families. That's been an interesting challenge, of course, over the last 10 or 12 years, with wounded and other things.

But I think as we look to the future here what I'm hearing from some of our folks is particularly troubling, and it gets back to uncertainty. As we all—of course, we all want the economy to get better and we'd like it to be better soon, as fast as it can possibly happen. But when that happens and as that happens, I guess is a better way to say it, as that happens, then this competition for our

best and brightest talent is going to go up. In that environment, I'm concerned that as they are weighing, not the personal threats to themselves, which they are willing to take, but when they are weighing the financial certainty for their families, that they'll come down on a different side than government service.

So I think that's an important question for us. We have an all-volunteer military. It's been stressed in a lot of different ways. This is another stressor on it. So I think we need to be mindful of this because we are competing for the best and brightest talent. We've been getting it. I believe again they are magnificent people that raise their right hand, whether that's a civilian or uniformed or whether they serve as a contractor. It doesn't seem to much matter; they're all working hard to do the right things.

It's preserving that, and there is an impact here with what is going on. There is an impact on them. It is coming to our level. They are telling us that there's an impact on them, and we need to be mindful of it.

Senator KAINE. General Alexander, could you comment additionally?

General ALEXANDER. Senator, two broad areas. First, I agree with everything that you read there. I think it's 100 percent on track.

We're impacted in Cyber Command in two areas. The continuing resolution impacts our ability to train more and we need to do that to get this force stood up. And I think by singling out the civilian workforce for furloughs we've done a grave injustice. You know, we're trying to get people to come in and support us in this technical area. People are leaving industry to come in and work with us. Now that they get there, they're saying: Did I make the wrong decision? You're going to furlough me now X percent of the time. I already took a salary reduction to come to work for you. I think it's a great thing for our Nation. But if this is the way it's going to be, I can't afford to do this to my family.

That's a big impact across our workforce and we shouldn't do that.

Senator KAINE. Let me stay on cyber and just move to a related area that raised some questions earlier as well. That is trying to pass the right kind of balanced cyber legislation. A lot of it is a dialogue between policymakers and the private sector and they have legitimate concerns. Thus far in your own experience, has the private sector expressed those concerns in the right way? Namely, has it been a series of, well, don't do this to us, don't do that to us, don't do this to us, or have they been offering ways that we can accomplish the goal in a productive and constructive way? Because if the answer to that is no, that might be something that we could help with, to try to smoke out the positives, the positive and constructive advice about how to balance some of these important considerations.

General ALEXANDER. Senator, I think the big problem is every sector approaches it slightly different. So what you get is 18, 20 different views, groups of views, on cyber and cyber legislation, what we need and how we need to do it. I think the executive order, that which Senator Graham and Senator Whitehouse are referring to, are in the right way: Get industry to sit down with the government

officials, put the Director of NIST in charge, bring all our technical talent there, and start talking with industry on the best way sector by sector, and then bring that back up to the administration, to you, and say: Here's what we think the way to work with industry to help make their networks more resilient.

What you'll find is each part of our industry sectors are at different states of cyber readiness, if you will, and that's the real problem that we face. I've talked to lots of CEO's out there on this topic area and you get from one side to the other. When you do that, you see that—when you really start drilling down, you see that some of them really need help, want help, are concerned about regulation and how we do it. Some of them don't need help and are concerned about the "help" we're going to give them.

So I think what we have to do is address each of those concerns and do it in a fair and equitable way. I think that executive order reach-out is a great step in the right direction.

Senator KAINE. Thank you both very much.

Mr. Chairman, thanks.

Chairman LEVIN. Thank you, Senator Kaine.

Senator Inhofe, you all set?

If there are no other questions, we just want to thank you both for your great service to our country, your great testimony this morning, thoughtful, considered, and we are very appreciative of it; and we will stand adjourned.

[Whereupon, at 12:20 p.m., the committee adjourned.]

STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

12 MARCH 2013

Thank you very much Chairman Levin and Ranking Member Inhofe for inviting me to speak to you and your colleagues today on behalf of the men and women of U.S. Cyber Command. I have the honor of leading them on a daily basis, and let me assure you there is not a finer and more dedicated team of Service members and civilian personnel anywhere. It gives me great pleasure to appear before you to talk about their accomplishments, and to describe some of the challenges they face in performing their difficult but vital mission of keeping U.S. military networks secure, helping to protect our nation's critical infrastructure from national-level cyber attacks, assisting our Combatant Commanders around the world, and working with other U.S. Government agencies tasked with defending our nation's interests in cyberspace.

USCYBERCOM is a subunified command of U.S. Strategic Command in Omaha, though we are based at Fort Meade, Maryland. We have approximately 834 active-duty military and civilians assigned from an authorized end-strength of 917 (plus contractors), and a budget of approximately $191 million for Fiscal Year 2013. USCYBERCOM has strong, evolving, and growing cyber components representing each of the Services: Fleet Cyber Command/Tenth Fleet, Army Cyber Command/Second Army, Air Force Cyber Command/24th Air Force, and Marine Forces Cyber Command. Each of our Service Cyber Components also has representation at our headquarters. Combined we and they have more than 11,000 people in our force mix.

US Cyber Command shares its headquarters with key mission partners in the National Security Agency (NSA), which I also lead. USCYBERCOM's co-location with NSA promotes intense and mutually beneficial collaboration. The Department of Defense established U.S. Cyber Command in 2010 to leverage NSA's capabilities. This partnership is key to what we are doing now, and provides the essential context for all the activities I shall describe below. The people under my command and direction at USCYBERCOM and NSA are collectively responsible for operating the Department's information networks, detecting threats in foreign cyberspace, attributing threats, securing national security and military information systems, and helping to ensure freedom of action for the United States military and its allies in cyberspace—and, when directed, defending the nation against a cyber attack. Also nearby at Fort Meade is another key mission partner, the Defense Information Systems Agency (DISA). The constellation of agencies and capabilities in the Washington DC region makes for a unique synergy of people and ideas—a nexus for military and national cybersecurity innovation.

USCYBERCOM has deployed representatives and mission support elements worldwide. We have an expeditionary cyber support unit forward in Afghanistan. We also have liaison officers at each Combatant Command

(serving as that Command's CSE lead) and in several other key offices and agencies in the Washington area. The flow of information and advice across USCYBERCOM and its Service components and the commands, agencies, and foreign mission partners here and overseas is improving slowly but steadily.

Since I last spoke with you in March 2012, our progress has accelerated. In December we moved ahead with building a balanced and highly capable military cyber force designed to meet our joint warfighting requirements. We have laid out and codified team composition, training, and certification standards to field a world-class force in support of the Combatant Commands (CCMDs). Although we have much work to do, we are focused on doing it right and meeting the CCMDs' and the nation's most pressing cyber defense requirements. In short, we have moved ahead to normalize cyber operations within the U.S. military, and to turn that capability into a reliable option for decisionmakers to employ in defending our nation. This progress will not only make our military more capable but our networks and information more secure. We have serious threats facing us, as I shall explain. Our progress, however, can only continue if we are able to fulfill our urgent requirement for sufficient trained, certified, and ready forces to defend U.S. national interests in cyberspace.

The Strategic Landscape

U.S. Cyber Command operates in a dynamic and contested environment that literally changes its characteristics each time someone powers on a networked device. Geographic boundaries are perhaps less evident in cyberspace, but every server, fiber-optic line, cell tower, thumb drive, router, and laptop is owned by someone and resides in some physical locale. In this way cyberspace resembles the land domain—it is all owned, and it can be re-shaped. Most networked devices, for example, are in private hands, and their owners can deny or facilitate others' cyber operations by how they manage and maintain their networks and devices. Cyberspace as an operating environment also has aspects unique to it. Events in cyberspace can seem to happen instantaneously. Data can appear to reside in multiple locations. There is a great deal of anonymity, and strongly encrypted data are virtually unreadable. In cyberspace, moreover, sweeping effects can be precipitated by states, enterprises, and individuals, with the added nuance that such cyber actors can be very difficult to identify. The cyber landscape also changes rapidly with the connection of new devices and bandwidth, and with the spread of strong encryption and mobile devices. Despite the unique characteristics of cyberspace, states still matter because they can affect much of the physical infrastructure within their borders. Convergence is our watchword; our communications, computers, and networks are merging into one digital environment as our political, economic, and social realms are being re-shaped by the rush of innovation.

In this environment that is both orderly and chaotic, beneficial and perilous, we at USCYBERCOM have to focus on actors who possess the capability—and possibly the intent—to harm our nation's interests in cyberspace or to use cyber means to inflict harm on us in other ways. Unfortunately, the roster of actors of concern to us is growing longer and growing also in terms of the variety and sophistication of the ways they can affect our operations and security.

State actors continue to top our list of concerns. We feel confident that foreign leaders believe that a devastating attack on the critical infrastructure and population of the United States by cyber means would be correctly traced back to its source and elicit a prompt and proportionate response. Nonetheless, it is possible that some future regime or cyber actor could misjudge the impact and the certainty of our resolve.

We have some confidence in our ability to deter major state-on-state attacks in cyberspace but we are not deterring the seemingly low-level harassment of private and public sites, property, and data. As former Secretary of Defense Panetta explained to an audience in New York last October, states and extremist groups are behaving recklessly and aggressively in the cyber environment. Such attacks have been destructive to both data and property. The Secretary mentioned, for example, the remote assaults last summer on Saudi Aramco and RasGas, which together rendered inoperable—and effectively destroyed the data on—more than 30,000 computers. We have also seen repressive regimes, desperate to hold on to power in the face of popular resistance, resort to all manner of cyber harassment on both their opponents and their own citizens caught in the crossfire. Offensive cyber programs and capabilities are growing, evolving, and spreading before our eyes; we believe it is only a matter of time before the sort of sophisticated tools developed by well-funded state actors find their way to non-state groups or even individuals. The United States has already become a target. Networks and websites owned by Americans and located here have endured intentional, state-sponsored attacks, and some have incurred damage and disruption because they happened to be along the route to another state's overseas targets.

Let me draw your attention to another very serious threat to U.S. interests. The systematic cyber exploitation of American companies, enterprises, and their intellectual property continued unabated over the last year. Many incidents were perpetrated by organized cybercriminals. Identity and data theft are now big business, netting their practitioners large profits and giving rise to an on-line sub-culture of markets for stolen data and cyber tools for stealing more. Much cyber exploitation activity, however, is state-sponsored. Foreign government-directed cyber collection personnel, tools, and organizations are targeting the data of American and western businesses, institutions, and citizens. They are particularly targeting our

telecommunications, information technology, financial, security, and energy sectors. They are exploiting these targets on a scale amounting to the greatest unwilling transfer of wealth in history. States and cybercriminals do not leave empty bank vaults and file drawers behind after they break-in—they usually copy what they find and leave the original data intact—but the damage they are doing to America's economic competitiveness and innovation edge is profound, translating into missed opportunities for U.S. companies and the potential for lost American jobs. Cyber-enabled theft jeopardizes our economic growth. We at USCYBERCOM work closely with our interagency partners to address these threats.

We must also watch potential threats from terrorists and hacktivists in cyberspace. The Intelligence Community and others have long warned that worldwide terrorist organizations like al Qaeda and its affiliates have the intent to harm the United States via cyber means. We agree with this judgment, while noting that, so far, their capability to do so has not matched their intent. This is not to downplay the problem of terrorist use of the Internet. Al Qaeda and other violent extremist groups are on the Web proselytizing, fundraising, and inspiring imitators. We should not ignore the effectiveness with which groups like al Qaeda and its affiliates radicalize ever larger numbers of people each year—on more continents. The Federal Bureau of Investigation and other agencies cite instances in which would-be terrorists found motivation and moral support for suicide attacks at jihadist websites and chat rooms. This is an especially serious and growing problem in areas of hostilities where our troops and personnel are deployed. Another threat that is not growing as fast as we might have feared, on the other hand, is that of hacktivists with a cause or a grievance that leads them to target U.S. government and military networks. Our vulnerabilities to this sort of disruption remain, but 2012 saw fewer such incidents than 2011.

Looking Ahead: The Command's Priorities

I have established several priorities for U.S. Cyber Command in dealing with these risks and threats. We are actively working to guard the Department of Defense's networks and information and helping to defend the nation. Key to countering these threats is learning <u>how</u> to grow our capabilities in this challenging domain. We have no alternative but to do so because every world event, crisis, and trend now has a cyber-aspect to it, and decisions we make in cyberspace will routinely affect our physical or conventional activities and capabilities as well. USCYBERCOM is building cyber capabilities into our planning, doctrine, and thinking now—while we as a nation have time to do so in a deliberate manner. We do not want to wait for a crisis and then have to respond with hasty and ad hoc solutions that could do more harm than good.

When I say we are normalizing cyber operations, I mean we are making them a more reliable and predictable capability to be employed by our senior decisionmakers and Combatant Commanders. Normalizing cyber requires improving our tactics, techniques, and procedures, as well as our policies and organizations. It also means building cyber capabilities into doctrine, plans, and training – and building that system in such a way that our Combatant Commanders can think, plan, and integrate cyber capabilities as they would capabilities in the air, land and sea domains.

In keeping with the Department of Defense's *Strategy for Operating in Cyberspace*, U.S. Cyber Command and NSA are together assisting the Department in building: 1) a defensible architecture; 2) global situational awareness and a common operating picture; 3) a concept for operating in cyberspace; 4) trained and ready cyber forces; and 5) capacity to take action when authorized. Indeed, we are finding that our progress in each of these five areas benefits our efforts in the rest. We are also finding the converse—that inertia in one area can result in slower progress in others. I shall discuss each of these priorities in turn.

Defensible Architecture: The Department of Defense (DoD) owns seven million networked devices and thousands of enclaves. Cyber Command works around the clock with its Service cyber components, with NSA, and with DISA to monitor the functioning of DoD networks, including the physical infrastructure, the configurations and protocols of the components linked by that infrastructure, and the volume and characteristics of the data flow. This is a dynamic defense, and it consistently provides better security than the former patch-and-firewall paradigm. Patches and firewalls are still necessary—I wish everyone kept theirs up-to-date—but they are an insufficient defense for DoD networks. Dynamic defenses have brought about noticeable improvements in the overall security of DoD information environment. We know for a fact that our adversaries have to work harder to find ways into our sensitive but unclassified networks. Unfortunately, adversaries are willing to expend that effort, and DoD's architecture in its present state is not defensible over the long run. We in the Department and the Command are crafting a solution. The Department's bridge to the future is called the DoD Joint Information Environment (JIE), comprising a shared infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize information technology (IT) efficiencies. The JIE will be the base from which we can operate in the knowledge that our data are safe from adversaries. Senior officers from USCYBERCOM and NSA sit on JIE councils and working groups, playing a leading role with the office of the DoD's Chief Information Officer, Joint Staff J6, and other agencies in guiding the Department's implementation of the JIE. NSA, as the Security Adviser to the JIE, is defining the security dimension of that architecture, and has shown how we can pool big data and still preserve strong security. We have even shared the source code publicly so public and private architectures can benefit

from it. DoD is benefitting from that knowledge and from our growing understanding of the totality of measures, procedures, and tools required to assure the health and security of even the biggest networks and databases.

Increased Operational Awareness: Enhanced intelligence and situational awareness in our networks will help us know what is happening in the cyberspace domain. This effort can be likened to a cyber version of the tactical air picture of friendly, neutral, and aggressor aircraft that a Combined Air Operations Center in a Combatant Command typically maintains. We are now issuing a weekly Cyber Operating Directive (CyOD) across the DoD cyber enterprise for just this purpose, so that all "friendlies" understand what is happening in cyberspace. Our improving knowledge of what is normal in cyberspace is crucial to grasping what is not normal. We at USCYBERCOM are also helping DoD increase our global situational awareness through our growing collaboration with federal government mission partners like the Department of Homeland Security (DHS), the FBI, and other departments and agencies, as well as with private industry and with other countries. That collaboration in turn allows us to better understand what is happening across the cyber domain, which enhances our situational awareness, not only for the activities of organizations based at Fort Meade but also across the U.S. government. I am happy to report that at least one of our foreign partners has volunteered to invest in this and enter its own network traffic data to contribute to a common picture.

Operating Concepts: Our operating concept calls for us to utilize our situational awareness to recognize when an adversary is attacking, to block malicious traffic that threatens our networks and data, and then to maneuver in cyberspace to block and deter new threats. I am pleased to report that in December, the Department endorsed the force presentation model we need to implement this new operating concept. We are establishing cyber mission teams in line with the principles of task organizing for the joint force. The Services are building these teams to present to U.S. Cyber Command or to support Service and other Combatant Command missions. The teams are analogous to battalions in the Army and Marine Corps—or squadrons in the Navy and Air Force. In short, they will soon be capable of operating on their own, with a range of operational and intelligence skill sets, as well as a mix of military and civilian personnel. They will also have appropriate authorities under order from the Secretary of Defense and from my capacity as the Director of NSA. Teams are now being constructed to perform all three of the missions given to U.S. Cyber Command. We will have 1) a Cyber National Mission Force and teams to help defend the nation against national-level threats; 2) a Cyber Combat Mission Force with teams that will be assigned to the operational control of individual Combatant Commanders to support their objectives (pending resolution of the cyber command and control model by the Joint Staff); and 3) a Cyber Protection Force and teams to help operate and defend DoD information environment.

Trained and Ready Forces: Each of these cyber mission teams is being trained to common and strict operating standards so that they can be on-line without putting at risk our own military, diplomatic, or intelligence interests. Doing this will give not only U.S. Cyber Command's planners, but more significantly our national leaders and Combatant Commanders, a certain predictability in cyber capabilities and capacity. Key to building out the Cyber Mission Force articulated in our Force Planning Model is having the training system in place to train each of the cyber warriors we need, in the skill sets we require and at the quality mandated by the cyber mission. We have that training system in place for the operators, and now we need to build the accompanying Command and Staff academic support packages and programs to ensure our officers and planners know how to effectively plan for and employ cyber capabilities for our nation. As a result of this operator and staff training system, decisionmakers who require increments of cyber skills to include in their plans will know how to ask for forces to fill this requirement, and planners will know how to work cyber effects into their organizations' plans. To build the skills of the force—as well as to test the ways in which its teams can be employed—U.S. Cyber Command has sponsored not only an expanding range of training courses but also two important exercises, CYBER FLAG and CYBER GUARD. The latter assembled 500 participants last summer including a hundred from the National Guards of twelve states. They exercised state and national-level responses in a virtual environment, learning each other's comparative strengths and concerns should an adversary attack our critical infrastructure in cyberspace. CYBER FLAG is our annual exercise at Nellis Air Force Base in Nevada and we conduct it with our inter-agency and international partners. Our most recent running of CYBER FLAG introduced new capabilities to enable dynamic and interactive force-on-force maneuvers at net-speed, while incorporating actions by conventional forces as well at Nellis' nearby training area.

Capacity to Take Action: Successful operations in cyberspace depend on collaboration between defenders and operators. Those who secure and defend must synchronize with those who operate, and their collaboration must be informed by up-to-date intelligence. I see greater understanding of the importance of this synergy across the Department and the government. The President recently clarified the responsibilities for various organizations and capabilities operating in cyberspace, revising the procedures we employ for ensuring that we act in a coordinated and mutually-supporting manner. As part of this progress, the Department of Defense and U.S. Cyber Command are being integrated in the machinery for National Event responses so that a cyber incident of national significance can elicit a fast and effective response to include pre-designated authorities and self-defense actions where necessary and appropriate. USCYBERCOM is also working with the Joint Staff and the Combatant Commands to capture their cyber requirements and to implement and refine interim guidance on the command and control of cyber forces in-

theater, ensuring our cyber forces provide direct and effective support to commanders' missions while also helping U.S. Cyber Command in its national-level missions. In addition, we are integrating our efforts and plans with Combatant Command operational plans and we want to ensure that this collaboration continues at all the Commands. Finally, most cyber operations are coalition and interagency efforts, almost by definition. We gain valuable insight from the great work of other partners like the Departments of Justice and Homeland Security, such as in their work against distributed denial of service attacks against American companies, which in turn helps DoD fine-tune defenses for the DoD information environment. We also benefit from sharing with the services and agencies of key partners and allies. We welcome the interagency collaboration and evolving frameworks under which these efforts are proceeding, especially such revisions that would make it easier for the U.S. Government and the private sector to share threat data, as the administration previously emphasized. In addition, new standing rules of engagement for cyber currently under development will comply with and support recently issued policy directives on U.S. cyber operations.

Building for the Future

We have made strides in all of our focus areas, though what gratifies me the most is seeing that we are learning how they all fit together. We are building quickly and building well, but we are still concerned that the cyber threats to our nation are growing even faster. From the technological, legal, and operational standpoints we are learning not only what is possible to accomplish but also what is wise to attempt. Our plans for U.S. Cyber Command over the foreseeable future—which admittedly is not a very distant horizon—should be understood in this context.

In a speech last fall, then-Secretary Panetta emphasized the Department's need to adjust our forces as we transition away from a decade of war. He explained that a wise adjustment makes cuts without hollowing out the force, while also investing in ways that prepare us to meet future needs. We will do that, he said, by increasing our investments in areas including space and cyber. It is fair to ask how we plan to use such new resources while others are trimming back. Our new operating concept to normalize cyber capabilities is just the sort of overarching theme to unite the whole institutional push. We need to foster a common approach to force development and force presentation—up to and including the Service component and joint headquarters—given the intrinsically joint nature of this domain.

Let me emphasize that this is not a matter of resources alone – it is a matter of earning trust. We will continue to do our work in full support and defense of the civil liberties and privacy rights enshrined in the U.S.

Constitution. We do not see a tradeoff between security and liberty. We can and must promote both simultaneously because each enhances the other. U.S. Cyber Command takes this responsibility very seriously. Indeed, we see this commitment in our day-by-day successes. We in the Department of Defense and DHS, with DOJ and industry, for instance, have shown that together we can share threat information, to include malware signatures, while still providing robust protection for privacy and civil liberties..

Building the Department's defensible cyber architecture will let us guard our weapons systems and military command and control as well as our intelligence networks. We hope to take the savings in personnel and resources gained by moving to the JIE and have the Services repurpose at least some of them to hunt for adversaries in our DoD networks and even to perform full-spectrum operations. Although doing so will require a large investment of people, resources, and time, in the long run it will be cheaper to train Service personnel than to hire contractors. Moving to the JIE will make sharing and analytics easier while also boosting security. I know this sounds paradoxical but it is nonetheless true, as NSA has demonstrated in its Cloud capability. If we know what is happening on our networks, and who is working in them and what they are doing, then we can more quickly and efficiently see and stop unauthorized activities. We can also limit the harm from them and more rapidly remedy problems, whether in recovering from an incident or in preventing one in the first place. This is our ultimate objective for operations on our Department of Defense information architecture.

As we grow capacity, we are building cyber mission teams now , with the majority supporting the Combatant Commands and the remainder going to USCYBERCOM to support national missions. When we have built this high-quality, certified, and standardized force, we will be able to present cyber forces with known capability sets to our Combatant Commanders—forces they can train with, plan for, plan on, and employ like forces and units any other military domain. This gets at the essence of normalizing cyber capabilities for the Department of Defense. Furthermore, we want to increase the education of our future leaders by fully integrating cyber in our existing war college curricula. This will further the assimilation of cyber into the operational arena for every domain. Ultimately we could see a war college for cyber to further the professional military education of future leaders in this domain.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak to you today. I hope you will agree with me that U.S. Cyber Command has made progress across the board in the last year, thanks to the support of Congress and our interagency and international partners, as well as the hard work of its many dedicated men and women. The novelist and

visionary William Gibson once noted “The future is already here, it’s just not evenly distributed.” We are seeing that future at U.S. Cyber Command. Cyber capabilities are already enhancing operations in all domains. We are working to contain the vulnerabilities inherent in any networked environment or activity while ensuring that the benefits that we gain and the effects we can create are significant, predictable, and decisive. If I could leave you with one thought about the course of events, it is that we have no choice but to normalize cyberspace operations within the US military and make them part of the capability set of our senior policymakers and commanders. I am ready to take your questions and to clarify our Command’s achievements and challenges, and to discuss any concerns that you might wish to share.