[H.A.S.C. No. 112–26]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2012

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES HEARING

ON

BUDGET REQUEST FOR U.S. CYBER COMMAND

HEARING HELD
MARCH 16, 2011

U.S. GOVERNMENT PRINTING OFFICE
65–593 WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MAC THORNBERRY, Texas, *Chairman*

JEFF MILLER, Florida
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
CHRIS GIBSON, New York
BOBBY SCHILLING, Illinois
ALLEN B. WEST, Florida
TRENT FRANKS, Arizona
DUNCAN HUNTER, California

JAMES R. LANGEVIN, Rhode Island
LORETTA SANCHEZ, California
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
TIM RYAN, Ohio
C.A. DUTCH RUPPERSBERGER, Maryland
HANK JOHNSON, Georgia
KATHY CASTOR, Florida

KEVIN GATES, *Professional Staff Member*
MARK LEWIS, *Professional Staff Member*
JEFF CULLEN, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2011

WEDNESDAY, MARCH 16, 2011

FISCAL YEAR 2012 NATIONAL DEFENSE AUTHORIZATION BUDGET REQUEST FOR U.S. CYBER COMMAND

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

FISCAL YEAR 2012 NATIONAL DEFENSE AUTHORIZATION BUDGET REQUEST FOR U.S. CYBER COMMAND

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, March 16, 2011.

The subcommittee met, pursuant to call, at 3:50 p.m. in room 2212, Rayburn House Office Building, Hon. Mac Thornberry (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. THORNBERRY. As you all can tell, the votes have discombobulated the schedule. I think we are going to go ahead and get started in the interest of time.

We appreciate both of our witnesses and all our guests being here.

The first hearing of this subcommittee posed the question, What should be the role of the Department of Defense to defend the country in cyberspace? Today, we ask the same question.

The example we used at our previous hearing was, if a formation of planes or hostile-acting ships came barreling towards the Houston ship channel, I think we would have some sort of idea of what we would expect the Government to do in protecting those facilities and the Americans in them. But it is a harder question to say, if a bunch of packets come barreling through the Internet toward the same facilities, what would we expect the Government to do to defend them? Is the Government capable of doing what we expect, and is the Government authorized to do what we expect?

There seems to be virtually unanimous agreement that the threat to our country in cyberspace is growing. DNI [Director of National Intelligence] Clapper testified a few weeks ago during the worldwide threat hearing that "the threat is increasing in scope and scale, and its impact is difficult to overstate." He made a number of other statements in his testimony, something like two-thirds of U.S. firms report they have been the victim of cyberspace incidents or information breaches. Almost half of U.S. computers have been compromised, according to another survey.

Today, General Alexander—in addition to the questions I posed, today General Alexander will also give us an update on Cyber Command and its budget request for 2012 and how it is doing in accomplishing its mission of defending DOD [Department of Defense] networks.

But, as Deputy Secretary Lynn wrote in *Foreign Affairs*, "The best-laid plans for defending military networks will matter little if civilian infrastructure—which could be greatly targeted in a military conflict or held hostage and used as a bargaining chip against the U.S. Government—is not secure."

In sum, I believe that our Government and our country have not yet come to grips with the unique national security challenges that cyber poses. The changes in technology have simply outpaced the modernization of our laws, regulations, and policies. A great deal of work has been done in this area from, among others, our witnesses and the distinguished ranking member of this subcommittee, but yet we still haven't really grappled with these key issues.

For the last 8 months, Congress has waited to receive the White House's proposals on cybersecurity. We continue to hear that they may come soon. But I do note that in his July 1 letter asking for the White House proposals, Majority Leader Reid and six committee chairmen from the Senate wrote, "Each day, the threat to cyberspace—and to the American citizens, businesses, service members, critical infrastructure, and Government agencies that depend on it—only increases."

And they also said, "Securing the vast digital infrastructure of our Nation's communications networks and information systems—our cyberspace—is essential to the future of our Government, our economy, and the security of our Nation." I would submit, gentlemen, that that is the reason we are here today.

When Mr. Langevin comes, I will give him the opportunity to make whatever opening comments he would like to make. But until then, let me go ahead and yield to our distinguished witnesses for a summary of their opening statement.

Without objection, your complete statements will be made part of the record.

Today we have with us General Keith Alexander, Commander of U.S. Cyber Command and Director of the National Security Agency, and Dr. James Miller, Principal Deputy Under Secretary of Defense for Policy.

Thank you both for being with us.

And I presume, Dr. Miller, you will go first.

[The prepared statement of Mr. Thornberry can be found in the Appendix on page 31.]

Dr. MILLER. Thank you, Chairman Thornberry, members of the subcommittee, thank you for inviting me to testify.

Mr. THORNBERRY. There is a problem with our sound. We all may have to really speak up. I worry about the court reporter, whose job it is to take down every word you say. Jeff will continue to work on this problem, but if you would like to go ahead with raised voice.

STATEMENT OF DR. JAMES N. MILLER, PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY, U.S. DEPARTMENT OF DEFENSE

Dr. MILLER. Mr. Chairman and members of the subcommittee, thank you for inviting me to testify this afternoon. I am very pleased to join the CYBERCOM [U.S. Cyber Command] Com-

mander and National Security Agency Director, General Keith Alexander.

As you know, the Department of Defense is investing heavily in information technology, with $38.4 billion proposed for fiscal year 2012. We are making that investment because IT [information technology] is an enormous force multiplier for military, intelligence, and business operations. Given DOD's reliance on IT, our proposal to spend $3.2 billion for cybersecurity in fiscal year 2012, including $159 million for USCYBERCOM, makes good sense.

As I describe in my prepared statement and as the chairman alluded to, the threat to DOD and other critical networks is large and it is increasing. DOD is undertaking five key cyberspace initiatives to improve our posture, and I would like to say just a few words about each.

First, in order to properly train, organize, and equip our forces, DOD recognizes cyberspace as a domain for military activities, analogous to the maritime, air, land, and space domains. CYBERCOM, headed by General Alexander, is a key step in improving our posture.

Because we realize that cyber defense will not always succeed, all combatant commands and the services must be prepared to operate in a degraded cyber environment in which data networks are not fully reliable and access may be disrupted.

DOD's second strategic initiative is to employ new operating concepts both for cyberspace hygiene and for active cyber defenses. DOD's active cyber defenses include a perimeter defense of the dot-mil Internet domain that screens incoming traffic for malicious code and malware. And because no perimeter defense is fail-proof, DOD also hunts for intrusions on our own networks as well. We look for anomalies like viruses, worms, and other software that could cause damage to our networks and systems.

DOD's third initiative is to work closely with other U.S. Government departments and the private sector to create a national approach to cybersecurity. On September 27, 2010, Secretary Gates and Secretary of Homeland Security Napolitano signed a memorandum of agreement to allow the DHS [Department of Homeland Security] to draw on the cybersecurity capabilities already established by the National Security Agency and USCYBERCOM. A Joint Coordination Element, headed by DHS, now resides at Fort Meade and at NSA [the National Security Agency] headquarters.

A great deal of sensitive but unclassified information resides on the networks of the 2,600-plus cleared defense contractors that work with our military, and DOD is requesting $113 million over the Future Years Defense Program to upgrade this pilot to a full program. We are also exploring other pilot projects with industry that would allow DOD to further extend its suite of cybersecurity capabilities to companies in the defense industrial base.

Our fourth strategic cyberspace initiative is to build robust relationships with U.S. allies and international partners. We have already worked particularly closely with Australia, Canada, New Zealand, and the United Kingdom. And, over the last year, we have significantly expanded collaboration with NATO [the North Atlantic Treaty Organization] to implement the Alliance's emphasis on cyber defense as agreed in its new Strategic Concept.

Finally, DOD is working to ensure that we stay on the cutting edge with respect to both people and technology for cyberspace. We are taking a number of steps to recruit and retain talented civilian and military cyber personnel, including better utilizing the incredible expertise resident in the National Guard and Reserve.

On the acquisition side, it currently takes the DOD's acquisition processes 81 months, on average, to make new computing systems operational. That means by the time they are fielded, they are already three to four generations behind the state of the art. We are working to get cycles of 12 to 36 months as opposed to 7 or 8 years.

In conclusion, I want to thank the subcommittee for its focus on cyberspace. As a department, I believe we have made a lot of progress in developing our approach and in improving cybersecurity, but we have a lot of work left to do. I look forward to working with Congress and the subcommittee to improve our Nation's cyberspace posture as well.

And I look forward to your questions.

[The prepared statement of Dr. Miller can be found in the Appendix on page 35.]

Mr. THORNBERRY. I think they are trying to reset the system, and so they are all off—a fascinating thing to have happen on a cyberspace hearing. I appreciate everybody's indulgence.

General Alexander, please proceed.

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

General ALEXANDER. Chairman Thornberry, Ranking Member Langevin, distinguished members of the committee, it is an honor and a privilege to be here to testify with Dr. Miller.

Chairman Thornberry, the key points that you made, first, on where we are and where we are going, I absolutely agree 100 percent. I think you hit that correct.

Thanks for helping us build Cyber Command. I want to hit a few key points on what we have done, where we are, where we are going, and why we are at where we are today.

If you recall, a few years ago we looked at the threat. What Director Clapper said to you was absolutely right: The threat is growing every day. It is something that we have to look at from a military perspective. It is the reason we put Cyber Command at NSA, to leverage our Nation's capability in cyberspace.

You are seeing what is happening in the commercial sector, where we are having exploits going on all the time. Seventy-five percent of the population's computers have been exploited for criminal purposes. If you look at the amount of activity that is going on with new devices, the amount of e-mail and stuff, this area is exploding rapidly—tremendous opportunities and tremendous vulnerabilities.

In 2008, we had some malware, malicious software, come into our networks. When that malware hit our networks, it is what started U.S. Cyber Command, because the Secretary of Defense realized that we need to bring our defense together with other capabilities in the Nation, do that at NSA, leverage that platform.

NSA was one of the initial ones that found the problem, came up with a solution for it. And when we looked at that, that is what we need in our Nation, and that is what the military needs.

We have moved quickly in putting together Cyber Command. May 2010, we had our initial operating capability. October 2010, full operational capability for the staff. We have stood up the four components under that, and we are growing capacity. That will take some time, to build that capacity, but every day is an improvement.

We are building plans with the other combatant commands to help in cyberspace. And we are defending and operating the military networks today—a huge step forward. And we are doing that by bringing the full capability of the Defense Department and the intel community together under one roof. I can't tell you how important that is. It is huge in our capabilities.

So when you look at that, the Defense Department has a tremendous jump forward in what we are doing and how we are doing it. And the ability and agility to move quickly between operations in defense when events like what has happened in Japan to our networks, we can quickly accommodate, whether it is a natural disaster or a manmade disaster. I think that is a huge step forward.

So I wanted to leave time for questions, and I know we have been asked to go quickly. But there are a few things I would like to hit that Secretary Lynn hit in the article that you referenced. He mentioned five key areas about cyberspace; it is a domain analogous to air, land, sea, and space. He talked about the active defense, he talked about critical infrastructure, he talked about partnering with our allies, and he talked about leveraging technology.

Two of those are key—they are all key, of course—but two of those are key for this discussion, and that is, how are we going to defend? And the active defense is what we did in leveraging what NSA can do with what the Defense Department is doing.

And, from my perspective, that is key. How are we going to hunt in our networks? How do we provide a capability that goes beyond what you can commercially buy, by leveraging our intelligence community and our military capabilities to help expand our defense? How do you leverage that global cryptologic platform as an early warning capability? It is those kinds of things that we have to look at.

And, finally, when we prove that that is good for the military networks, I think he made a great point that resonates with what you said: How do we then extend that, lawfully, while protecting civil liberties and security, to the rest of Government and critical infrastructure? And, of course, doing that right, that is what is taking time, that is what everyone is working on. I think that is a huge step forward.

I will tell you that one of the things that, from my perspective, is so important in this area—you know, our Nation built the Internet. We are the ones that developed this, the iPad and many of the devices that we have. We are an innovation nation; we are the ones who came up with that. It seems to me, we are the ones that ought to solve this security problem. And we can. And it is going to take a partnership between us and industry. It is something that we

ought to work together. And we can do this; we just need to drive through it.

Mr. Chairman, that is all I have.

[The prepared statement of General Alexander can be found in the Appendix on page 48.]

Mr. THORNBERRY. Thank you. I appreciate your comments.

Let me yield to the ranking member for any comments he would like to make. And if he wants to go ahead and do his questions right after that. I yield to him.

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Mr. Chairman, first of all, for calling this very important subcommittee hearing.

I want to thank Dr. Miller and General Alexander for being here today. I want to welcome you.

And, in particular, General, I want to just take a moment to commend you on the successful stand-up of your new command over the past months.

And I want to thank you both for appearing today to discuss what I believe is one of the most important missions and national security issues facing our Nation today.

It is difficult to fully appreciate the importance of cybersecurity issues to our national security. From day-to-day tasks to critical operations, our warfighters depend on the integrity of our networks.

At the same time, cyberspace itself has become weaponized. The STUXNET virus as well as massive denial-of-service attacks successfully targeting our allies in Georgia and Estonia have given us a glimpse of the damage cyber-weapons can cause.

In some ways, thinking about conflict in cyberspace reminds us of some warfighting basics. The principles of offense and defense appear to remain largely the same, but the speed of information is so fast that complexity increases exponentially. Also, unlike the land, sea, or air, this virtual, manmade domain is limitless.

I believe that we must better understand how the United States should safeguard our critical networks, while at the same time developing the full spectrum of cyber tools to deal with conflict in a new environment.

General Alexander, last September, when you appeared before the Armed Services Committee, I asked you about your role in defending critical infrastructure from cyber attack that may reside in other parts of the Government or in private hands. You noted that your role as head of USCYBERCOM was to protect only military networks. And that is within your authority, and it, for the most part, is limited there.

At an Emerging Threats Subcommittee hearing later that day with the chiefs of our Services' cyber components, I revisited your answer and asked what they were doing to protect military bases that solely rely on civilian critical infrastructure. Their answers, unfortunately, were grim but not unexpected. For example, Vice Admiral Barry McCullough, head of the Navy's 10th Fleet, testified that, and I quote, "These systems are very vulnerable to attack," end quote, noting that much of the power and water systems for

our military bases are served by single sources that have only very limited backup capabilities.

With an attack like the one demonstrated by Idaho National Labs in their Aurora experiment on a power station, potentially requiring weeks or months to recover from, our bases could face serious problems maintaining operational status. Beyond even the massive damage to our economy and civilian institutions that a major attack on our critical infrastructure could have, clearly this is a vital military concern, as well.

Today, I reintroduced language, which the House passed in our National Defense Authorization Act last year, which would enable the White House to better coordinate our Federal cyber defenses and secure our critical infrastructure. I believe it is essential that we continue to make progress in managing this threat.

Although we have not yet faced a catastrophic cyber attack—and that is very fortunate—I do recognize that every day we see lower-level intrusions and thefts of everything from sensitive defense information to information on our financial system and critical infrastructure, as suggested in numerous press reports. While I am certainly thankful that we have so far been spared a major attack, the low level of these incidents has in some ways hindered our ability to move forward on solving this issue.

As the commander of CYBERCOM and the director of the National Security Agency, General, you direct our Nation's most powerful capabilities in the cyber realm. And I know, from speaking with you, that you also share my concerns that we have not yet fully seen the extent of the damage that cyber-weapons can wreak.

I know that defending against a collapse of our financial system or a meltdown of our power grid is outside the scope of the Department of Defense's responsibilities, in many ways, but if done intentionally, it would still amount to an act of war.

Today, I look forward to discussing and hearing further about how Cyber Command is growing and how your component commands are coming on line. I also look forward to hearing how the Administration is developing an overarching approach to cybersecurity and how DOD's role may need to evolve.

Most of all, I hope to understand what the Administration plans to do to fill the gap between these growing threats and our ability in the public and private sectors to manage them. What authorities should we examine and what tools can the Government develop to increase our ability on a national level to meet these challenges?

Again, I want to thank you both for being here today. I appreciate your testimony, and I look forward to our question-and-answer period. Thank you.

Mr. Chairman, with that, I will yield back to you, unless you want me to go into my questions.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 33.]

Mr. THORNBERRY. I think if the gentleman wants to proceed with his questions, we will operate under the 5-minute rule.

Mr. LANGEVIN. Thank you, Mr. Chairman.

General, if I could, perhaps I would begin with you.

It is clear that if enemy bombers were heading to the United States and we had actionable intelligence that they were clearly

targeting critical infrastructure within our Nation, that the Air Force and other components of the military would take them down. And it is clearly the responsibility of DOD to stop that attack.

If there were an attack in cyberspace, an attack on the SCADA [Supervisory Control and Data Acquisition] system, with the clear intention of taking down sectors of our electric grid, do you have the authority to stop that attack? And, if not, who does?

General ALEXANDER. We do not have the authority to stop that attack. And on the critical infrastructure, I think that would fall to DHS. DHS has some of the authority, and I think extending that to critical infrastructure is something that the Government is addressing in the White House-led legislative proposals to ensure that we encompass that.

Right?

Dr. MILLER. That is right.

Mr. LANGEVIN. General, then, let me ask you this: How do you think CYBERCOM should work with other Government agencies and the private sector to leverage the powerful capabilities that you possess for the protection of networks and infrastructure not specifically within the dot-mil domain? In particular—well, let me stop there, and I will come back if I need to.

General ALEXANDER. To answer that question, I am going to give you two, Congressman, two pieces of that, break it out into components.

First, for Cyber Command, technically there are two things that we can do, the Defense Department and the intel community, Cyber Command. It is, we can provide malicious software signatures to help protect that, and early warning. So those are the two capabilities.

The issue that you raise is, so how do we go about doing that, the roles and responsibilities between the Defense Department, DHS, and the intel community? And I think that is where the partnership that Secretary Gates and Secretary Napolitano addressed, and their initial memorandum of agreement in September 2010 is focused on addressing that. We have to bring those two departments together. I think both Secretaries see that.

And the intent of that memorandum of agreement is a first step in how we leverage the capabilities that NSA has to help DHS. So I think that is a step in the right direction.

Mr. LANGEVIN. General, we know that the Tutelage program is designed to provide perimeter defense to the dot-mil network. What is the best way to extend similar protection to the dot-gov network? And who does that? How do we do it?

General ALEXANDER. I believe the best way is to take that capability and work with industry to do that in a manner similar to what we are trying in the Defense Industrial Base Pilot with DHS and the Defense Department.

In that pilot, the Department of Homeland Security and the Defense Department are working with the Tier 1 Internet service providers to provide that technical capability to them, along with some of the signatures and stuff, to defend a couple of defense industrial base companies. About 30 of them I think is what it will end up being. And it is showing that you can do that, that it scales across

that level. We will demonstrate that with a few of the capabilities that we have.

I think concurrent with that, as we are doing that, we have to look at the authorities and legislation to do the rest: What is required, and how do we quickly move to do that? Technically, we can do that very quickly. We want to make sure that we then have the authorities to do that, as well. And the pilot would show that we can do that.

Mr. LANGEVIN. And so then you have touched on, perhaps, taking the next step. Then, also, what is the best way to defend the dot-com network, particularly on critical infrastructure? So much of it is owned and operated in private hands. How do we then take that to the next step? And where do those responsibilities and authorities lie?

General ALEXANDER. From a technical perspective, the easiest way to do that is to partner with the Tier 1 Internet service providers. Government traffic and critical infrastructure traffic can be segregated in those areas and protected by those companies easiest. And our ability to work with them in a classified environment to ensure they have the signatures and stuff is probably the technically quickest way to go and the best way to go. It scales, and it shows it. And that is what the pilot would do.

If we can do it for the Government, the way the Government is spread out, that would scale also to critical infrastructure if we deemed it necessary to do those, as well.

Mr. LANGEVIN. Very good.

I see my time has expired. I have other questions, but thank you for your answers. And I will yield back at this time.

Mr. THORNBERRY. I thank the gentleman.

Dr. Miller, let me, just to be clear, ask you: Do you agree with Secretary Lynn's comments that the best-laid plans for defending military networks will matter little if civilian infrastructure is not secure?

Dr. MILLER. Yes, sir, I do.

Mr. THORNBERRY. And my understanding, from the exchange from Mr. Langevin and General Alexander, is that, currently, Cyber Command does not have authority to make civilian networks secure.

Dr. MILLER. That is correct. CYBERCOM's mission is to provide the connectivity and oversight of our networks and to protect them and to be prepared to conduct full-spectrum cyberspace operations as directed by the President and Secretary of Defense.

The National Security Agency, as you know, has provided technical assistance to our interagency partners, in particular working with the Department of Homeland Security. And the cyber pilot program that General Alexander talked about is a great example of that. We think we need to do more of that and to move forward as quickly as possible.

Mr. THORNBERRY. Well, that gets me to the next question. In the same article, Deputy Secretary Lynn said that the Pentagon was working with Homeland Security and the private sector to look for innovative ways to use the military's cyber defense capabilities to protect the defense industry, as a start.

So what are some of those innovative ways?

Dr. MILLER. Sir, the principal one that we are focused on now in bringing the innovation and new technologies to them is to look at the application of the systems that you referred to earlier and that General Alexander spoke about to help on perimeter defense. That is working with the ISPs [Internet service providers], as General Alexander noted.

The other side of it, just like for DOD, we need to think about the cyber hygiene and what we can do internally. We need to think about how to hunt on our own networks and look for the problems that may already exist. And we need to work on that perimeter defense. I think all of those apply, as well, to dot-gov, to the rest of the Government. And all those principles apply, as well, to the critical infrastructure in particular, the 18 designated areas of critical infrastructure.

And so, as we look at what can be done to improve the posture from where we are today, the legislative proposals that the Administration is considering could span all of those: What are the incentives and assistance that can be provided for cyber hygiene, for example, as well as for the active defense?

Mr. THORNBERRY. Yeah. Well, as I say, we are anxiously awaiting those.

Last question: General Alexander, are you convinced that you can share some of this sensitive information to help provide greater perimeter defense and protect national security at the same time?

General ALEXANDER. Mr. Chairman, I am convinced that the Internet service providers can protect sensitive information.

Mr. THORNBERRY. Okay.

Let me yield at this point to Mr. Kline.

Mr. KLINE. Thank you. Thank you, Mr. Chairman.

And thank you, gentlemen, for being here, for your testimony.

I find myself still scratching my head over the same issues that we have heard discussed here, and that is, how do you even make a distinction between an attack on defense and keep it separate from an attack on something that is directly related to defense? A critical infrastructure question. Clearly, if you shut down the financial system in the United States, it would affect defense, it would affect everything.

So I want to make sure I am clear on two things. One, I understand we are all anticipating this prospective legislation—although I must say, we have way too much experience in this committee with legislation, putting things into law, directing the Department of Defense to do stuff, and then the Department of Defense just deciding not to do it, frankly.

We have put in law, for example, Mr. Thornberry and I worked very hard a couple of years ago on the NDAA [National Defense Authorization Act] directing the Secretary of Defense and the DNI to come up with a charter for the National Reconnaissance Office. It is a year and a half late now. It has been in law, but we haven't seen the results. And I know people are working. In fact, we have had interim reports.

So while I am delighted that there is prospective legislation, I am just suggesting that might not be the whole answer. I trust, General and Mr. Secretary, that you are working on how to fight this in any case, despite the legislation.

I want to see if I understand this. I am looking at the mission of USCYBERCOM as stated here in front of me: Plan, coordinate, and so forth. And it says, "and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace, and deny the same to our adversaries."

So, if directed, then you would step in and provide defense, active or passive, in the event of an attack on infrastructure? Is that correct or not correct?

General ALEXANDER. Well, that is correct as you stated. Let me just give you, if I could, Congressman, a couple points on that.

What that really drives to is—as part of my confirmation hearing, Senator Levin asked a very similar question, which was, so what does that mean? And the specifics of it are: If we are overseas in an area of hostilities, Cyber Command would be operating under Title 10 authorities——

Mr. KLINE. Uh-huh.

General ALEXANDER [continuing]. And we would be taking on the adversary, and we would have the authority to operate in cyberspace in that case.

The issue becomes a little bit more difficult when you start looking at cyberspace as a global capability and bouncing through neutral countries. Now what are the authorities of land warfare? What are the laws and what are the policies on it? You have the inherent right of self-defense, but what can you do to stop somebody in a neutral country? And in cyberspace it is easy to jump through neutral countries to attack someone. And the third and the most difficult is what happens if they use the United States infrastructure to attack the United States? How do you do that? All of those are key things.

For us to operate overseas, it is an execute order from the Secretary of Defense and the President. And that is what that specifically lays out. And that execute order gives us the authority to operate under those conditions and defines those conditions for us.

Mr. KLINE. What about if it is not overseas, which is kind of an antiquated, bizarre concept when we are talking about cyberspace, but what if it is not overseas? Is there a "when directed" still possible here?

General ALEXANDER. That is correct. There is a "when directed." And that is——

Mr. KLINE. And by whom?

General ALEXANDER. It would be by the Secretary of Defense and the President.

Mr. KLINE. Okay.

I have just about run out of time, but very quickly, there are a number of issues about getting adequately trained personnel in high-technical areas. It is true in space, and I would think it would be true in cyberspace.

And so, are you having difficulties or is there anything we could do that would help you recruit and retain people who can actually take on this task?

General ALEXANDER. There are some things, Congressman, that I think we will need to work jointly. And that is, like we do, proficiency pay for linguists and others, what is it that we need for

our cyber personnel? We are going out to hire, the services are. Right now, that is not an issue. But the services are discussing that type of pay for those to get it. We do want to create a force.

I think the other thing that we are looking at is how do we collapse some of our military occupational specialties down into a few that allow us to look at the full spectrum: Defend, operate, all the way through. I think we need to do that, and the Services have been wonderful in setting that up. And the way that we would define that is by looking at how we are going to operate in those foreign areas, how do we need our forces to be developed.

This is a very technical area. There is discussion, and we will evolve how this command works, I think, over the next few years. We have had great success, on the NSA side, of hiring a highly talented workforce and keeping them. Our retention is amongst the best in Government. So I think we can do the same in cyberspace. And I think we will get a lot of people that want to take this mission on.

Mr. KLINE. Okay. Thank you. I trust you will let us know if you need legislative assistance.

I yield back. Thank you.

Mr. THORNBERRY. Mr. Gibson.

Mr. GIBSON. Thanks, Mr. Chairman.

And I thank the distinguished panelists here today. I thank them not only for their testimony, which has been illuminating, but also for their leadership in this key area. And as we proceed, you know, given classification issues, if we start to move into an area, I assume that you will make it clear to me.

But I am interested in probing a little bit further the issue of unity of effort. And I have a question both on the governmental side, the whole Government side, and then also on the private side. I think I will start with the private side; it looks to be simpler.

Do we have a list of instructions for individuals, what to do if they sense they are under some kind of cyber attack, similar to our SAEDA [Subversion and Espionage Directed Against the Army] instructions of how to report, that we pass out to infrastructure or proliferate in any way?

Dr. MILLER. This is outside the scope of the Department of Defense responsibilities. What we have is a—as a Government, working together on a National Cyber Incident Response Plan, part of that is to clarify what those activities and responses would be. I think it is fair to say we have some more work to do there. And I would be happy to respond for the record with more details.

[The information referred to can be found in the Appendix on page 71.]

General ALEXANDER. Could I add, Congressman, a couple things on that? And I did throw that over on Dr. Miller, because I think the first part is, it is really, how do we train our teams to hunt and operate within our systems? So system administrators today need to evolve to people who can police networks tomorrow.

And when they do that, part of the training that we give our red, our blue, and some of our what we call green teams is just what you are talking about. That has to be a continuous process, not something that happens once every 2 years. So how do we evolve

that force will be a key part of the defense, and that is part of that active defense that I referred to.

Mr. GIBSON. Yeah. Very good. And I think you would appreciate that standardized reporting format would probably be helpful as we go forward.

And then, related—now we are in the governmental realm—I am trying to get a sense of—and I can imagine the challenge that you have, trying to coordinate this effort toward unity of effort.

So is this event-driven, or is it battle rhythm-driven? Is there a working group that meets across the intelligence communities, the DHS and the DOD? How do you go about coordinating your effort now, given the challenges that you have?

General ALEXANDER. Sir, we do have meetings, especially in the area—let me focus just a little bit more into looking at malicious software, tactics, techniques, and procedures, people that are trying to get into the networks. We do have meetings both within the Government that looks at this—so the Computer Emergency Response Teams at DHS, within DOD and across the Government work that.

Private industry, selected parts of those, also participate in that at times, because they have some expertise. And going back and forth on those is key. And the reason private industry is brought in is, some of the signatures for the antivirus community that private industry creates helps protect Government systems. And we want to ensure that that is done right and that they have the full advantage of that.

Mr. GIBSON. Thanks very much.

Chairman, I yield back.

Mr. THORNBERRY. Mr. West.

Mr. WEST. Thank you, Mr. Chairman and Mr. Ranking Member.

And, sirs, it is a pleasure and honor to see you all here today.

Four elements of national power, the DIME [Diplomatic, Information, Military and Economic] theory, and, of course, the "I" stands for "information." So I think it is very important that we recognize that aspect here on this modern battlefield. And we, you know, congratulate you on standing up the CYBERCOM.

But this is one of my big concerns: You know, what can we do to combat the proliferation of Islamic terrorism propaganda on the Internet? Because I see this as just another weapon on this modern-day battlefield. And if we are serious about this global war on terror, this propaganda is truly a tool or a weapon that they are levying against us.

Now, does that fall under CYBERCOM's purview? And, if not, who is contending or dealing with that?

General ALEXANDER. I think that is a policy issue, in terms of whether we choose to stem the flow of radical propaganda and how. Technically, Cyber Command could be one of the agencies given that mission to go do. We have not been given that mission, under either a CT [counterterrorism] or a CYBERCOM authority.

So I think the question is, one, has a decision been made to do just that? And, to my knowledge, there is no decision to block the radical propaganda on the networks. If it was, then it could technically go to either Cyber Command or one of the other agencies.

Mr. WEST. So who makes the decision?

General ALEXANDER. That would be the White House and the Principals Committee.

Dr. MILLER. That would be a decision at the level of the President and, as the general said, of the Cabinet, as well.

There is no question that this Administration, as past administrations, are working to counter the ideology that you spoke about. The Internet has an important role in that, in terms of how we get our message out. And, obviously, it is part of how these groups have used—you know, it is something that these groups have used, as well.

But you have put your finger on a central policy question that remains, essentially, open.

Mr. WEST. Well, my fear is that the longer it remains open, the more we get exploited and the more we get infiltrated across this country. So at what point in time are we going to tackle this question?

Dr. MILLER. The authorities for dealing with that are not principally Department of Defense authorities.

General ALEXANDER. And there is one other thing, Congressman, if I could, on this, just to add on that.

If we see this on U.S. infrastructure and it is wrong, we can reach out, through the FBI [Federal Bureau of Investigation], and ask that that be removed. And we have a high success rate in getting that done. So when we see things that are particularly wrong, we reach out. And all the companies, when they see that, they take it off, both here and global.

Mr. WEST. Okay.

General ALEXANDER. And so, there is a way of doing that when we see those. So I didn't want you to think—the way I answered it is, we are not reaching out and causing it to be removed globally. We can reach out and ask that it be removed globally. And we are having a pretty good success at doing that.

Dr. MILLER. And if I could just add very briefly, the "D" in your DIME model, sir, the diplomatic effort is absolutely important.

Mr. WEST. Absolutely.

Dr. MILLER. And that is something that this Administration has obviously pursued.

Mr. WEST. Okay. I got it, but, you know, we are getting our butts handed to us on that means. And when I think about Major Hasan and some of the things that he was able to utilize the Internet for, you know, I don't want to see a repeat of those type of circumstances.

So thank you very much, and I yield back.

Mr. THORNBERRY. I thank the gentleman. And as I am sure he knows, there is a number of folks who have served in-theater who share his frustration, who think there is a lot more we could be doing but are not doing. And I am very sympathetic with that view, as well.

General Alexander, let me follow up on what Mr. Kline was asking about on people. And I know you said you would get back to us on additional authorities. And you said you have a great record of retaining people at NSA. But those are not necessarily military folks who may go through basic training and all the rest.

Can you get and keep the kind of people you need for CYBERCOM with the military requirements? Or does there have to be some greater flexibility than we are used to?

General ALEXANDER. Well, I am an optimist, Chairman. I think we can, one, get them. I do think it may require more authorities, but we have to look at that.

And, more importantly, I would like to put forward this thought: We want NSA to have one certain level, technical level of expertise that Cyber Command can use. And we want Cyber Command to have a breadth and a deployment capability.

And so, these two have to work together. And I think we can do both. I think we can get the service people on one side. That may require some additional authorities. We have to look at it and come back to you. And I think we want the NSA infrastructure to have this technical depth that we can rely on back and forth. I think that is absolutely vital.

Dr. MILLER. I would just briefly add that we owe a report on this issue, Section, I think, 934 of the National Defense Authorization Act.

And in addition to the factors that the general talked about, I think we need to look hard at what we can do under existing authorities, including making better use of the Guard and Reserve. That is an essential part of what we need to do.

The type of people that we are looking for will span a wider range than the profile of people that we—the type of people that we are looking for with the skills for cyber will span a wider range than the standard profile for military service. And we need to have a higher degree of flexibility and continue to look to target those groups and to work on some of the pilot programs we have under way now, to work with them and to have outreach, so they see what DOD can provide for their education and see that they can make a contribution to national security, as well.

Mr. THORNBERRY. Well, we want to work with you. You made an impression on me in your written statement, General, where you said this was the thing you were most concerned about, or however you phrased it.

But, please, go ahead.

General ALEXANDER. I was going to add that—I hate to give the Navy all the credit here, with him sitting right behind me—but the Navy Postgraduate School has also started a master's degree course in January that will produce a master's in cyber that is a technical degree, either in computer science or EE [electrical engineering], with the majority of the courses being in cyber- and cybersecurity-related things.

So that is a step in the right direction and some of the things that we need to do more of.

Mr. THORNBERRY. Okay.

Dr. Miller, one hears—and maybe one of you all mentioned it in your written testimony, back to the authorities issues—about the military's ability to provide support to civilian authorities when called upon to do so. How does that fit in a cyber context?

Dr. MILLER. Sir, let me talk about both sides of that, if I can.

The first, as we were discussing earlier, is that the Department does recognize that we are dependent on both our partners in Gov-

ernment, so the dot-gov, and our partners in the industry to be able to conduct just military operations and to succeed in those operations so that we have a stake, in addition to the stake we have in the broader security of the Nation, we have a stake in just our ability to operate, itself.

The Department of Defense, as you alluded to, has authorities to provide defense support to civilian authorities under existing law. And the challenge associated with that in this area is that it gives a good set of authorities for responding to an incident. And what is not so clear is that it gives the appropriate set of authorities to assist in prevention of attack in the first place.

And as we have looked at possible legislation, we are looking at what additional authorities may be required for the Department of Homeland Security so that it can provide that degree of protection, and then what set of authorities may be necessary or changes may be necessary for the Department of Defense to assist in providing that prevention, as opposed to solely focusing on response.

You have asked exactly the right question. We intend to address it in legislation. And we understand that there are legitimate concerns about imposing costs on private industry, and we need to think through that. But we also understand that, as we have discussed earlier, that we have a lot of catching up to do.

Mr. THORNBERRY. Yeah. Well, and as your answer recognizes, response after the fact to a cyber event is not really a very good answer to the challenges we face there.

So, let me just ask about a couple more things, and then I will yield to the ranking member and Mr. Gibson, if they have other questions.

Again, I can't remember exactly which of you talked about this. But there were two efforts under way: One is the Enduring Security Framework, and the other is the Defense Industrial Base Pilot.

Could either or both of you all expand a little on what those are and where we are with them?

General ALEXANDER. The Enduring Security Framework is a partnership between Government with DHS, DOD, the DNI, and industry to look at critical cybersecurity issues throughout the different components from communications devices, computers, and others.

I think that is a great partnership between the Government and industry in identifying problems and solutions to those problems. If we can identify those problems, it has been our experience that industry, in developing much of that equipment, will go solve those, free to the Government.

That is a huge step forward, and we have made some tremendous jumps in that area. I think industry has more than done their share. It has been a privilege and honor to work on that. That has been great.

The Defense Industrial Base Pilot takes the technology that we have within the Department and uses some of that with some of the Tier 1 Internet service providers to test and ensure that that would work under the concept that I discussed earlier, where the Tier 1 Internet providers ensure that we can do what we are doing now for the Defense Department for these defense industrial base companies.

Once we have done that, the key is now identifying the authorities and ensure that we have the authorities to do the rest of it. So we are only going to do a few narrow things under the DIB [Defense Industrial Base] Pilot, a few narrow activities. Once we have shown that we can do those, the rest of those activities will be added.

We will have to ensure that we have the legal framework for that and everybody agrees with that for the rest of those. And that may be parts of the stuff that come forward from the White House on the legislative proposals that we have.

Dr. MILLER. And, sir, if I could add very briefly, the Enduring Security Framework, we have found that the industry that participate help both on helping us understand the problem and working the solution. And that is, as the general said, very important.

I want to distinguish, as we talk about the DIB Pilot, there are really two things under way. One is a broad Defense Industrial Base Pilot, in which we are sharing information about potential threats and looking at how to do that more effectively. It has been a two-way street. It has been very effective. And we are looking to continue that and grow that.

It has been focused primarily on the cyber-hygiene side, if you will, on defending the networks better. The new element that the general has been referring to has been added to that, and we are currently examining how to implement that. We have called that, for shorthand, the Opt-In Pilot because companies would opt in to participate on that. And as the general said, we are working with a number of defense industrial base companies and several Internet service providers. That has not yet kicked off. It is something that I hope that we are very close to initiating.

And by way of analog, it is looking for part of the dot-com to bring what Einstein 3 is supposed to bring to that dot-gov. And, as General Alexander said, it is not the full suite, but we are looking at a way to get started and show that we can do this and to make it work.

Mr. THORNBERRY. And about how long would it take, do you think, to prove that it can work?

Dr. MILLER. About 90 days we are looking at to execute this pilot.

Mr. THORNBERRY. Okay, good. Thank you.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

General Alexander, CYBERCOM has maybe two, maybe, primary missions among several, but two primary missions: First, to ensure that our military networks stay online, and, also, to support our warfighters in their missions around the world.

We talked before about the network defense side of the issue, but I would like to turn to the second side, if I could, of support to the warfighter. You rightly recognize that cyberspace is a new domain, similar to land, air, sea, and space. How do you make sure that cyber is treated equally and not just as a supporting entity?

Can you outline the command structure for integrating nonkinetic cyber effects into both tactical and operational levels of a conflict? And beyond the use of cyber domain, how are cyber mission areas different from the electronic warfare mission areas?

General ALEXANDER. Well, let me start with the first one, and then I will come back to electronic warfare, if I could.

On the first one, our staff is organized like the rest of the COCOM staffs, the combatant commander staffs, with the J3, J5, J2, J6, et cetera. Our planning folks reach out to the combatant commands, and we are working with those combatant commands on their plans to integrate cyber into those plans from both a defense and a full-spectrum capability.

My experience to date is that the commands have jumped on this. Every one of them has been eager and helpful to do that. I am extremely pleased that they are rolling this into the full spectrum. They realize the importance of it, both to defending our capabilities and extending those out.

If you were to make bubbles on the role of cyber and electronic warfare, they are going to touch together, electronic warfare predominantly being looked at primarily today, if you will, for jamming radars back and forth. I mean, that is the way we look at it, in physical space by radio waves. In cyber, we are acting within networks.

You can picture a time in the future where those two may come together, and it may be that the Department begins to bring some of that together, from both a technical perspective and an operational perspective. We are not there today because the way we build our EW [electronic warfare] capabilities is separate and apart, as part of the defensive systems of aircraft and other things like that.

I did go to school in some of that, so I do understand those parts. And I think you can see them coming together as the digital technology matures.

Mr. LANGEVIN. Thank you. Anything else in the area of electronic warfare that you want to get into?

General ALEXANDER. Not that I can think of, Congressman.

Mr. LANGEVIN. Okay.

Dr. Miller, and also to you, General, in addition to the $159 million provided in the President's fiscal year 2012 budget to support CYBERCOM, what other costs are associated with cyber operations across the Department for fiscal year 2012? To what extent will DOD's current efficiency and cost-saving efforts impact CYBERCOM's current and future cybersecurity funding, if at all? And to what extent is DOD taking steps to ensure that CYBERCOM and associated military components are organizing in a manner that prevents or minimizes duplication?

Dr. MILLER. Sir, let me first say, glad to provide for the record the breakdown of the costs in more detail than I did in my prepared statement. What I could do is refer to a $3.2 billion total for cybersecurity and the $159 million associated with USCYBERCOM.

The other—the largest single category is information assurance, which includes our public key infrastructure and key management initiative. That is at a little over $2 billion for fiscal year 2012.

Rather than go through each of the other categories, I would just, I guess, add, we have noted the importance of science and technology, and about $258 million of that is in the S&T realm. We will provide the rest of those, if you like, for the record.

As we look at the work on efficiencies and the importance of both saving money and improving security—I will turn it over to General Alexander—one of the most innovative and interesting ideas and concepts for how to pursue those in tandem is to look at how we can move to a cloud-based architecture in a way that improves security.

If we do it the wrong way, it could increase our cybersecurity challenges. If we do it appropriately over time and move to virtualization of some of the, if you will, interior of the architecture, we will have the ability to present a much more challenging target to those who want to attack us.

I think General Alexander can speak in much more detail than I can to that issue.

General ALEXANDER. Congressman, let me answer two parts of that, taking off from what Dr. Miller said.

First, on the IT efficiencies, one of the things that we looked at: What was the best way that we could help secure the Defense Department's networks, given the vast topology of those networks? And it was our opinion that the best way was to go to a thin cloud, virtual cloud environment, analogous to the way that Google, AT&T, and others are doing, but do that for the Defense Department.

As we looked at that, we also believe that we can do that more efficiently in terms of manpower and moneys. That is yet to be proven, but it does give us a much more defensible way.

So the IT efficiencies is something that Secretary Gates has pushed out that we are looking at how can we now help do that. And what our intent is, if we can do this right, we can now take part of the workforce that we have in IT and train them to be full-spectrum cyber capability. That is something that, working with the service, will help build the capacity quicker, that I mentioned is that shortfall.

So I think that is one of the things that we are looking at. We have discussed it with the service chiefs. That is something that we have to walk through. The service components are looking at it. That is a huge step. Now, to get there, NSA is actually testing out parts of that right now in our infrastructure, and we will prove that that is right.

The other thing, that duplication of effort, I would just tell you that that is one of the things, as a CYBERCOM commander, that I take very seriously. How do we ensure that the services are doing this as a joint team versus each one of them doing the same tool four times?

We have great cooperation with the services in doing that. Our components said, we are bringing all of that together. Our J3 and J5 will take that on. Our suite of tools will be looked at and scrubbed in that way. And we have already started that with our planning process.

Mr. LANGEVIN. Very good.

With that, gentlemen, thank you very much for your testimony. I know that this is an enormous challenge that we all face in cyberspace, and I just appreciate your dedication and the work you are doing.

Thank you.

Mr. THORNBERRY. Mr. Gibson.

Mr. GIBSON. Thanks, Mr. Chairman.

And, really, just a summary of what I am taking away from the hearing and from also reviewing the written testimony, I think Cyber Command is doing a tremendous job in gaining situational awareness, getting organized, trying to get their arms around the threat and to take concerted action.

But, to a degree, our country is hampered, the effort toward unity of effort—that we need mission clarity, authorities, legal framework, and organizational design. And what strikes me is that these are similar findings to the QDR [Quadrennial Defense Review] independent panel and the need towards looking at both congressional, organizational reform so that we can facilitate better, legislate better, and provide better oversight, and then also executive reform, executive branch reform, so that the DOD can get the guidance it needs to move forward.

So these are areas of interest to me, Mr. Chairman. And I look forward to—I appreciate you calling this hearing and the testimony from our expert witnesses here. And I look forward to working with you as we go forward.

I yield back.

Mr. THORNBERRY. I thank the gentleman.

The areas he identified are also of interest to me, as he knows, so I want to pursue it along with the gentleman.

General Alexander, following up on your conversation with Mr. Langevin, do you have the authority you need, as CYBERCOM commander, to eliminate duplication in the services?

General ALEXANDER. I believe I have all the authority I need to eliminate duplication with the services. More importantly, I have their support in doing it. They want to do this. It makes sense. Nobody is pushing back. The key is finding all of that for all of us, because there is a lot of ingenuity that goes on.

To date, I have not found anyone that has pushed back on that. I believe that, through both the Joint Staff and the JROC [Joint Requirements Oversight Council] process, we can push that. And through the Deputy Secretary and the policy level, we will get all the support we need. I don't see any issues with that. It is more of just making sure that they surface.

Mr. THORNBERRY. I am always concerned when something becomes a very, you know, high-priority issue, then all sorts of programs have that label put on them to take advantage of the budgetary things that go with it. And ferreting out what is real and needed versus what may be an effort to gain more of the defense pie is an important capability, I think, for you to have.

Can you talk a little more generally, though, about budget? Obviously, we are going to be in a limited budget for the Government, for the Defense Department for some years to come.

As we think about cyber and spending money, you know, it doesn't cost very much money to send an electron through a fiberglass pipe. But where is our money going to have to go in order to defend the country properly? I mean, I assume people has got to be number one.

But can you elaborate, not just on this year's budget, but on those trends over the next several years and what you see the most growth in when it comes to cyber?

General ALEXANDER. Chairman, I think you hit it on the head. People is the big thing here in cyber and for our future. Investing in people is key.

We are building capacity. And, as you correctly noted, that is one of the key things that we have to go build and go work, and the Services are helping us do that. In my budget, both the military and the civilian side, that is the biggest portion of the budget—people.

The next is facilities to operate in, the IT infrastructure that we need to operate. That accounts for another 25 percent of the budget. And operations is the last part. So, if you break it out, people is the biggest share of the budget.

One of the things that I would just highlight is we did look at building an integrated cyber center that brings together all the different elements that we have within the Department, all the different centers within our Department and potentially across the Government into one facility that allows us to operate seamlessly from peace time to crisis, back and forth. I think that is huge, and in this budget here is the planning and development of that facility.

Dr. MILLER. Sir, if I could add very briefly, for overall IT, the request for fiscal year 2011 was $36.6 billion, for 2012 was $38.4 billion. We actually hope that that number will come down over time, as we move to a different architecture and be able to make some savings there.

For overall expenditures relating to cybersecurity, the numbers, in fiscal year 2010 the number was about $2.96 billion, 2011 request was $3.2 billion or a little under, and for 2012 we are a little over $3.2 billion.

So we have increased somewhat. Particularly, I think, we are focusing those resources better, as we look to, for example, increase substantially how much we hunt on our own networks and so forth. But we would be happy to provide the next level of granularity, if you like. I am afraid that if I did it real-time, you would, you know——

Mr. THORNBERRY. Yeah. The staff could take it, but I am not sure that I could. But it is, I think, helpful for us to see the longer-term trends, because I think we are all going to be challenged in that regard.

Dr. Miller, one thing we really haven't touched on too much today is the whole subject of international cooperation in getting any of this done. We have talked about how geography doesn't matter very much in cyber, but can you just briefly touch on the international aspect of this?

Dr. MILLER. Sir, I would be very glad to.

As I had talked about before, working with our international allies and partners is one of the key five initiatives that we have under way as part of our strategy. So we recognize its importance. And we recognize that, because we operate in fighting the coalition, that the security of our information, the security of our operations

is also going to be dependent on the security of our partners' and allies' networks, as well.

As we have begun really pushing out on cybersecurity efforts internationally, the first focus—I should put that differently—a very significant focus has been on working with our allies, Great Britain, Australia, New Zealand, and Canada. We have long-standing relationships with them on intelligence issues, and that has been a good foundation for what we do in cyber, as well.

A very significant effort over the last year with NATO. And having cybersecurity being one of the key thrusts of the NATO Strategic Concept that was brought forward at the Lisbon summit, I think, is a good accomplishment. The cybersecurity center that has been established has begun to operate, and we have a lot more work to do there in NATO, in terms of implementing that effort.

We have also worked with other partners and allies around the globe, including, for example, the Republic of Korea and Japan, and are beginning to have, I think, useful conversations there.

One of the other areas, sir, that I just want to add is that we need also to have conversations about cyber and other strategic issues with Russia and with China. I think we have made some headway with respect to Russia and having the initial conversations on cybersecurity. Our lead on this for the national security staff, Howard Schmidt, took a team there just a little over a month ago to have this—to begin this conversation. And so far, with China, we have not yet really been able to have the same level of conversation.

I think transparency and understanding about how each of us approaches this challenge is very important to avoid any misunderstandings or miscalculations.

Mr. THORNBERRY. Finally, for me, I think, General Alexander, if you had to grade our ability to defend DOD networks, what sort of grade would you give us at this stage, like, A through F?

General ALEXANDER. I would give us today probably a C, going up. And the reason I say a C is, we are working extremely hard on building the hardening part of our networks. We have done an awful lot of work to bring in the host-based security system and made tremendous movements. And we are moving in that range and building that up and training the force and hardening that. And it has made tremendous progress over the last 2 years. When you looked at the problems we had on our networks a few years ago to where we are today, it is a huge improvement.

I would like to say an A, but I think it is going to take some time to get us to an A. And an A is where I believe nobody could penetrate that network. But we have made it extremely difficult for adversaries to get in, and every day we improve that.

And that has the visibility and support of the Joint Staff and the Secretary. They have personally gotten involved. I had to take the reports up to both of them. And they are looking at that across all of the services. And each of the services are working it hard. We do that by network, by service, by COCOM, by agency. And we are looking at it in a very detailed way on our network operations and network security.

But I would say a C today and going up.

Mr. THORNBERRY. Well, and the "going up" was really my follow-up question. In earlier hearings, we have heard testimony that the advantage is with the attacker, and not only that, but the gap is growing so that the attacker has more advantage, if you look at the Internet as a whole, and versus the attempts to defend.

But I take it from what you have said that that gap, when it comes to defending military networks, is closing, that our ability to defend is—well, as I say, the gap is closing versus the attackers. Is that right?

General ALEXANDER. That is correct.

Mr. THORNBERRY. A significant difference from what we have heard from the civilian infrastructure, I would say.

I understand Mr. Johnson has a question.

Mr. JOHNSON. Yes, I do. Thank you, Mr. Chairman, for holding this very important hearing.

And we certainly need to be attuned to the fact that, for us to get on the dean's list, General Alexander, we are going to have to spend a lot more money than we are spending, and we will have to spend in accordance with long-term budgets, as opposed to short-term continuing resolutions. And it is the welfare of the people that is at stake.

Dr. Miller, you are, no doubt, familiar with the firm Palantir Technologies, are you not?

Dr. MILLER. I am not deeply familiar. I know the name, sir.

Mr. JOHNSON. And what about Berico Technologies?

Dr. MILLER. I also know the name.

Mr. JOHNSON. All right.

General Alexander, have you worked with Palantir in any of your official capacities?

General ALEXANDER. I am familiar with it. We have seen some of their technology, and they have demonstrated that. I am not sure of the number of contracts that we have with Palantir, to be honest.

Mr. JOHNSON. What about Berico?

General ALEXANDER. The same. I know the name. I would have to go back and look and see exactly what the contracts are with Berico.

Mr. JOHNSON. General, can you explain what services and capabilities those two firms offer to the Department of Defense and the intelligence community?

General ALEXANDER. My recollection of Palantir was a way of visualizing what is going on in the networks. One of the problems that we have is, how do you see what is going on in cyberspace? How do you actually see a network in a way that is meaningful to help defend and operate that? Especially if you have a network that has 15,000 different enclaves and all these different pieces, how do you make that meaningful?

And my recollection, working with Palantir, was, here is an idea that we could use for how to look at networks and how to secure it. We are looking at multiple options for how you actually see that. That is one of the things I think I put in my statement, you know, situational awareness, how do you actually see? I think that is an important step for us to all have that common situational awareness.

Mr. JOHNSON. Are those tools that are developed for use by the defense and intelligence communities by those contractors, do those contractors have the ability to use those tools, or the authority, actually, to use those tools in the private sector? Can they market those tools, in other words, to the private sector?

General ALEXANDER. I think every contract is written differently that gives you authorities to do things, and I would have to go look at how those contracts were written. I am not personally familiar with the contracts, so I would have to go look at that. And I don't know who those contracts are with specifically, so I would have to check that out.

But, generally speaking, in the development of a tool or a capability, in the contract it specifies whether that can be used broadly or whether it can be used only for the Government. And it depends on where it is being developed, for whom, and how.

Mr. JOHNSON. Dr. Miller, anything you want to add on that?

Dr. MILLER. Sir, General Alexander has it exactly right. And I can't provide any more details. We would have to go back and look at the individual contracts to answer those questions.

Mr. JOHNSON. Dr. Miller, would you be so kind as to provide my office with the DOD contracts with Palantir Technologies, Berico Technologies, and the firm HBGary Federal as soon as possible?

Dr. MILLER. Sir, I will do everything possible to do so. What I will need to do is, frankly, talk to our general counsel and make sure that the provision of that type of information is allowed contractually. And, in any case, we will get back to you as quickly as possible with as much information as possible.

Mr. JOHNSON. The contract could bar the executive branch from providing information to the legislative branch?

Dr. MILLER. No. No, sir. I guess I would like to be able to provide that information to you, and without knowing all the organizations within the Department that have the contracts, I am going to have to go back and—it will take a bit of time to be able to map that out.

And I also need—I need to have an assessment of whether or not—not of whether or not to provide the information, but in what form to provide the information to you. If you are asking for just the stack of contracts, I will say I will take that back to the Department and——

Mr. THORNBERRY. Yeah, Dr. Miller, if you would take the request back, get the lawyers to look at it, see what is possible. If it is not possible to provide the information the gentleman is asking, if you would ask the appropriate folks at the Department to let us know why. And, also, any information provided, of course, we would ask that it be provided to the whole subcommittee, so that all members can have it.

[The information referred to can be found in the Appendix on page 71.]

Mr. THORNBERRY. Does that sound good?

Mr. JOHNSON. Yes. Thank you, Mr. Chairman. And that will conclude my questions.

Mr. THORNBERRY. I thank the gentleman.

And I thank the witnesses very much for being here to testify, for your patience with our delays and other problems, which were rapidly solved.

Dr. MILLER. Mr. Chairman, if I might, in response to an earlier question about what the Government is doing with respect to radical groups' propaganda, I said it was an open policy issue. If I could have just a moment, I would like to clarify?

Mr. THORNBERRY. Sure.

Dr. MILLER. What I should have said is that it is a recurring, ongoing policy issue; that these issues need to be dealt with on a case-by-case basis; that, as the Congressman said, it is all the tools available to us, including diplomatic tools; and that, on a case-by-case basis, there will be a question about our desire to promote free speech and our real, not just desire, but requirement to protect our forces and our people.

And so I just wanted to—it is not a question of whether the issue is addressed. It is a question of how, in each case. And one would have to get down to the "eaches" to respond effectively.

I appreciate the opportunity to clarify that, sir.

Mr. THORNBERRY. No, I appreciate you bringing that. And I will also talk to Mr. West about my Smith-Mundt Repeal Act. It may be of interest to him as we pursue those issues.

So, again, we thank you all very much for being here, for the work you are doing in this area. And we anxiously await the Administration proposals so that we can all get to work on specific things.

With that, the hearing is adjourned.

[Whereupon, at 5:07 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 16, 2011

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 16, 2011

Statement of Chairman Mac Thornberry (R-Texas)

House Subcommittee on Emerging Threats and Capabilities

Hearing on

Fiscal Year 2012 National Defense Authorization Act—

Budget Request from the U.S. Cyber Command

March 16, 2011

The first hearing of this subcommittee posed the question: What should be the role of the Department of Defense to defend the country in cyberspace? Today, we ask the same question.

The example we used at our previous hearing was, if a formation of planes or hostile-acting ships came barreling toward the Houston ship channel, we have some idea of what most of us would expect from the government. They may try to identify who is in those ships or planes; they may try to divert them or even shoot at them. But, the bottom line is that we expect our government to protect us from threats we cannot handle on our own.

What about in cyberspace? If a bunch of packets come barreling through the Internet toward the same facilities, what do we expect of the government then? And is the government capable and is it authorized to do what we expect?

There seems to be virtually unanimous agreement that the threat to our country in cyberspace is growing.

DNI Clapper testified before during the Worldwide Threat Hearing that, "the threat is increasing in scope and scale, and its impact is difficult to overstate." Today, General Alexander will also give us an update on U.S. Cyber Command, its budget request for 2012, and how it is doing in terms of accomplishing its mission of defending Department of Defense networks.

But as Deputy Secretary Lynn wrote in *Foreign Affairs*, "The best-laid plans for defending military networks will matter little if civilian infrastructure—which could be directly targeted in a military conflict or held hostage and used as a bargaining chip against the U.S. government—is not secure."

In sum, I believe that our government and our country have not yet come to grips with the unique national security challenges cyber poses. The changes in technology have simply outpaced the modernization of our laws, regulations, and policies.

It seems to me that, despite a lot of good work from, among others the Ranking Member of this subcommittee and our witnesses, that we have not really grappled with and decided many of the key issues.

For the last eight months Congress has waited to receive the White House's proposals on cybersecurity. We continue to hear that they may come soon. But I note that in his letter of July 1, 2010, asking the White House to send its suggestions, Majority Leader Reid and six Senate Committee Chairs wrote, "Each day, the threat to cyberspace—and to the American citizens, businesses, servicemembers, critical infrastructure, and government agencies that depend on it—only increases." They also wrote, "Securing the vast digital infrastructure of our nation's communications networks and information systems—our cyberspace—is essential to the future of our government, our economy, and the security of our nation."

That's the reason we are here today.

Statement of Ranking Member James R. Langevin
House Armed Services Subcommittee on Emerging Threats and Capabilities
Hearing on
Budget Request for the U.S. Cyber Command

March 16, 2011

General Alexander, Dr. Miller, welcome. General, I want to commend you on the successful stand up of your new Command over the past months and thank you both for appearing today to discuss what I believe is one of the most important missions of our nation.

It is difficult to fully appreciate the importance of cybersecurity issues to our national security. From day-to-day tasks to critical operations, our warfighters depend on the integrity of our networks. At the same time, cyberspace itself has become weaponized. The STUXNET virus as well as massive denial-of-service attacks successfully targeting our allies in Georgia and Estonia have given us a glimpse of the damage cyberweapons can cause.

In some ways, thinking about conflict in cyberspace reminds us of some warfighting basics: the principles of offense and defense appear to remain largely the same, but the speed of information is so fast that complexity increases exponentially. Also, unlike the land, sea, or air, this virtual manmade domain is limitless. We must better understand how the United States should safeguard our critical networks while at the same time developing the full spectrum of cyber tools to deal with conflict in a new environment.

General Alexander, last September, when you appeared before the Armed Services Committee, I asked you about your role in defending critical infrastructure from cyberattack that may reside in other parts of the government, or in private hands. You noted that your role as head of US CYBERCOM was to protect only military networks. At an Emerging Threats Subcommittee hearing later that day with the chiefs of our service cyber components, I revisited your answer and asked what they were doing to protect military bases that solely rely on civilian critical infrastructure. Their answers were grim, but not unexpected.

Vice Adm. Barry McCullough, head of the Navy's 10th Fleet, testified that, "These systems … are very vulnerable to attack," noting that much of the power and water systems for our military bases are served by single sources and have only "very limited" backup capabilities. With an attack like the one demonstrated by Idaho National Labs in their Aurora experiment, on a power station potentially requiring weeks or even months to recover, our bases could face serious problems maintaining operational status. Beyond even the massive damage to our economy and civilian institutions that a major attack on our critical infrastructure could have, clearly this is a vital military concern as well.

Today I reintroduced language, which the House passed in our National Defense Authorization Act last year, which would enable the White House to better coordinate our federal cyber defenses and secure our critical infrastructure. I believe it is essential that we continue to make progress in managing this threat.

Although we have not yet faced a catastrophic cyber attack, every day we see lower level intrusions and thefts of everything from sensitive defense information, to information on our financial system and critical infrastructure, as suggested in numerous press reports. While I am certainly thankful that we have so far been spared a major attack, the low level of these incidents has in some ways hindered our ability to move forward on solving this issue. As the Commander of CYBERCOM and Director of the National Security Agency, you direct our nation's most powerful capabilities in the cyber realm, and I know from speaking with you that you also share my concerns that we have not fully seen the extent of the damage that cyberweapons can wreak. I know that defending against a collapse of our financial system or a meltdown of our power grids is outside the scope of the Department of Defense's responsibility, but if done intentionally, it would still amount to an act of war.

I look forward to hearing about how Cyber Command is growing and how your component commands are coming on line. I also look forward to hearing how the Administration is developing an overarching approach to cyber security, and how DoD's role may evolve. Most of all, I hope to understand what the Administration plans to do to fill the gap between these growing threats and our abilities in the public and private sectors to manage them. What authorities should we examine and what tools can the government develop to increase our ability on a national level to meet these challenges? Thank you once again. And I look forward to your testimony.

NOT FOR DISTRIBUTION UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE

STATEMENT OF

DR. JAMES N. MILLER
PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE
FOR POLICY

BEFORE THE

HOUSE OF REPRESENTATIVES
COMMITTEE ON ARMED SERVICES
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MARCH 16, 2011

NOT FOR DISTRIBUTION UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE

Chairman Thornberry, Ranking Member Langevin, and members of the subcommittee, thank you for inviting me to discuss Department of Defense (DoD) efforts in cyberspace, and the role of U.S. Cyber Command (USCYBERCOM). I am very pleased to join the USCYBERCOM Commander and National Security Agency (NSA) Director, General Keith Alexander.

The Department is investing heavily in information technology – $38.4 billion proposed for FY2012 – because it is an enormous force multiplier for military, intelligence, and business operations. In fact, DoD has over 15,000 networks and seven million computing devices, across hundreds of installations in dozens of countries around the globe.

Yet DoD's networks – as massive as they are – represent only part of our nation's growing reliance on cyberspace. Virtually every realm of civilian life now depends upon access to the Internet and other data-transmission networks. We use these networks every time we draw money from an ATM, open a webpage, or use our cell phones. With this reliance comes vulnerability; now that so many of our essential civilian and military functions depend on computer networks, we must recognize that any large-scale interference with such networks represents a potentially significant threat to our national security.

Understood in this context, DoD's proposal to spend $3.2 billion for cybersecurity in FY2012, including $159 million for USCYBERCOM, represents a sound investment in our national security.

We recognize that in the current fiscal climate, we must make hard choices about how we allocate scarce resources – both within the Pentagon and across the government. That is why I want to briefly describe the threats and vulnerabilities we face in cyberspace – as well as our plans to address them.

Threats and Vulnerabilities

DoD networks are attacked thousands of times each day, and scanned for vulnerabilities millions of times each day. Over one hundred foreign intelligence agencies are attempting to get into DoD's networks. Unfortunately, some incursions – by both state and non-state entities – have succeeded. These breaches have occurred mostly on unclassified networks, but in some cases on our classified networks as well.

The capabilities of state and non-state actors to exploit, disrupt, or even destroy DoD information systems are increasing. State actors are boosting their investments in cyberspace capabilities, and pose a considerable threat to U.S. cybersecurity. Al-Qaida, the Taliban and Hizbollah have long used cyberspace to plan their operations and influence global populations. Al-Qaida has vowed to launch a cyber attack on the United States. As technologies improve, non-state adversaries will be capable of conducting increasingly sophisticated cyberspace operations.

The theft of valuable information is to date the most concerning consequence of cyber intrusions. Over the last several years, malicious actors have stolen terabytes of data – including information used in the development of weapons systems – from companies in the U.S. defense industrial base (DIB). Leading information technology companies have also lost intellectual property as a result of sophisticated operations perpetrated against corporate infrastructures. More recently, critical infrastructure has been targeted, including our electric grid and the financial-services sector.

Moreover, cyber threats do not come exclusively from the outside. To the extent that we succeed in improving our defenses against external actors – and we must do so – outside actors will have greater incentives to try to use insiders to gain access to our networks. As we have

witnessed in WikiLeaks, insiders may sometimes prove willing to help disseminate sensitive information, even if it puts at risk the lives of many who support the United States, and damages U.S. national security.

One of the complexities of cybersecurity is that the distinction between "external" and "internal" threats can be blurred. That's because some of the gravest threats can be located in the networks themselves, and in the worldwide chain of suppliers we rely on to build our cyberspace infrastructure in the first place.

The global distribution of information-technology (IT) manufacturing means that software and hardware are at risk of being tampered with before they are linked together in an operational system. Tampering can even occur as part of regular maintenance and updating functions that modern IT equipment requires. Counterfeit hardware and software have been found in DoD systems already. We must remain alert to the possibility that "rogue code," "backdoors," and "kill switches" could be written into computer chips used by the Department or by other U.S. critical infrastructure.

In the face of this urgent threat, the Department of Defense is undertaking five initiatives to reduce its vulnerability. Because cybersecurity is a "team sport," two of our five strategic initiatives focus on partnerships with other government agencies, private companies, and allied nations.

1. Treating Cyberspace as a Domain for Organizing, Training, Equipping, and, When Directed, Operating

For the purposes of organizing, training, equipping, and, when directed, operating our forces, DoD recognizes cyberspace as a domain for military activities, analogous to the maritime,

air, land, and space domains. This understanding is essential for allowing DoD to clearly establish and achieve its cyberspace missions.

This initiative is not about "militarizing" cyberspace, any more than maintaining the U.S. Navy is about "militarizing" the ocean. Rather, our posture acknowledges a basic reality: Cyberspace presents security challenges that are too novel and too serious for it to be treated as an add-on to our traditional operations on land, at sea, or in the air. Just as in other domains, the Law of Armed Conflict applies to our activities in cyberspace, and civil liberties and privacy rights must be protected.

In order to focus DoD's cyberspace efforts, the Department established USCYBERCOM, as a subordinate command to United States Strategic Command. USCYBERCOM reached initial operating capability on May 21, 2010, and final operating capability on October 31, 2010.

DoD has requested $159 million for USCYBERCOM in FY2012. This includes:

- Facilities at Fort Meade, Maryland ($18M);
- Personnel ($47M);
- Information Technology and Communications support, including information technology fee-for-service, hardware, and software, as well as multiple networks and enclaves ($17M);
- Operations for day-to-day supplies, travel, training and support for the design of a Joint Operations Center ($36M);
- Research, development, test and evaluation ($26.0M), including a joint threat incident database and an Internet Service Provider Test Bed to create realistic environments; and
- Military construction ($15.0M).

Each of the military Services has established component commands of USCYBERCOM to effectively organize, train and equip America's soldiers, sailors, airmen and Marines for cyberspace operations. All four Services are developing service-specific capabilities, requirements, and skills for future cyber operations. In addition to taking steps to ensure that our DoD-operated networks, systems, and net-centric warfighting capabilities are available, all combatant commands and the Services must also prepare to operate in a "degraded cyber environment" in which cyberspace access is not assured or could be interrupted. To better understand this rapidly unfolding area, DoD conducts red-team assessments about future cyber threats to inform its strategic and operational planning.

All of these measures help ensure the U.S. military is prepared, if directed, to conduct full-spectrum cyberspace operations. Whether protecting U.S. interests in cyberspace or supporting broader military operations, our force needs to be as prepared to operate in cyberspace as it is in the traditional land, air, sea, and space domains.

2. Employing New Operational Concepts

DoD's second strategic initiative is to employ new defense operating concepts to protect our networks and systems. This includes advanced tools for cyberspace hygiene and active cyber defenses.

The first layer of defense is enhanced cyber hygiene, which includes such seemingly mundane but essential measures as updating the virus definitions of protective software. In addition to systems that ensure each DoD computer has "downloaded the patch," we now have host-based security services that can better map our systems, determine who is using them, and detect suspicious behavior.

Active cyber defense is crucial to detecting and stopping threats to our systems. It includes a perimeter defense of the dot.mil domain that screens incoming traffic for malicious code and malware. Because no perimeter defense is fail-proof, DoD also hunts on its own networks – looking for anomalies like viruses, worms and other software that could cause damage to our networks and systems. The Department has requested increased funds to carry out this protective self-surveillance, and to stop the intrusions that are found.

In addition to these measures, DoD is conducting research and development of new defense operating concepts, including the use of multiple networks to add resiliency; new "clean-slate" architectures to secure networks against the insider threat; and the use of cloud computing, virtualization, and advanced encryption.

3. Working with Other Government Agencies and the Private Sector

DoD's third strategic initiative is to work closely with other U.S. government departments and the private sector to create a national approach to cybersecurity. To this end, DoD supports the efforts of DHS, the lead department for protecting the Nation's critical networks.

To allow the Department of Homeland Security (DHS) to draw upon the cybersecurity capabilities already established by the National Security Agency and USCYBERCOM, Secretary of Defense Gates and Secretary of Homeland Security Napolitano signed a Memorandum of Agreement (MOA) on September 27, 2010. This agreement establishes a Joint Coordination Element at NSA, led by a senior DHS official with an NSA Deputy, which will improve the synchronization of our operational planning, help develop threat assessments, provide intelligence support, and allow for the joint development of new capabilities. A dedicated civil-liberties and privacy office supports this effort. DoD works with other departments and agencies

as well, as demonstrated by the Defense Cyber Crime Center's partnership with the FBI and other law enforcement agencies to create the National Cyber Investigative Joint Task Force (NCIJTF).

A great deal of sensitive but unclassified information resides on the networks of companies that work with our military, including approximately 2,600 cleared defense contractors. In 2007, DoD initiated a pilot program to determine whether the Department could help improve the cybersecurity of these affiliated systems. This three-year pilot program, with 36 different companies, significantly increased information sharing about the threats faced by companies, as well as information about how best to defeat those threats. Accordingly, DoD is requesting $113 million over the Future Years Defense Program (FYDP) to upgrade this pilot to a full program. We are also exploring other pilot projects with industry that would allow DoD to further extend its suite of cybersecurity capabilities to companies in the defense industrial base.

Pilot programs figure into the Department's strategy to protect or supply chain as well. The pilots that we have developed, if successful, will move towards full operational capability by FY2016, and will help DoD to reduce risks in the components that make up our operational systems.

4. Build Relationships with Allies and Partners

DoD's fourth strategic cyberspace initiative is to build robust relationships with U.S. allies and international partners. The Internet is a network of networks comprised of thousands of Internet service providers (ISPs) and billions of end users across the globe. No single state or agency can maintain effective cyber defenses on its own. DoD, in coordination with the State Department and other agencies of the U.S. government, will seek strong international relationships to defend U.S. and allied interests in cyberspace. The development of shared

situational awareness and warning capabilities will increase collective cybersecurity. Crucially, these partnerships will help us develop a global cyber-forensics capability to identify and track those responsible for incursions as well. In this new era, any hope that we have of deterring potential adversaries depends on our establishing accountability, and this will require extensive international cooperation.

To deter malicious behavior in cyberspace, DoD also supports the effort to define and promote international norms and principles regarding cyberspace. By clarifying acceptable behavior, enabling international communication, and minimizing the potential for misunderstanding and escalation, such standards will provide a foundation for the deterrence of malicious activities.

DoD has worked closely to build collective cyber defenses with Australia, Canada, New Zealand, and the United Kingdom. Over the last year, DoD has expanded its collaboration to include NATO. The Deputy Secretary of Defense travelled to Brussels twice over the last year to clarify the importance of cyberspace in NATO's new strategic concept and to help define an alliance agenda for rapidly deploying more advanced cyber defenses. DoD has initiated discussions with other allies and partners as well; working closely with the State Department, DoD will continue to explore new opportunities for international cooperation in cyberspace.

5. Workforce Development and Technological Innovation

The last initiative that I want to discuss – but far from the least important – is our effort to build a pool of talented civilian and military personnel to help DoD achieve its cyberspace missions, and to accelerate technological innovation.

Within DoD and across the government, the development of a cybersecurity workforce is a matter of national security. To build a capable cyber workforce, DoD will focus on attracting

talented personnel in the early stages of their careers. DoD will expand its educational scholarships, like the Information Assurance Scholarship Program, the Scholarship for Service program, and the U.S. Cyber Challenge. The Cyber Patriot program, one of the world's largest high-school cyber defense competitions, will help DoD to develop a talent base for future defense and national security missions. Going forward, DoD will seek to enhance the Information Technology Exchange Program. This program, which is just getting underway, will allow for the expanded exchange of IT and cybersecurity personnel between government and industry.

DoD is fortunate to have access to a great deal of relevant expertise already – our National Guard and Reserve personnel include many advanced technology professionals who have a strong academic or professional grounding in cyber-related issues. It is incumbent upon the Department to utilize this current and future expertise as much as possible – breaking down traditional organizational barriers wherever they impede our efforts to put the best men and women on the front lines of our nation's cyber defense.

Our organizational challenges in cyberspace are not limited to the assignment of our personnel. They also haunt our acquisition systems – with potentially harmful results for our national security. It currently takes the Department of Defense approximately 81 months to make new computing systems operational. This means that by the time DoD has fielded its computing systems, they are already three to four generations behind the state of the art.

We must adjust DoD's acquisition processes to reflect the life cycle of technology development and the different uses to which IT is put. This means operating at cycles of 12 to 36 months as opposed to seven or eight years. DoD also needs to test and develop its systems on an incremental basis, rather than through the simultaneous deployment of large, complex

systems, that has proved so problematic. Through its legislation on IT acquisition reform, Congress has given the Department the tools to do better, and we must do so.

Our current procedures compel us to make long-term predictions about the future state of network technology – and then lock ourselves into the products and programs that emerge from those prognostications. In a field as dynamic and fluid as cyberspace, this is a recipe for high-stakes failure. We need a much more responsive approach, one that will allow for modular, adaptive investments and technological enhancements.

Even as DoD works to accelerate the deployment of new technologies, we must enhance security measures in procuring software and hardware. No backdoor can be left open; no system installed without proper vetting. To this end, DoD has recently announced several important initiatives to strengthen DoD's cyberspace technological capabilities.

- DoD is requesting $500 million in new Defense Advanced Research Projects Agency funds over the FY2012-2016 FYDP for cyberspace technologies, with a focus on areas like cloud computing, virtualization, and encrypted processing.
- The Department will continue to execute our cybersecurity pilot programs, as funded in FY2010, which provide seed capital to leading-edge technology companies to develop dual-use technologies that serve America's cybersecurity needs.
- We are developing a National Cyber Range that will help DoD and the U.S. government to operate successfully in a contested cyber environment. This facility will create models of the Internet and various networks, affording the military, other U.S. government agencies, the private sector, and potentially international allies and partners the opportunity to test new concepts and simulations at an effective scale. DoD is working

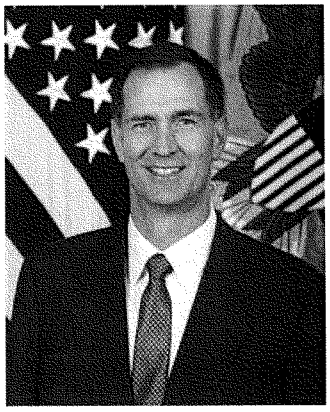
with other agencies of the U.S. government to create a transition plan now and to manage the issues associated with the conversion.

Conclusion

Thank you for this opportunity to describe some of the challenges the Department of Defense faces in cyberspace. With help from Congress, DoD is moving aggressively to protect our networks and help ensure our nation as a whole is better able to defend itself against threats in cyberspace. We have made significant strides in the last year – and I believe that our agenda is robust. I look forward to working with Congress to ensure we have the necessary capabilities to keep our country safe and our forces strong. I look forward to your questions.

Dr. James N. Miller

Principal Deputy Under Secretary of Defense for Policy



Dr. James N. Miller was confirmed by the U.S. Senate as the Principal Deputy Under Secretary of Defense for Policy on April 2, 2009. He serves as the principal staff assistant to the Under Secretary of Defense for Policy and provides advice and assistance to the Secretary of Defense and Deputy Secretary of Defense on all matters concerning the formulation of national security and defense policy and the integration and oversight of DoD policy and plans to achieve national security objectives.

Prior to his confirmation, Dr. Miller served as Senior Vice President and Director of Studies at the Center for a New American Security. Previous positions include serving as Senior Vice President (2003-2007) and Vice President (2000-2003) at Hicks and Associates, Inc.; Deputy Assistant Secretary of Defense for Requirements, Plans, and Counterproliferation Policy (1997-2000); assistant professor at Duke University (1992-1997); and senior professional staff member for the House Armed Services Committee (1988-1992).

A member of the International Institute for Strategic Studies, Dr. Miller has served as an advisor to the Combating WMD Panel of DoD's Threat Reduction Advisory Committee and the Defense Science Board, as senior associate at the Center for Strategic and International Studies, and as senior associate member at St. Antony's College, Oxford. In 2000 he received the Department of Defense Medal for Outstanding Public Service.

Dr. Miller received a B.A. degree with honors in economics from Stanford University, and Master's and Ph.D. degrees in public policy from the John F. Kennedy School of Government at Harvard University.

NOT FOR DISTRIBUTION UNTIL RELEASED BY THE

HOUSE COMMITTEE ON ARMED SERVICES

STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

16 MARCH 2011

NOT FOR DISTRIBUTION UNTIL RELEASED BY THE

HOUSE COMMITTEE ON ARMED SERVICES

Chairman Thornberry, Ranking Member Langevin, and distinguished members of the Subcommittee on Emerging Threats and Capabilities, thank you for inviting me today to represent the extraordinary men and women of the United States Cyber Command and deliver the Command's posture statement. I want to begin my remarks by thanking you and your colleagues in Congress for helping us to build this Command and assisting its efforts to accomplish its mission. Cybersecurity is vital to our nation—perhaps now more than ever—and part of our task is ensuring that our nation understands what it is that you, the White House, and the Department of Defense have charged us to do and why it is so important that we do it well. I look upon these remarks before you as an invitation for dialogue about the roles, missions, and capabilities of Cyber Command, and I am eager to hear your views on how we are doing and where we should be going.

Before proceeding, I also wish to thank the great leaders and partners we have had in building the capabilities of US Cyber Command since its creation last year. Secretary of Defense Gates, Deputy Secretary Lynn, Chairman Mullen, and Vice Chairman Cartwright have been particularly supportive, as has General Kehler, the new Commander of US Strategic Command. Our Combatant Commands, moreover, have been appreciative of our initial steps, applauding initiatives to pioneer new ways of presenting cyber capabilities to the Joint force. We also owe a great deal of gratitude to the dedicated professionals of the National Security Agency / Central Security Service (NSA/CSS) whom it is also my honor to lead. Their contributions are significant, along with those of the Defense Information Systems Agency and our many other partners inside and outside of the U.S. government. There are many others I

could name here, but in the interest of brevity and to leave more time for a dialogue with you, I shall forbear.

If you will, allow me to brief you on what has been happening at US Cyber Command and where we are trying to go. Constructing a new Command while conducting operations is quite a challenge, especially in a time of rapid technological and policy changes, but we have produced results that have made our nation stronger and more secure. Let me emphasize this point: Cyber Command has already returned cybersecurity dividends on the investments of time and resources dedicated to its creation. We are making progress, and with your help, we will surmount the issues that remain for us as we accomplish our mission.

The Road to Full Operational Capability

US Cyber Command achieved full operational capability (FOC) on 31 October 2010 as a subunified command under US Strategic Command (USSTRATCOM). The road to FOC culminated roughly according to the timetable prescribed by the Secretary of Defense when he directed the establishment of the Command back in June 2009. Initial operational capability (IOC) was originally projected to have been reached that October, but that date slipped to May 2010, when my nomination to serve as its first Commander was confirmed by the Senate. We put the months between October 2009 and May 2010 to good use, however, building a consolidated staff to merge the two legacy organizations, Joint Functional Component Command for Network Warfare (JFCC-NW) and Joint Task Force for Global Network Operations (JTF-

GNO), which together became Cyber Command. We also outlined the tasks needed to move us to FOC once the clock started running. Though the interval between initial capability in May and attaining full operational capability in October was only five months instead of the planned twelve, we were able to accomplish a number of key activities. Moreover, we did all this while accelerating the tempo of daily operations that had been established by JTF-GNO and JFCC-NW.

Despite the compressed schedule, the consolidated staff at the nascent Cyber Command was able to accomplish a great deal by last October. We established a Joint Operations Center, transferred operational control of the JTF-GNO mission set to Ft. Meade, Maryland, and stood down JTF-GNO's 24/7 watch center in Arlington, Virginia, which helped USSTRATCOM disestablish JFCC-NW and JTF-GNO. The latter task took a considerable amount of planning and careful orchestration because JTF-GNO's activities and workforce had to be transitioned from Northern Virginia to Ft. Meade while ensuring the daily functioning of the Department of Defense's networks were unimpaired. We established effective operational command and control processes for the consolidated mission sets. A Joint Intelligence Operations Center was established. Our Service cyber components were formally assigned to USSTRATCOM, and we continued building relationships with key partners. We embedded liaison officers at the Combatant Commands and set conditions to expand their presence to larger Cyber Support Elements. We deployed expeditionary teams to support operations in Iraq and Afghanistan. We also made progress in our support of operational planning by the Combatant Commanders and in building processes for them to issue requirements for cyber support. We accomplished all of this

without negative mission impact, keeping the Department's operations secure while making the transition transparent to users of its information systems.

Our overall success during this critical phase was not without challenges, and there remain some important issues yet to be resolved even after Cyber Command's attainment of FOC. The Department has a shortfall of cyber force capacity to plan, operate, and defend its networks and ensure freedom of action and maneuver for our nation in cyberspace. Additionally, we are still discussing across the Administration how to best defend against a "Cyber 9/11" that affects our critical infrastructure and beyond. Finally, we have only begun our effort to take advantage of significant efficiencies in designing and managing our information technology architecture.

US Cyber Command continues to build synergy with NSA/CSS to take advantage of NSA/CSS's infrastructure and expertise, which remain crucial to our progress. Our co-location allows the government to maximize our collective talent and capabilities. The Command's Fiscal Year 2012 budget is projected to be $159 million, and our workforce at that point is slated to be 464 military personnel and 467 civilians for a total of 931 employees plus focused contract support. The overall mission of this team is to plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of specified Department of Defense information networks; and prepare to, and, when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US and Allied freedom of action in cyberspace, and deny the same to our adversaries. Let me turn now to the environment in which we are executing that mission.

Current Perspectives

When I spoke before the full committee last fall, a month before the declaration of full operational capability, I offered my explanation of cyberspace, noting the importance to our nation of maintaining our freedom of action to this new, unique, man-made domain and preserving our security in it. I also spoke of the challenges that we face in doing so. Yours is one subcommittee that needs no reiteration of these points, and so I shall move on directly to more recent developments and our evolving perspectives on how to deal with them.

The cyber threat continues to mature, posing dangers that far exceed the 2008 breach of our classified systems we discussed last fall. Our leaders from President Obama on down have emphasized this point, and for good reason. Our nation now depends on access to cyberspace and the data and capabilities residing there; we are collectively vulnerable to an array of threats ranging from network instability to criminal and terrorist activities to state-sponsored capabilities and actions that are progressing from exploitation to disruption to destruction. While I hasten to say that we have not suffered disastrous or irreparable harm in cyberspace from any of these risk categories, we must be prepared to counter this evolving threat.

Both external actors and insider threats pose significant challenges to our cybersecurity.

No state actor, of course, has admitted to launching disruptive cyber attacks on another state. Yet incidents have occurred that look a great deal like such attacks. The cyber assaults on

Estonia in 2007 spurred us and our NATO allies to deliberate regarding what in cyberspace would constitute an "armed attack" on an alliance member that would trigger the North Atlantic Treaty's provisions on collective defense. The following year, the invasion of Georgia coincided with precisely targeted cyber attacks, marking one of the first times we have seen such "cyber supporting fires." The coincidence was so perfect that independent observers concluded there was no coincidence—that the hackers who temporarily crippled the Georgian government's response and communications with the outside world had practiced their assaults and responded to official cues when they mounted them for real.

We have recently seen Internet access manipulated or curtailed by governments to suppress and disrupt even peaceful protests by their own citizens. In addition, we believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for destructive cyber effects, having long been mostly theoretical, are now real and increasingly available; we must worry not just about their intentional use, but also about their accidental release. Segments of our nation's critical infrastructure are not prepared to handle this kind of threat.

Bear in mind that we also watch with concern the growing capabilities of non-state actors. The threats we see here are asymmetric, meaning that comparatively new or lesser players can cause effects commensurate with state-sponsored actions; a small and inexpensive operation can divert government resources for spotting and diagnosing a problem, neutralizing the malware employed, patching the exploited vulnerability, and recovering from the

institutional (and personal) damage it caused. Although individuals with computer skills have independently shown that such attacks can be launched by even a lone actor with a laptop and a motive, we are chiefly focused on terrorists and well-organized cyber criminals. The former continue to grow more proficient in using the Internet as a medium for recruitment, coordination, and other activities, and they are becoming ever-more sophisticated in doing so. Cyber criminals are more interested in the theft and exploitation of sensitive data that can bring them a profit, either directly through fraud or identity theft, or indirectly through the pirating of intellectual capital. Indeed, observers such as Senator Sheldon Whitehouse and a bipartisan team of colleagues last summer called this as "the biggest transfer of wealth through theft and piracy in the history of mankind"—a transfer that has significantly lowered the cost for potential adversaries to close and counter our technological lead. Such activity is crime, of course, and belongs more properly in law enforcement than military channels, but when a prime target of such crime is our defense industrial base, we in the Department of Defense have a role to play in the response. We also find that state actors and terrorists can exploit the breaches and tools made by criminals, much as a dangerous pathogen opportunistically employs a disease vector to enter a host. Indeed, sometimes the state and non-state actors collaborate on matters of mutual interest.

Various threats that emanate from poor cyber hygiene, inadvertent misuse, and malicious actions also create significant security challenges. After all, even the most astute malicious cyber actors—those who can break into almost any network that they really try to penetrate—are usually searching for targets of opportunity. They search for easy vulnerabilities in our systems security and then exploit them. I am very concerned by the ways in which neglect makes us vulnerable. The unapplied software patches, the firewalls left unattended, and the anti-virus

suites that never get updated even in the US military cause us more trouble than I like to admit, especially when a risk to one is a risk shared by all. Now multiply those problems across the government and the private sector, and realize that we have networked our vulnerabilities while segmenting our defenses among the .mil, .gov, .com, and .edu Internet domains. Each domain (and often each system) has been left to fend for itself against cyber actors who care little for legal distinctions and organizational boundaries. And finally there is the insider threat; I am sure I need not remind anyone that some of the largest security breachs in history have originated from insider threats.

The recent creation of Cyber Command has garnered a great deal of interest from foreign militaries and the governments that oversee them. We see frequent media reports on nations contemplating the creation of their own "cyber commands." I see this as a sign not necessarily of a "militarization" of cyberspace but rather a reflection of the level of the concern with which civilian and military leaders around the world are viewing current problems. Many such steps are essentially defensive, and if so many nations are interested in improving their defenses, they are probably even more willing to talk about ways they can reduce common threats. There is a rough, *de facto* deterrence at the strategic level of cyberspace. Although no one knows how a cyber war would play out, even the most capable state actors seem to recognize that it is in no one's interest to find out the hard way. I am convinced this concern has led to a certain degree of restraint by states that we deem capable of causing very serious cyber effects. Lest optimism obscure real threats, however, I must add that we have no certain capability to restrain the behavior of radical, non-state extremists.

In sum, our adversaries in cyberspace are highly capable. Our defenses—across dot-mil and the defense industrial base (DIB)—are not. Our economy, our society, and all of us have become directly or indirectly dependent on access to and freedom of movement in cyberspace—and indeed our military is equally dependent on such access—and thus we cannot be content with a situation in which we are sometimes our own worst enemies.

Next I want to tell you about some of the things we are doing and planning at Cyber Command to ensure that the Department of Defense has done all it can to defend and deter determined adversaries, mitigate dangerous threats, and address nagging vulnerabilities, so that even our most capable opponents will know that interfering with our nation's equities in cyberspace is a losing proposition.

Working toward the Future

As you can gather from the foregoing discussion, US Cyber Command faces serious challenges as it comes together to do urgently needed work in cyberspace. Our establishment reflects the department's need to manage cyber risk, secure freedom of action, and ensure the development of integrated capabilities. Our intent is to overcome the challenges we face through the concerted efforts of implementing The National Military Strategy of the United States of America 2011. We will pursue resolution of the capacity, resources, and information technology efficiencies issues we face through the five strategic initiatives of the department's strategy. We intend to:

- Treat cyberspace as a domain for the purposes of organizing, training, and equipping, so that DoD can take full advantage of cyberspace's potential in military, intelligence, and business operations
- Employ new defense operating concepts, including active cyber defenses, such as screening traffic, to protect DoD networks and systems
- Partner closely with other U.S. government departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cyber security
- Build robust relationships with U.S. allies and international partners to enable information sharing and strengthen collective cyber security.
- Leverage the Nation's ingenuity by recruiting and retaining an exceptional cyber workforce and to enable rapid technological innovation.

In this context, let me show you the reasoning behind our planning and activities, and give you a sense of where we might need assistance in reaching our goals. The best way to organize this discussion is by our Command's mission areas. As noted earlier, we were established to operate and defend Department of Defense networks. When I see you again a year from now, I intend to report that we are executing that mission and achieving greater security for our networks.

Our first duty is to ensure that Department of Defense networks are secure. Securing these networks is crucial to protecting our data, to our warfighting potential, and ultimately to the defense of our nation. Until recently we all viewed our networks as a great force multiplier—the magic that let us put ordnance on target and dispatch planes, troops, and ships to where they were needed, when they had to be there. Today, however, we understand that those networks

represent a serious vulnerability, and we dread the thought of someone getting inside to bring them down or, perhaps even worse, to make a few subtle changes to the integrity of our data that bring all our military operations to a halt. Without fast, assured, and safe data flows we will not be able to fight our adversaries the way we as Americans think they should be fought. We are not necessarily close to losing that edge, but potential adversaries understand where it lies, and are certainly contemplating ways of blunting it in any future conflict.

Cyber Command is working to preserve that information advantage in many ways. We are directing the operations of the Department's information networks, which knit together seven million computing devices spread across fifteen thousand networks. The recent move of the Defense Information Systems Agency to a new facility near us on Fort Meade has enabled even greater collaboration between our two organizations. Cyber Command and DISA collaborate on a daily basis to monitor the functioning of the Department's information networks. That work includes the maintenance of sensors to detect and block adversary activity in those networks, the inspection of security settings and practices, and the investigation of real and suspected incidents. Together we are making progress in all of these areas, and I am more comfortable today than I was twelve months ago in our ability to stop intrusions and adapt to changing adversarial practices almost as fast as they evolve. The new sensor capabilities we are deploying and the aggressive inspection regime now coming together will improve our situation even more over the year to come.

We also plan, in partnership with NSA, the defense of specified Department of Defense information systems, knowing that we have to stay ahead of the cyber threat in technological

terms. Here US Cyber Command and our partners in the Department are working on ways of shifting to a different and more defensible architecture for providing information services to users. A year from now we should be well on our way to having a hardened architecture proven and in place, which provides a new level of cyber security. The idea is to reduce vulnerabilities inherent in the current architecture and to exploit the advantages of "cloud" computing and thin-client networks, moving the programs and the data that users need away from the thousands of desktops we now use—each of which has to be individually secured for just one of our three major architectures (NIPRNet, SIPRNet, and JWICS)—up to a centralized configuration that will give us wider availability of applications and data combined with tighter control over accesses and vulnerabilities and more timely mitigation of the latter. Moving to a cloud architecture has the advantages of producing economies of scale and reducing the Department's information technology costs. This architecture would seem at first glance to be vulnerable to insider threats—indeed, no system that human beings use can be made immune to abuse—but we are convinced the controls and tools that will be built into the cloud will ensure that people cannot see any data beyond what they need for their jobs and will be swiftly identified if they make unauthorized attempts to access data.

A year from now I look forward to telling you that we have "operationalized" our Department's networks. We will, of course, continue to do this with full regard for and protection of the privacy and civil liberties of US persons as well as in compliance with all applicable laws and regulations. The idea is to transform the Department of Defense's information systems from something to be passively guarded into a suite of capabilities that offer our commanders and senior leaders opportunities to adjust our defenses. If people who seek to

harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behavior change. The technology is ready and I encourage a conversation on the privacy and civil liberties impact of such technology and how to adjust laws and policies to allow the use of this technology for cyber defense.

Our Command's mission document states that we coordinate, integrate, and synchronize activities to direct the operations and defense of the Department of Defense's networks. In practice, that means we spend a great deal of time talking with leaders and experts in the Department, the U.S. Government, private industry, and other nations as well. This effort begins, of course, with US Cyber Command Service cyber components that provide the forces that implement our plans and execute our directives (they are the Army Cyber Command, Marine Corps Forces Cyber Command, Fleet Cyber Command, and Air Force Cyber Command). We are still maturing the way in which we and they will interact to support and be supported by the geographic combatant commands in various situations. Our mission depends as well on the work of the National Security Agency, which provides the expertise and intelligence that are indispensable to understanding what is happening in cyberspace. We are constantly engaged with DISA as well, and our relationship with them will likely change substantially and become even closer in the near future. In addition, since I spoke to you last fall we have strengthened our strategic partnership with the Department of Homeland Security in accord with the recent agreement concluded by Secretaries Gates and Napolitano. A senior DHS official now works at NSA with us and attends many of our leadership meetings, and several government agencies are also represented 24 hours a day in our Joint Operations Center. These measures, along with complementary measures at Department of Homeland Security and other partners, should

provide a whole-of-government awareness of what everyone is seeing so that we can plan for and execute authorized and coordinated joint actions in the event of an emergency. Finally, we are active players in the Department of Defense's productive discussions between government and industry over how to share information regarding common threats and potential ways of mitigating them. The vast majority of our military's information packets ride on commercial infrastructure, and thus we need to develop shared insights into those dependencies for mission assurance purposes.

The second part of our mission at Cyber Command is to be prepared to conduct full spectrum military cyberspace operations in order to enable actions in all domains. As I noted above, states and non-state actors have already experimented with ways of harassing or attacking rival governments, whether to make a strategic point or in conjunction with kinetic attacks. Our military and our nation would be unwise to assume that we have seen the last such attacks. We are prepared, when directed and in full compliance with applicable laws, including the Constitution, federal statutes, and the Law of Armed Conflict, to respond when we or our allies are threatened or subjected to the use of force in the cyberspace. The President has emphasized that our digital infrastructure is a strategic national asset and insisted that preparing our government for the task of protecting strategic national assets in cyberspace is a national security priority. Our efforts to do this are designed to achieve two goals:

- First, we protect US and allied freedom of action in cyberspace. It is no longer possible to conceive of our nation functioning properly or even defending itself without the ability to create, transmit, and secure masses of digitized data. Making our access to cyberspace

impossible or even problematic would represent a strategic threat to America's vital interests—one that our Command has been established and tasked to prevent with respect to DoD's operations in the cyberspace. Furthermore, our cybersecurity is inextricably linked with that of our allies, and our interests in cyberspace often coincide with those of other states with whom we have less-formal ties. The lack of geographic borders in cyberspace means that a threat to one can be a threat to all, which gives us a real incentive to share situational awareness and best practices that help to protect our military, government, and private networks and data.

- Second, when directed, we need to deny freedom of action in cyberspace for our adversaries pursuant to appropriate authorization and consistent with applicable law. Working with the Executive Office of the President and other U.S. government departments and agencies, US Cyber Command stands ready to support the development of all necessary policies for cyberspace operations. As with all activities that DOD pursues, operations are only executed with a clear mission and under clear authorities, and they are governed by all applicable laws, including the Law of Armed Conflict. We cannot afford to allow cyberspace to be a sanctuary where real and potential adversaries can marshal forces and capabilities to use against us and our allies. This is not a hypothetical danger; we have seen adversaries use the Internet to harm US forces and coalition partners. At Cyber Command much of our focus is on helping our troops in the field limit their vulnerabilities in and from cyberspace. This effort reflects the likelihood that; henceforth all conflicts will have some cyber aspect, and our efforts to understand this development will be crucial to the future security of the United States. DoD is

collaborating with the Executive Office of the President and other Departments and Agencies to resolve outstanding policy and authority questions.

We are making progress executing these missions, but I also want to share with you one of my chief concerns. The importance of the cyber mission is something that our Department and its constituent Armed Services did not anticipate or build forces to address. As we improve our common operating picture and our intelligence to understand what is happening, as well as our operations to create effects, we are finding that we do not have the capacity to do everything we need to accomplish. To put it bluntly, we are very thin, and a crisis would quickly stress our cyber forces. The problem has two facets—there are too few trained Service personnel out there in the first place, and also the Services need to hold on to as many of them as they can. Thus in both of the mission areas above, the biggest issue I see is the need for collaborative force development (including joint standards, recruitment, training, deployment, sustainment, and retention).

We at Cyber Command also need to grow the authorities we work under. A year from now we hope to have robust authorities for key enablers like budgeting, training, and career development, as well as for the swift acquisition and testing enabling technologies. We will also build our collaboration with national and Service research and development laboratories. All of these steps will, I believe, make us much better postured to accomplish the mission that our nation has entrusted to us.

Conclusion

I thank you again for calling me before you today and allowing me the opportunity to submit this posture statement on behalf of US Cyber Command. The Department of Defense took an important step for our nation in creating this Command and declaring it to be in full operational capability status last fall. I have described our philosophy of actively managing the Department's information networks—not just to defend them, but to use them as a tool to assist our warfighters, planners, and commanders by preserving their freedom of action—and also to be as ready to use our own capabilities to disrupt any adversarial use of cyberspace against US interests. If I may, I'd like to reiterate our intention to:

- Increase the capacity of the cyber workforce;
- Implement and exploit, in a strengthened partnership with NSA, the transformation of the Department's networks;
- Work with the Combatant Commands to synchronize processes and planning to deliver the joint effects they require;
- Support DOD, DHS, and other Government partners in the extension of cyber defense capabilities across the U.S. Government's network and,
- With DHS, increase our government's dialogue with private partners on the protection of our nation's critical infrastructure.

We in Cyber Command operate with respect for civil liberties and in compliance with the laws governing the privacy of our fellow Americans, in accord with the directives of the national command authority, and, in conjunction with our mission partners in the Departments of Defense and Homeland Security, law enforcement, the intelligence community, industry, and academia. We do not see the security of our nation and the protection of civil liberties and privacy as a balance; rather, we believe we can and must defend both. I thank you for your help in this endeavor, and I am confident that together we will succeed. And now I look forward to your questions.

Biography - Director, National Security Agency/Central Security Service

GEN Keith B. Alexander
United States Army

General Keith B. Alexander, USA, is the Commander, U.S. Cyber Command (USCYBERCOM) and Director, National Security Agency/Chief, Central Security Service (NSA/CSS), Fort George G. Meade, MD. As the Director of NSA and Chief of CSS, he is responsible for a Department of Defense agency with national foreign intelligence and combat support responsibilities. NSA/CSS civilian and military personnel are stationed worldwide. As Commander, USCYBERCOM, he is responsible to plan, execute and manage forces for coordinating DoD computer network attack (CNA) and computer network defense (CND) as directed by USSTRATCOM.

He was born in Syracuse, NY, and entered active duty at the U.S. Military Academy at West Point.

Previous assignments include the Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army, Washington, DC; Commanding General of the U.S. Army Intelligence and Security Command at Fort Belvoir, VA; Director of Intelligence, United States Central Command, MacDill Air Force Base, FL.; and Deputy Director for Requirements, Capabilities, Assessments and Doctrine, J-2, for the Joint Chiefs of Staff. GEN Alexander has served in a variety of command assignments in Germany and the United States. These include tours as Commander of Border Field Office, 511th MI Battalion, 66th MI Group; 336th Army Security Agency Company, 525th MI Group; 204th MI Battalion; and 525th MI Brigade.

Additionally, GEN Alexander held key staff assignments as Deputy Director and Operations Officer, Army Intelligence Master Plan, for the Deputy Chief of Staff for Intelligence; S-3 and Executive Officer, 522nd MI Battalion, 2nd Armored Division; G-2 for the 1st Armored Division both in Germany and Operation DESERT SHIELD/DESERT STORM in Saudi Arabia.

GEN Alexander holds a Bachelor of Science degree from the U.S. Military Academy and a Master of Science degree in Business Administration from Boston University. He holds a Master of Science degree in Systems Technology (Electronic Warfare) and a Master of Science degree in Physics from the Naval Post Graduate School. He also holds a Master of Science degree in National Security Strategy from the National Defense University.

His military education includes the Armor Officer Basic Course, the Military Intelligence Officer Advanced Course, the U.S. Army Command and General Staff College, and the National War College.

His badges include the Senior Parachutist Badge, the Army Staff Identification Badge, and the Joint Chief of Staff Identification Badge.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

MARCH 16, 2011

RESPONSE TO QUESTION SUBMITTED BY MR. THORNBERRY

General ALEXANDER. In accordance with the requirements of Section 934, of the FY11 National Defense Authorization Act, the Office of the Secretary of Defense is drafting a report to Congress on the Cyber Warfare Policy of the Department of Defense. The department is currently coordinating the response to that reporting requirement to meet the extended July 1, 2011 report due date. [See page 12.]

RESPONSE TO QUESTION SUBMITTED BY MR. JOHNSON

Dr. MILLER. [The information referred to is classified and retained in the subcommittee files.] [See page 24.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 16, 2011

QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. What is the average cost of a breach in the Department of Defense for mission critical systems as measured in either dollars or degraded mission capability?

Dr. MILLER. [The information was not available at the time of printing.]

Mr. THORNBERRY. What do you estimate the overall loss for breaches is in the DoD or by Military Service element?

Dr. MILLER. [The information was not available at the time of printing.]

Mr. THORNBERRY. As outlined by the DOD's Strategic Management Plan, the DOD currently has a strategic performance goal to protect its IT infrastructure. The key measure of performance to meet that goal is the percentage of IT systems that are compliant with certification and accreditation processes. Considering the importance of this mission, shouldn't we have a more robust set of performance measures related to cyber? If so, what do you think those additional metrics should be.

Dr. MILLER. [The information was not available at the time of printing.]

Mr. THORNBERRY. How do Defense Support to Civil Authorities (DSCA) authorities in the DOD work in the realm of cyber?

Dr. MILLER. [The information was not available at the time of printing.]

Mr. THORNBERRY. What progress has U.S. Cyber Command and/or DOD made in developing a lexicon for cyberspace-related terms that can be used throughout DOD and across the federal government?

General ALEXANDER. Within the DoD, lexicons are strongly linked to doctrine. The Joint Staff J–7 authorized the development of cyberspace operations test doctrine, including a proposed cyber lexicon, in December of 2009. By April 2010, the J–7 published a draft of Joint Test Publication (JTP) 3–12, Cyberspace Operations. After an initial round of coordination, the Evaluation Draft of JTP 3–12 was released in September 2010 to be evaluated for effectiveness by use in exercises and operations.

Mr. THORNBERRY. How is U.S. Cyber Command working with the services and DOD to ensure that they have the right mix of military, civilian, and contractor personnel to conduct cyberspace operations?

General ALEXANDER. United States Cyber Command (USCYBERCOM) is a key contributor along with the Office of the Under Secretary of Defense, Policy, the Office of the Assistant Secretary of Defense (Network and Information Integration) and the Department of Defense (DoD) Chief Information Officer, the Services, and other partners within the DoD Cyber Community of Interest to finalize the Cyber Workforce Development Study in response to the Defense Planning Programming Guidance. The goal of this study is to assess the current and future DoD cyber workforce requirements (including DoD civilians, contractors, and active and reserve components). USCYBERCOM's focus in this effort is providing information on cyber work roles and training requirements. USCYBERCOM will continue engagement and provide recommendations for recruiting, training, and retaining the cyberspace workforce and associated resourcing requirements for implementation.

Mr. THORNBERRY. How do Defense Support to Civil Authorities (DSCA) authorities in the DOD work in the realm of cyber?

General ALEXANDER. Consistent with the authorities granted in Department of Defense (DoD) Directive 3025.dd, United States Cyber Command (USCYBERCOM) may provide Defense Support to Civil Authorities (DSCA) assistance as directed by the President or Secretary of Defense (SECDEF).

USCYBERCOM works closely with US Strategic Command and US Northern Command to answer any routine Requests for Assistance (RFA) from the Department of Homeland Security (DHS). A 26 Sept 2010 memorandum signed jointly by the Secretaries of Homeland Security and Defense solidified the support relationship between DoD and DHS making collaboration between the two departments official policy. It encourages information sharing and mutual support.

USCYBERCOM assistance may be technical assistance or recommendations for immediate defensive actions; similarly, they might entail recommendations for more systemic mitigation, such as improvements in network configurations and improvements in information assurance measures or best practices. Additionally, USCYBERCOM continually assesses the cyber threat to DoD's military networks

and information systems to ensure we are prepared to provide support to civil authorities in the event of a cyber threat to the nation's critical infrastructure. If a major cyber event struck the nation, however, SECDEF would determine the most appropriate combatant command to lead the DSCA effort.

Mr. THORNBERRY. DHS recently tested something called the National Cyber Incident Response Plan as part of CyberStorm III. Do you have any insight into how effective that plan was during the exercise? What should the interagency community, including DOD and the Intelligence Community, take from that plan?

General ALEXANDER. [The information referred to is classified and retained in the subcommittee files.]

Mr. THORNBERRY. What transition pathway courses of action do you envision for the DARPA National Cyber Range (NCR)? What role do you envision for CYBERCOM in that transition process?

General ALEXANDER. United States Cyber Command (USCYBERCOM) considers the National Cyber Range (NCR) as the prototype development portion to the larger Cyber Range Environment (CRE) initiative. DARPA is the NCR lead with prototype completion projected for mid-/late-FY12. Transition funding for FY13 and out-year sustainment are undetermined at this time.

Currently, there are three possible courses of action:

1) Once NCR prototype development is completed in FY12, provide adequate transition and sustainment funding and advocate integration into the larger CRE "whole of government" range that Department of Homeland Security (DHS), Industry and Department of Defense (DoD) could use for operational training and experimentation and testing of future technical architectures.

2) Complete NCR prototype development as scheduled in FY12, and operate as a stand-alone range for specific/limited DHS, Industry and DoD use for experimentation and testing.

3) Complete NCR prototype development, and offer technology/software tools to other existing DoD/Federal government ranges for reuse/integration without a transition or any sustainment program considerations.

USCYBERCOM's sees potential in this prototype effort, and envisions our role as providing support/operational expertise to DARPA with potential use cases, lessons learned, and possibly assist with technology transition under whichever course of action is chosen.

QUESTION SUBMITTED BY MR. RUPPERSBERGER

Mr. RUPPERSBERGER. U.S. Cyber Command was stood up at Fort Meade and reached full operational capability in the Fall of 2010. What do you expect to be the final footprint of CYBERCOM will be?

General ALEXANDER. With regard to the United States Cyber Command (USCYBERCOM) personnel footprint, the current planning projections for FY11 are approximately 1,404 military, civilian, and contractor personnel. The demographic for the personnel footprint includes 260 Officers, 204 Enlisted, 467 Civilians, 237 Contractors and 236 Augmentees. The USCYBERCOM footprint planning projections include space to support a ten percent increase in the staffing to support Combatant Commands, other government agency liaisons and integrated personnel as well as military reserve support. The National Security Agency (NSA) provides current facility support through existing owned and leased facilities. FY13 begins the military construction (MILCON) of the Integrated Cyber Center (ICC). This FY13 MILCON establishes USCYBERCOM's Joint Operations Center (JOC) and will accommodate the command's most critical cyber warriors.