[H.A.S.C. No. 111–179]

# U.S. CYBER COMMAND: ORGANIZING FOR CYBERSPACE OPERATIONS

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED ELEVENTH CONGRESS
SECOND SESSION

HEARING HELD
SEPTEMBER 23, 2010

U.S. GOVERNMENT PRINTING OFFICE
62–397 WASHINGTON : 2010

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.

HOUSE COMMITTEE ON ARMED SERVICES

ONE HUNDRED ELEVENTH CONGRESS

IKE SKELTON, Missouri, *Chairman*

JOHN SPRATT, South Carolina
SOLOMON P. ORTIZ, Texas
GENE TAYLOR, Mississippi
SILVESTRE REYES, Texas
VIC SNYDER, Arkansas
ADAM SMITH, Washington
LORETTA SANCHEZ, California
MIKE McINTYRE, North Carolina
ROBERT A. BRADY, Pennsylvania
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
MADELEINE Z. BORDALLO, Guam
BRAD ELLSWORTH, Indiana
CAROL SHEA-PORTER, New Hampshire
JOE COURTNEY, Connecticut
DAVID LOEBSACK, Iowa
JOE SESTAK, Pennsylvania
GABRIELLE GIFFORDS, Arizona
NIKI TSONGAS, Massachusetts
GLENN NYE, Virginia
CHELLIE PINGREE, Maine
LARRY KISSELL, North Carolina
MARTIN HEINRICH, New Mexico
FRANK M. KRATOVIL, Jr., Maryland
BOBBY BRIGHT, Alabama
SCOTT MURPHY, New York
WILLIAM L. OWENS, New York
JOHN GARAMENDI, California
MARK S. CRITZ, Pennsylvania
LEONARD L. BOSWELL, Iowa
DAN BOREN, Oklahoma
HANK JOHNSON, Georgia

HOWARD P. "BUCK" McKEON, California
ROSCOE G. BARTLETT, Maryland
MAC THORNBERRY, Texas
WALTER B. JONES, North Carolina
W. TODD AKIN, Missouri
J. RANDY FORBES, Virginia
JEFF MILLER, Florida
JOE WILSON, South Carolina
FRANK A. LoBIONDO, New Jersey
ROB BISHOP, Utah
MICHAEL TURNER, Ohio
JOHN KLINE, Minnesota
MIKE ROGERS, Alabama
TRENT FRANKS, Arizona
CATHY McMORRIS RODGERS, Washington
K. MICHAEL CONAWAY, Texas
DOUG LAMBORN, Colorado
ROB WITTMAN, Virginia
MARY FALLIN, Oklahoma
DUNCAN HUNTER, California
JOHN C. FLEMING, Louisiana
MIKE COFFMAN, Colorado
THOMAS J. ROONEY, Florida
TODD RUSSELL PLATTS, Pennsylvania
CHARLES K. DJOU, Hawaii

PAUL ARCANGELI, *Staff Director*
KEVIN GATES, *Professional Staff Member*
KARI BINGEN, *Professional Staff Member*
JEFF CULLEN, *Staff Assistant*

# CONTENTS

## CHRONOLOGICAL LIST OF HEARINGS

2010


Page

HEARING:

Thursday, September 23, 2010, U.S. Cyber Command: Organizing for Cyberspace Operations ..... 1

APPENDIX:

Thursday, September 23, 2010 ..... 25


**THURSDAY, SEPTEMBER 23, 2010**

**U.S. CYBER COMMAND: ORGANIZING FOR CYBERSPACE OPERATIONS**

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS


McKeon, Hon. Howard P. "Buck," a Representative from California, Ranking Member, Committee on Armed Services ..... 2

Skelton, Hon. Ike, a Representative from Missouri, Chairman, Committee on Armed Services ..... 1


WITNESSES


Alexander, Gen. Keith B., USA, Commander, U.S. Cyber Command ..... 3


APPENDIX


PREPARED STATEMENTS:

Alexander, Gen. Keith B. ..... 33

McKeon, Hon. Howard P. "Buck" ..... 31

Skelton, Hon. Ike ..... 29

DOCUMENTS SUBMITTED FOR THE RECORD:

[There were no Documents submitted.]

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING:

[There were no Questions submitted during the hearing.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING:

Mr. Miller ..... 49

Mr. Skelton ..... 47

Mr. Turner ..... 50

# U.S. CYBER COMMAND: ORGANIZING FOR CYBERSPACE OPERATIONS

---

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
*Washington, DC, Thursday, September 23, 2010.*

The committee met, pursuant to call, at 10:05 a.m., in room 2118, Rayburn House Office Building, Hon. Ike Skelton (chairman of the committee) presiding.

## OPENING STATEMENT OF HON. IKE SKELTON, A REPRESENTATIVE FROM MISSOURI, CHAIRMAN, COMMITTEE ON ARMED SERVICES

The CHAIRMAN. Good morning. We welcome you to our hearing today, a hearing on U.S. Cyber Command, organizing for cyberspace operations.

We will hear for the first time in this committee since Cyber Command was established from General Keith Alexander, the first commander of U.S. Cyber Command. He also continues to serve in his role as the director of National Security Agency [NSA].

General Alexander has had a long record of service to our Nation and is a genuinely nice person, to boot. I think perhaps the most important thing for the American people to learn from this hearing is that they have exactly the right person in charge of this new command. General Alexander is simply the best, though I will note that there are some other generals from his class at West Point who also haven't done too badly.

General Alexander, we certainly welcome you and thank you for your testimony today.

U.S. Cyber Command, or CYBERCOM as it has been called, has been tasked with conducting the full range of activities needed for the Department of Defense [DOD] to operate effectively in cyberspace. Of one thing I am confident: Cyberspace will be a big part of future warfare.

That means we can't afford to get this wrong. The establishment of CYBERCOM is a critical milestone for our Nation's defense. Cyberspace is an environment where distinctions and divisions between public and private, government and commercial, military and non-military are blurred. And while there are limits to what we can talk about in this open forum, the importance in this topic requires that we engage in this discussion in a very direct way and include the public.

The threats facing the Nation in cyberspace are daunting and have been underappreciated until recently. Just within the DOD, there are some—more than 15,000 different computer networks, in-

cluding 7 million computing devices on 4,000 military installations around the world.

These information systems face thousands of attacks a day from criminals, terrorist organizations, and more recently from more than 100 foreign intelligence organizations. DOD recently announced a new cyber strategy to deal with that burgeoning threat.

To understand how well prepared the Department of Defense is to handle the magnitude of the threat, we need to ask some fundamental questions. Where are we today with CYBERCOM? Where do we want to take it in the future? And do we have what we need to get there?

An additional challenge for this committee is determining how CYBERCOM fits into the broader national security effort. DOD has traditionally led the way in protecting information systems, so it is natural for CYBERCOM to play a role beyond just protecting military networks. What that role should be, however, needs very careful analysis.

We know that as a Nation we must do more to improve security in cyberspace and manage risk without choking off creativity or innovation.

And, General, we look forward to hearing your testimony today on how you intend to address these very, very important issues.

[The prepared statement of Mr. Skelton can be found in the Appendix on page 29.]

The CHAIRMAN. Now let me turn to my friend, my colleague, the gentleman from California, Mr. McKeon.

**STATEMENT OF HON. HOWARD P. "BUCK" MCKEON, A REPRESENTATIVE FROM CALIFORNIA, RANKING MEMBER, COMMITTEE ON ARMED SERVICES**

Mr. MCKEON. Thank you, Mr. Chairman. I want to thank you for holding today's hearing on Cyber Command and, General Alexander, for joining us today. And I would like to align myself with your remarks about how fortunate we are to have General Alexander as the first commander of Cyber Command and to have you in this place at this time. We are very fortunate. Thank you.

Cyber is an operational space that extends well beyond Internet searches and e-mail messages into a world of networking, interconnected systems, and pathways that can reach into individual components of critical weapons systems. The potential for harm from malicious activity reaches beyond the traditional military sphere of influence, as financial systems, critical domestic infrastructure—such as power and water treatment plants—and personal information all can be touched and disrupted through cyberspace.

With this in mind, I look with great anticipation to Cyber Command becoming fully operational next month. The Department of Defense in many ways has been at the leading edge of defending against malicious cyber activity and in understanding the problems and opportunities that cyberspace brings to our Nation. And I believe we have in General Keith Alexander the most appropriate person to lead this newly formed command under U.S. Strategic Command.

U.S. Cyber Command will be the touch-point for all things cyber within the department and will therefore carry a heavy burden. The services have built an infrastructure physical capability, as well as policies and processes, to handle the extensive activity that must be conducted in the cyber realm. Now General Alexander will have to ensure those efforts are brought under one vision and one mission, and it is nice to see that support group sitting right there behind you, all the services, everybody working together, because this is very, very important.

Now General Alexander will have to ensure those efforts are brought under one vision and one mission, with the goal of maintaining our military's ability to conduct its operations in cyberspace. Let there be no doubt: This space is contested and presents a persistent vulnerability for our military, civilian, and commercial infrastructures, especially as we increase our dependence on it.

As then-DNI [Director of National Intelligence] Dennis Blair commented on in testimony to the Senate Select Committee on Intelligence on February 2nd, we cannot be certain that our cyberspace infrastructure will remain available and reliable during a time of crisis.

In his recent Foreign Affairs opinion piece, Deputy Defense Secretary William Lynn also touched on the significant threat that exists in cyberspace. The department is under constant attack, and attacks will only increase in a crisis situation. Accordingly, the department must ensure the appropriate investments in technology infrastructure and people are being made and the appropriate authorities, processes, policies and organizations are in place to allow our Nation's military to meet today's challenges.

The establishment of Cyber Command meets an important step in strengthening the department's cyber capabilities. As confirmed in the 2010 Quadrennial Defense Review, the Pentagon needs both a centralized command for cyber operations and the development of a comprehensive approach to cyber operations.

Despite this progress, many questions remain as to how Cyber Command will meet such a broad mandate. Your testimony today therefore will help this committee understand Cyber Command's functions and how the department is mitigating its vulnerabilities in cyberspace.

Thank you for joining us. I look forward to your testimony.

I yield back, Mr. Chairman.

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

The CHAIRMAN. I thank the gentleman from California.

General Alexander, we recognize you for your statement. However, would you be kind enough to introduce the folks behind you, who as I understand head up the commands of each of the services? Would you do that first, please?

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

General ALEXANDER. Chairman Skelton, Ranking Member McKeon, absolutely.

Let me introduce the folks that we have. First, Vice Admiral Barry McCullough, a leader of 10th Fleet, Fleet Cyber Command.

It pains me to say this as an Army guy, but I will tell you that they are out front. He has done a superb job leading his unit, working with some of the COCOMs [Combatant Commands] in setting up the tactics, the techniques, procedures, doctrine of how we will fight. We, working as a team, have put together a joint task force looking at this, how we would, Cyber Command, support the combatant commands. He has led a lot of that effort, done absolutely superb. They are doing great.

We have Lieutenant General George Flynn, U.S. Marine Corps, leading MARFORCYBER, perhaps one of the best in leading some of the stuff and issues that we have in situation awareness and in doctrine. And since he has that in the Marine Corps, he can do both for us. Absolutely superb to have him.

Coming on board, Major General Rhett Hernandez on 1 October will take over U.S. Army Cyber. He is right now at the deputy ops, G3/5. We have had a number of conversations on the way forward. He understands the mission. He and Army Cyber are jumping forward. They have put together a unit, and I think that is making great, great headway.

Last but not least, Major General Dick Webber, Air Force Cyber, 24th Air Force. A couple of things that they have done. One, he has set up his command down at San Antonio, Texas, done a superb job, recently gone through an I.G. [Inspector General] inspection to see if they are ready for their full operational capability, did a great job on that, passed that by Air Force Space. They have great folks. I was down there a few weeks ago. They are doing a great job, absolutely superb.

I would tell you, Chairman, one of the great honors and privileges for being in this job is to have the team behind us working this together and working with NSA and the intel community, absolutely superb.

One of the—one of the things that I wanted to do was, first, thank you and the committee for the support in helping us stand up U.S. Cyber Command and the component commands. Like you, we see this as something critical to the Defense Department to help us direct the operations in defense of our networks.

And as you stated, this is a complex issue. We face severe threats. Those threats to our national security, in my opinion, are real. It is occupying much of our time and attention. At the unclassified level, we have stated that we see probes and scans to our networks that come up on the order of 200,000, 250,000 times an hour, and we have got to be prepared to meet those.

Our services in combatant commands depend on a command-and-control system, a computer system that has the integrity and reliability to operate in combat. We have the mission to help ensure that that happens.

As you mentioned, we are approaching our full operational capability. I will tell you that we have met many of the tasks that we set out to do. As we described last time, we have brought the Joint Task Force-Global Network Ops up to Fort Meade, repositioned the Joint Ops Center there at Fort Meade. It is operating today. That was part of the BRAC [Base Realignment and Closure] process. Now we have co-located them with the NSA Threat Operations

Center, and that is a great step forward. That was done and completed in May and has been operating ever since.

Some of the issues that we work with are the issues that I think you would expect us to do. First and foremost, how are we going to support the combatant commands? How are we going to defend this network in crisis? And those are the things that we are taking on first, establishing the tactics, the techniques and procedures for doing just that, and we are breaking this out, looking at the most significant threats first and ensuring that if something were to happen, we can take those threats on.

I did provide a written statement for the record. As you know, Chairman, I am not that good at reading. I am an Army officer, so I would ask that that be submitted.

The CHAIRMAN. Without objection, that will be part of the record. Thank you.

General ALEXANDER. I would—I would tell you that this is a work in progress, what we are doing at Cyber Command. This is going to take time for us to generate the force. If I were—if you were to ask me what is the biggest challenge that we currently face, it is generating the people that we need to do this mission.

We have about—we have our command stood up, our staff stood up, but the force is what we now have to rely on. The services are expanding that mission, going to 1,000 per year over the next few years, and I think we are headed in the right time. That is the biggest focus that we have, how we get that force generated, and the topic of discussion throughout the department. And I will tell you, rest assured, we know that that is important to get this done.

I see these remarks and this opportunity to start the dialogue, an open, transparent dialogue on what we are trying to do in Cyber Command to defend our Defense Department's networks against attack and to accomplish other missions that we would have as delegated to us to defend other networks throughout the government.

And, Mr. Chairman, I would pass it back to you.

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

The CHAIRMAN. I certainly thank the gentleman.

Mr. McKeon, gentleman from California.

Mr. MCKEON. Thank you, Mr. Chairman.

General, how do you see the Cyber Command improving the department's ability to provide a trained cyber force to ensure that service research and development investments, and procurement programs will provide a united, comprehensive approach to DOD cyber operations?

General ALEXANDER. Congressman, I think the key thing on this is to do it as a joint organization, so the standards are the same throughout—throughout the command. So bringing in—whether it is the tools we create or the students we put through there, doing it as a joint force with one standard is the key thing, and we have taken that approach, so our cyber training is at one school.

And if we have to go to multiple schools, it will be done with one standard. And I think that is what we need to do, so that you know, our combatant commanders know, the folks that are forward know that whether they get a soldier, Marine, airman or sailor,

that that person is trained to a standard and can accomplish the mission that is expected of them.

Mr. MCKEON. How does Cyber Command provide U.S. Strategic Command with a wider menu of strategic options? How do you respond to concerns that the alignment of defensive and offensive capabilities represents too much cyber capability resting in one command or within the Department of Defense? And why were these two functions placed under your command? What operational efficiencies were achieved by this alignment?

General ALEXANDER. That is a great question—question, Congressman. Let me—let me just drop back and go to the 2008. As you may recall, there was a significant problem on our networks that we discovered. At that time, we had the defense and the operations in one command, under the Joint Task Force-Global Network Operations. And that task force got one level of intelligence and could see one part of the network.

Operating on the other side was the Joint Functional Component Command-Net Warfare, trained at a different level with different intel insights at a different classification level, same network, two organizations. And if you are operating at the National Training Center, you wouldn't have the defensive team out there defending and then take them off the field and run out with an offensive team. It is the same team.

And so the good thing that we have done here is we have brought those two together, merged those, and I think that is key to the success here. We need that to operate as one team.

The offense and defense cannot be different here, because these operations will occur in real time. And I think we have to be prepared to do that. It is not time to say, oh, this is your mission and you are on your own.

It is also experience that we have seen in some of our red team and blue teams of what is happening in our networks. And I think that is a—a huge and a positive step and goes significantly towards providing better support to the COCOMs.

Mr. MCKEON. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Historically speaking, we, you, are ahead of those examples within the military, particularly the Army, at the creation of a new system. The beginning of the Army Air Corps was not fully appreciated or understood in its initial foray into the military.

I think the same can be true in transferring the cavalry into the tank corps. That was not fully appreciated. But I think we do appreciate this new challenge. And we are up to the task, it appears.

I would like to ask you, what do you need from Congress? It is our duty, as you know, under the Constitution to provide and raise and maintain the military. What do you need from us at the inception of your command, which will be a long and historic command, long after everyone in this room passes from sight? So what do you need to get you off to a good start, unlike the cavalry going into the tanks and that flying machine of yesteryear?

General ALEXANDER. Chairman, two things go through my mind when you say that. One, I hope that is a long time. And, two, some-

body offered me some great courses. Now I know what they were talking about.

With respect to—to cyberspace, I think there are two things that we need your continued support on. First, in terms of resources, we need the continued support of Congress and the resources that the department is putting forward for the component commands that we have here. It is going to have to grow. Each of them are looking at this and addressing that, and we will need your continued support to make that happen.

And the second is authorities. Right now, the White House is leading a discussion on what are the authorities needed, and how do we do this, and what will the team—the Defense Department and Cyber Command is a member of that team—how will that team operate to—to defend our country?

What they will look at across that is, what are the authorities? What do we have legally? And then, given that, what do we have to come back to Congress and reshape or mold for authorities to operate in cyberspace? We would solicit your support on that, when that is brought forward from the White House.

The CHAIRMAN. Would you please describe for all of us the threat environment as you see it? And I know that is a complex answer, but would you do your best to describe the threat environment that you face on a daily basis?

General ALEXANDER. In an unclassified forum, let me give you the threat in these three broad—broad areas. Going back over time, since the—the inception of the Internet, as it were, probably the key thing that we have seen is hacker activity and exploitation. That is where someone comes in and takes information from your computer, steals your credit card number, takes money out of your account. We have seen that go on, and that endures. And it is perhaps the most significant form of the threat that we see today, not just stealing our intellectual property, but also our secrets in other parts of our networks.

The concern, though, is if you go to 2007, Estonia was the first time that a nation-state was attacked in cyberspace. And so we see a shift from exploitation to actually using the Internet as a weapons platform to get another country to bend to the will of another country. While it is hard to attribute that to a nation-state, you can see it did happen when two nations were quarreling over political issues.

That followed, again, by more attacks in 2008 into Georgia. Those were disruptive. And let me describe disruptive. I have four daughters and 12 grandchildren, so you are driving the vehicle with all these kids in the back, and you are trying to talk to someone in the front seat, and they are all talking real loud. It happens occasionally. That is a disruption. When they finally quiet down, you can talk again.

A disruptive attack prevents you from doing your business for the time being, but is normally something that you can recover from and then go on and do your business.

What concerns me the most is destructive attacks that are coming. And we are concerned that those are the next things that we will see. And those are things that can destroy equipment, so it is not something that you recover from by just stopping the traffic. It

is something that breaks a computer or another automated device and, once broken, has to be replaced. That could cause tremendous damage.

In the department's concern, if that were to happen in a—in a war zone, that means our command-and-control system and other things suffer. We have got to be prepared for that, both from a defensive perspective and then to ensure that the enemy can't do it to us again, so full operational capability.

The CHAIRMAN. General, you have the four service commanders seated behind you, and thank you for introducing them a moment ago. Would you tell us how they are supposed to interact with your command?

General ALEXANDER. The way—the way we have worked this to date is to set this up in the following manner, our first—what I will call our first version 1.0. When we look at what is going on globally, if there is a global cyber action against our department, the question is, how are we going to organize our forces? And what we don't want to do is say, well, the Navy will do Navy, and the Army will do Army, and the Air Force will do Air Force.

What we have come up with is we need to set up a joint task force or, in this case, perhaps a joint cyber ops task force, and that cyber ops task force would work with Cyber Command, but go forward to work with the combatant command to present forces from all the services to meet in operational mission. And then let us train as a first step how each of those forces would do that, what we would do for PACOM [Pacific Command], CENTCOM [Central Command], EUCOM [European Command], SOUTHCOM [Southern Command], and NORTHCOM [Northern Command], if required.

So what we are trying to do is organize that as a joint force so that in each case you would have folks from each of the services supporting that. Rather than having three services providing that to a combatant command, have it one, a cyber task force.

You—many make an analogy similar to the way SOF forces are presented, special ops forces are presented. I think that is a close analogy and probably something that we will get to. So that is how we are organizing it. And now what we are doing is working with the combatant commands on specific plans to see, do we have the force structure to meet what you would require in that plan? And if not, what force structure do we need? And use those force structure requirements to drive the growth that we would have in each of our components.

So that is a long-winded answer to get to it, but it is organizing in a joint force to accomplish those missions. I think that is the best thing for the department and our Nation.

The CHAIRMAN. Thank you.

Mr. Ortiz.

Mr. ORTIZ. Thank you, Mr. Chairman.

And thank you so much for—for what you do to keep our country safe and strong.

I mean, this seems to be like you have got to get very skilled people to work for you. I mean, how do you recruit them or how do you train them before you get them to work for you? And do you feel that you have enough staff to do what you have to do?

And my next question would be, I mean, if they were to disrupt and conduct an attack where you lose all kinds of communication, is there any way for a backup system?

General ALEXANDER. Let me answer this, first, with the recruit, train, and I will just add in retain. I think this is one of the key issues that we are looking at right now: What is the—if you will—the calculus for retaining this high-end talent?

Well, when we send them through school, they go for two years. It would be my preference that they don't cycle through their jobs as we would normally do in the military, but keep them in place longer.

My initial assessment is all the service chiefs and combatant commands see it similarly. We are going to need to keep people in place longer and to retain them. We are getting a lot of good folks. You know, I will tell you, it is a privilege and honor to see the great folks that we are getting in there. The key is, how do we retain them? Because everybody wants good people.

And so I think the bonus systems and other things are ones that we have to look at. That is yet to be done to ensure that we retain that right force.

Enough staff, I think we have enough staff. I think the staffs are, at least for right now, the right size. I think that first priority, grow the cyber force and cyber operators, make sure we have enough to meet those emerging combatant commander requirements. So I would focus on getting the forces that we need, then come back and re-address the staff one more time later, but I think we have got enough.

Now, hopefully my staff is not tuned into that right now, but I think that is true.

And your last question was, if they conduct an attack on us in cyberspace, do we have a backup system? So there are things that we have to look at in that area, whether it is a backup system or other options that—that would allow us the agility to maintain our command and control are things that we have to look at.

We are looking at those. We are coming up with, I think, some tremendously innovative things that I would prefer not to put out here right now, but I think it will provide exactly what you are asking for, that kind of agility for the command and control of our forces abroad.

Mr. ORTIZ. I know there is a lot of Members here, and I don't want to take too much time to allow other Members to ask questions. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Mr. Conaway.

Mr. CONAWAY. Thank you, Mr. Chairman.

The—in the open source press, a major disruption drove a task force—a deal called Operation Buckshot Yankee. Can you visit with us a little bit about what that was and what impact it had on the way you looked at the plans that you had in place up until that point in time when that happened?

General ALEXANDER. Thank you, Congressman. Yes, Operation Buckshot Yankee, a foreign adversary using an air gap jumping tool, had gotten some malicious software on to our classified networks.

Mr. CONAWAY. Would——

General ALEXANDER. The way that happens is, if you use a thumb drive or other removable media on an unclassified system, the malware would get on that removable media, ride that removable media over to the other system. And so think of it as a man in a loop wire, and so a person could be taking information they needed from an unclassified system, putting it onto a classified system, and so that software would ride that removable media and go back and forth.

It was detected by some of our network folks within the advanced network ops, our information assurance division at NSA. When we brought that forward, it caused a couple things to happen.

As I mentioned earlier, first, it became clear that we needed to bring together the offense and defense capabilities. And so Global Network Ops was put—Joint Task Force-Global Network Ops was put under my operational control in—within a month of that happening. And I think that started to change the way we look at this.

And then the Secretary of Defense set in motion the next step, which was to set up Cyber Command as a sub-unified command. And I think both of those are the right things to do. What it does is it gets greater synergy between those who are defending the networks and what they see and those that are operating in the networks abroad and what they see and bringing that together for the benefit of our defense. I think that is exactly what the Nation would expect of us.

Mr. CONAWAY. Okay. And you used the phrase air gap. That is the thumb drive that was——

General ALEXANDER. Right. So when a thumb drive goes from one computer, and when it is unplugged, now we call that the air. And then when it gets plugged in——

Mr. CONAWAY. Okay. Talk to us a little bit about your—the dual hats you wear, Cyber Command and heading—still heading NSA. I suspect I know what you—the end is—but can you walk us through how you are going to make sure both get your undivided attention?

General ALEXANDER. Yes. Well, I—well, I guess the initial quip was, I will work twice as hard. But the reality is, in cyberspace, that is—that is where NSA operates and has tremendous technical expertise. It has our Nation's expertise for crypto-mathematicians, for access, for linguists, for everything that you would need to operate in cyberspace.

And what the Secretary said is, we can't afford to replicate the hundreds of billions of dollars that we put into NSA to do another for Cyber Command and then another perhaps for DHS [Department of Homeland Security] and others. Let us leverage what we have and bring that together.

And so by bringing these two together, we have actually accomplished that goal. Now, they—they have and operate under separate staffs and under different authorities, as you know. And so under the Cyber Command, the thing that has helped, I always had, since I have been the director of NSA, the additional duty as the Joint Functional Component Command-Net Warfare, so I had

that job. What I didn't have was the staff, the—the horsepower and the staff that I have now, so actually that helps us.

And I think you can see the momentum picking up with that staff and the staffs of the folks behind us. When you bring this much talent to the problem, we are going to make progress, and we are. So I think that is a very good value added.

And I will tell you another thing. We have two great deputies. The NSA deputy, Chris Inglis, is one of the best people I have ever worked with. And on the cyber side, we have now Lieutenant General Bob Schmidle, Rooster, absolutely the same type person, just extremely competent, great to work with, a team player. And together they are forming the right team, and I think our Nation will benefit from that.

Mr. CONAWAY. Thank you for that. Let me follow up on—a little bit of what Solomon was saying. Our enemy for the most part is, you know, 14- to 25-year-old, you know, really bright folks who are off the reservation. To counter those, can you, in fact, attract and do the standards of personal conduct, background, and everything else that you have to have in order to allow them access to our secrets? Are there enough folks out there who are not tainted by, you know, previous conduct that you can still get into the system so we can take advantage of them and they can man these slots that you are forming?

General ALEXANDER. We are having great success to date, that if the economy were to pick up, that might change that calculus. But right now, we have great success in hiring, great outreach. We are getting great people.

In fact, on the NSA side, one of our positions, we had 800 applicants. And, you know, so when you look at that—so we are getting a great number of folks.

I think the real key goes back to an earlier question. So once you got those great people, now you are going to say, so how do you keep them? And I think it is by the job we do, by the leadership of the folks behind us, and how they lead and train those and the missions that we have.

If it is exciting, you know they will stay. And if we pay them right and take care of them, I think we will keep these folks.

Mr. CONAWAY. Thank you, Mr. Chairman. Yield back.

The CHAIRMAN. Mr. Taylor, please.

Mr. Taylor has asked that Mr. Kissell be called upon in his stead.

Mr. Kissell.

Mr. KISSELL. Thank you, Mr. Chairman. I thank the gentleman from Mississippi for yielding.

And, General, thank you and your staff for being here today. It is a very important issue. And I want to follow up the question a little bit more to what my colleagues have already asked about the recruitment of personnel.

In the recruiting of people to come in and be part of your staff, do they then work as civilians and not—not traditional military?

General ALEXANDER. We have a combination of both military and civilian.

Mr. KISSELL. Okay. And—and—and taking that a little bit further, how do we test our system in terms of bringing people in

and—and having self-inflicted attacks? How do we figure out, you know, where we think we are safe and by bringing people in to test it and—and having somebody who is capable to come in and test that type system?

General ALEXANDER. That is the great part, Congressman, about bringing together that offense with defense. The red teams, our red teams, our advanced network ops, are constantly doing that, hunting, checking our networks. It is something that we are going to have to grow.

I think one of the key things that we have put on the table is what I will call hunting on our networks for adversaries that are there. You are always going to have to do it. And that creates it from a more static capability to a more dynamic, because you are actually looking for something that is going on.

And, for example, if you had a bank and we set up a perimeter defense and then left every night, and every morning once a week we would see they got in there, so we keep changing the defense, that would be static. But now if we had a roving guard there waiting for people, trying to stop them, that would be more like the active defense that we are looking at in the future. I think we have got to do both.

Mr. KISSELL. And we know that the civilian side of cyber defense is—is—is certainly not what we have in the military. How does that affect your efforts to compensate for, to—to get around whatever the situation may be, the inadequacies in the civilian side? What does that mean for you guys?

General ALEXANDER. Well, we depend on many of those civilian networks and infrastructure for department operations, especially in crisis. And so our partnership with homeland security and others to help work that is a key issue that we are working with the Department of Homeland Security.

I think that—that team and partnership is growing. We need to keep pushing that forward, because some of those networks, those capabilities have to be there in crisis for our country.

Mr. KISSELL. What about outside of government? You say industry—the greater civilian world. Does their—their lack of defenses in so many places, does that hamper what you are doing? Or is this something you work around?

General ALEXANDER. Well, I think there are two—two parts to that. One is, I think industry also recognized the issues here and are trying to step forward, but we have to partner with industry, and I think it has to be a partnership. I think DHS has to be in that construct of that partnership.

The reason, much of the infrastructure that we have is owned by industry, that we operate on is owned by industry, and they have tremendous technical talent. We have to bring those together with what the government knows from a threat perspective and the tactics, techniques and procedures that we develop for operations.

And we have to bring both of those together and ensure that those are right. That is part of the discussion that is ongoing right now that will eventually result in, "Here is how the team will operate," that would result in the request for authorities that I think the White House will—is working now to bring forward.

Mr. KISSELL. Thank you, sir.

And thank you once again to the gentleman from Mississippi.

And thank you, Mr. Chairman.

The CHAIRMAN. Mr. Coffman, please.

Mr. COFFMAN. Thank you, Mr. Chairman.

I am—I am wondering, General, if you could review for us just for a minute—you mentioned 2007, the—the first cyber attack on Estonia. Where did that come from? What were the ramifications of that, that attack, in terms of the disruption?

General ALEXANDER. Absolutely. It is in open press, a lot of this, so I will give you the gist of it. And I know the—the reporters will get this more accurate.

But in May of 2007, there was a Russian statue that the Estonians were going to take down, a big political discussion between Estonia and Russia. Hacktivists from Russia appeared to attack it, and from around the world different computers were brought into play to send spam e-mail, a distributed denial-of-service attack, on much of the government of Estonia's infrastructure, making it almost impossible for their banks to do business internally and, for sure, externally to Estonia caused tremendous damage and has resulted in them building a cyber capability themselves.

So a huge problem, and it was all around that political issue. Attribution, saying specifically was this caused by one nation-state or another is difficult and not something that we have.

Mr. COFFMAN. Okay, thank you, General. The—how would you—in terms of the threat assessment—and I think you have described what the—what the tactical measures are, in terms of threatening our infrastructure. But could you, in terms of evaluating the peer competitors of the United States, in terms of their threats in cyberspace, how would you evaluate them? Let us say China, Russia. Who are the peer competitors of the United States that threaten us—that potentially would threaten us?

General ALEXANDER. That is a great question, Congressman, because in cyberspace, it is not so much necessarily the—the size of the country as it is the idea of the person who is creating the software.

I think there are a number of countries out there that are near peers to us in cyberspace, and hence the concern. This is an area that—that others can have an asymmetric capability and advantage.

And there are two parts to that question, if I could just add an extension to it, is, first, we think about nation-states, but just given that part of the discussion, the non-nation-state actors are also a concern. And then if you look in this, in this area, when people create tools, cyber tools, the unintentional distribution of some of those tools can cause the most problems. We have got to be prepared for all of that, for these nations that are out there.

And we are not the only smart people in this area. There are others that are just as capable of us and in some areas perhaps more capable. And so we have to ensure across that board that we cover that spectrum. China, Russia, and you can just go around the world and pick—most of the modern nations have capabilities that I think many could argue are near to us and in some areas may exceed our capabilities.

Mr. COFFMAN. General, who—who would exceed our capabilities?

General ALEXANDER. Well, it depends on the area. So if you were to—if you were to build a—a—a whole suite of tools—and if you go back to the 1950s, you know, it was a discussion about the different capabilities of us versus Russia, Russia had power capabilities over us in some areas, actual electrical power and the development of power engines and some capabilities, and we had it in perhaps the computer and some other areas.

We are going to see in the tools, the development of tools, one country may be the best at developing worms or viruses. Another may be the best at developing tools for exploitation that are stealthy. We don't see them. Another country may be the best at developing tools that can attack certain specific systems, because they see that as in their national interest.

And so our concern, my concern in answering this—and I think what we as a Nation have to look at, is you have to cover that whole spectrum to protect our country. And so what we have to do is—we are not going to be—we have to recognize that, first, there are other smart people out there, and that is why we have got to take this so serious. It is an asymmetric advantage that some could have over us, and we have got to put that defense up.

Mr. COFFMAN. Thank you.

Mr. Chairman, I yield back.

The CHAIRMAN. I thank the gentleman.

Mr. Reyes, please.

Mr. REYES. Thank you, Mr. Chairman.

General, good to see you, and thank you for the work that you are doing in this very critical area. I think it is—it is great news that we are getting the kind of talent that we know we are able to attract, and certainly getting 800 applicants for the position that you referenced is good news.

But I have got—the—the question I have is, you are dependent on all the services to provide you the personnel with these skills. And I am just curious, do you—do you think that all the services are—I guess, first of all, at the same level, in terms of attracting and providing for opportunities as a career in cyber, for—for their respective personnel? Do you think they are all at the same level?

And the second thing is, are there any concerns that you have—since you are dependent on them—that you have—you have expressed to the other services about this issue? It seems to me you are—you are dependent on their ability to give you that kind of support.

General ALEXANDER. I am optimistic that we will get the force that we need. We are pushing on the services to go faster to bring those forces in. And the issues that we have talked about—how do you not only recruit some of these, but how do you retain them? And in what—in what mix do you bring them in? Are they all military? Are they military-civilian? How do we add those mixes in? And how do they complement other actors that we have within NSA, the I.C. [Intelligence Community], and other elements of DHS, as an example? How do we bring all that together, are parts of the discussion.

If I were to tell you my greatest concern, it is moving fast enough to provide a capability to defend our networks in time if a crisis were to occur. We see that as our number-one mission: Be ready.

And right now, we—we have to build that force to get there. That is going to take some time. We have some force structure. The services have leaned forward on that. They are presenting some capabilities. We are moving down that road.

It doesn't—you don't instantly create a cyber actor or a cyber operator. It takes time. Some of the training programs go 18 months. And so even if we had 100 or 1,000 more today, we would want to send those through training.

Some of the discussions the service chiefs have had with me is, can we do on-the-job training for some of these folks that are pretty smart, put them in this area, and give us an increased capacity earlier, and then send them to a training program, a formal training program as we bring in others? We have got to look at all of that.

Mr. REYES. In the context of the threats that you just mentioned, we are focused mostly on attacks from other countries on our—through the—via the Internet. I am concerned, given the case of Private Manning and—and the WikiLeaks case, as well, about attacks within, you know—in other words, people that have access to our systems that deliberately either steal information from our secure systems or, in some cases, may be enemy agents that have access to them.

What—are you concerned about that? What are—what are we doing about that? And how can we—what can we do to minimize those kinds of concerns?

General ALEXANDER. Congressman, I am—I am concerned about it. It is an issue. I do think we have some ideas on how to address that, some of which we have already implemented, some that will need to be implemented as we transition to a new architecture. I think both of those will help address that problem.

There is always going to be concern about an inside actor and, I would just add to it, supply-chain issues. Both of those are going to be key things that we are going to have to look at. Knowing that those are issues will help us in the development and planning of our future systems, and I think we have got to address those with our eyes wide open.

It is always going to be a problem. There are things that we can do to mitigate it. We will never solve that 100 percent.

Mr. REYES. Thank you. Thank you, General.

Thank you, Mr. Chairman.

The CHAIRMAN. I thank the gentleman from Texas.

Mr. Wilson, please.

Mr. WILSON. Thank you, Mr. Chairman.

And, General, thank you very much for your service. I am very grateful that our colleague, Congressman Roscoe Bartlett of Maryland, for years has raised the concerns about cyber warfare and how this could affect the American people. And I appreciate your efforts to protect the American people.

Throughout my time in Congress and as the ranking member of the Military Personnel Subcommittee, I have had the opportunity to meet and hear from many wounded veterans. Many are eager to return to the fight. It seems to me it would be in the best interests of the Department of Defense to retain these individuals and their knowledge and their experience.

With that said, are there any efforts being made to retrain wounded warriors within the Cyber Command? If not, would that be a potential option?

General ALEXANDER. We do have within the services and within NSA a program to—to hire the wounded warriors, and we have brought some onboard that are operating either in this or one capacity or the other. That is a great point.

I would just like to emphasize, we can use these soldiers, sailors, airmen and Marines. They have tremendous capability, and they present a credible operator for the rest of the folks to see. So it is a huge step forward. And we have brought a number on board.

I think we could do more on that. We need to work with the services on that, and we are.

Mr. WILSON. And I have seen it firsthand. I was visiting at Landstuhl, and a young lady had lost both legs. And her—within 48 hours, her comments were, "I want to be back with my buddies." And so people do want to serve. And so I can see what you are doing is giving a great opportunity for very talented people who want to serve our country.

There has been concern of personal liberties and privacy being compromised with regard to cybersecurity. As a command, what will you do from a process perspective, as well as technological perspective, to ensure privacy and civil liberties are protected? Is there anything Congress can do to assist you in your efforts?

General ALEXANDER. That is a great question. Thank you, Congressman, because I think two parts to this. One, we have a responsibility to protect the civil liberties and privacy of the American people and of our people. That is non-negotiable. Constitution, that is what we are there for. We have to do that.

Now, there are two issues with this. One, transparency. What can we do to show you, Congress as an oversight body, what we are doing and the American people? And, two, how do we also help ensure that what they understand is accurate?

Because a lot of people bring up privacy and civil liberties. And then you say, well, what specifically are you concerned about? And they say, well, privacy and civil liberties.

So is this system—are you concerned that the anti-virus program that McAfee runs invades your privacy or civil liberties? And then answer is no, no, no, but I am worried that you would. And so now we are—so let us explain what we are trying to do to protect the department's systems.

And I think that is where Congress, the administration, the department can work together to ensure that the American people understand exactly what we are doing and how we are doing it. That is part of the transparency that I think needs to be put on the table.

What we can't do, we can't say, "Here is a specific threat that we are defend against and how we are defending against it," because the adversary within three days would be able to work around it. So it is those—those two things. That is a very important issue, I think, that we have to confront now and fix.

Mr. WILSON. And for the health and safety of the American people, such as electrical grids, you mentioned the banking, commerce system of Estonia, all of this is—is so important.

A final question. Your activities fall under Intelligence Title 50, Attack Title 10, and Law Enforcement Title 18. How do you balance these legal authorities?

General ALEXANDER. Well, for the—for the Title 10, they operate under the CYBERCOM hand. Cyber Command operates under Title 10 authorities to this committee, the House Armed Services Committee.

NSA, we operate under Title 50, intelligence authorities under the House Permanent Select Committee for Intelligence, and we have in our staffs the legal teams to ensure that we do these exactly right. And so any operations that Cyber Command does, defensively we have the standing rules of engagement laid out there, and any other operations that we would do would have to be done under an execute order through the Secretary of Defense to the President.

Mr. WILSON. And—and, again, thank you very much for your service and commitment to our country.

And I yield the balance of my time.

The CHAIRMAN. I thank the gentleman.

Mr. Critz, please.

Mr. CRITZ. Thank you, Mr. Chairman.

And thank you, General, for being here. Fortunately, in my part of the world, in western Pennsylvania, we have Carnegie Mellon University, and they have the CyLab, and they do a lot in cybersecurity. And we have been talking about this quite a bit.

And one of—one of the issues that seems to come up—and it seems like you have explained it—within the military, that we can be stovepiped in how we accomplish or how we do things. And it is good to see the different services working together, but I would be curious to hear how you are partnering or how you are working with not only private industry, but with the educational institutions out there that have expertise so that we are working cohesively, because I would assume that many of the threats are very similar.

General ALEXANDER. That is a great—a great question, because the universities, academic institutions, labs, industry are key partners in all of this, and we do have to reach out. And we reach out in a couple of ways.

As you may know, from an information assurance side, both we, NSA, Department of Homeland Security, and the department run a program, an education program that helps the universities. Here is a set of criteria for getting an information assurance degree, and we work with those universities, over 100 now, in doing that. I think that is absolutely the right thing to do.

And as we said earlier, we are not the only smart people in this area. In fact, many of us would argue, heck, our industry partners have tremendous capability, so partnerships with them makes a lot of sense. And setting up groups—and this is where Howard Schmidt, the White House coordinator, comes in and Homeland Security to bring these teams together. I think that is crucial, bringing all of the players together, industry, academia, and government, to solve these problems.

Mr. CRITZ. Well, thank you—thank you very much. And you mentioned about the 250,000 attacks per hour. I think that was the

number you used. And certainly that happens in industry, as well. In fact, some statistics show that patches to anti-virus can be re-engineered or reverse-engineered within moments, actually, as the patches come on board, so it is a major issue.

You mentioned about the—the thumb drives, how they carry viruses around, and certainly it is an educational process.

I have noticed, or have read about a culture shift that has been mentioned within the military. And I would be curious to hear your—your description of this culture shift and what it—what it really means.

General ALEXANDER. So we—we actually hit three parts that came out of that Operation Buckshot Yankee: culture, conduct and capability. On the culture side, it was getting commanders to understand this is commander's business. This isn't something that you say, "I am going to have one of my staff run." This is commander's business.

Commanders are responsible for the operation of their command, and this operational network is important to them. So the big jump first part was commanders have a responsibility.

The second part is understanding the responsibility to actually conduct the patches that you brought up, because if you don't fix the patches, as you rightly stated, an adversary sees a problem, within minutes of that problem being out there, they have a way to hit a system with that vulnerability that we are trying to patch.

If you haven't done the patch, you have a vulnerability that somebody will probably exploit. And if you don't do those patches on time, you risk not only your system, but the whole network. So getting those right and ensuring that commanders know that it is their business to do that, that has been the greatest cultural things that we have pushed forward in the military. Tremendous—tremendous jumps in from where we were two years ago to where we are today.

Mr. CRITZ. Well, thank you. And my final question is—you know, how can the Department of Defense be more proactive, rather than reactive, in the dot-mil domain mode of cyber defense, by incorporating the assurance, the resilience, and the performance?

General ALEXANDER. I think—I think the first step is, we have to look at the way we do business and the way our networks operate and, like industry, take that construct and see if there isn't a better model, a more efficient, a more defensible model, something that would be harder for our adversaries to penetrate, and that would provide equal or better command and control.

It is coming in the commercial side. You can see this with your iPad, your iPhones, the new technology, computing on the edge, all these things, cloud computing. Now we need to look at that. Is there opportunities now for the department and the government to use in creating more secure networks? Industry, academia, and government are all looking at this. We have got partners at all of those helping.

Mr. CRITZ. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Mr. McKeon, please.

Mr. MCKEON. Thank you, Mr. Chairman.

General, does Cyber Command have the mandate to support General Petraeus in Afghanistan by denying and disrupting Al Qaeda and the Taliban's use of cyberspace? Do you have the necessary authorities to carry out this function?

General ALEXANDER. We have actually deployed an expeditionary cyber support element to Afghanistan to support General Petraeus. I did not want him to beat me up for not doing that.

And we have a responsibility to help them protect their networks, the Afghan Mission Networks. We are working as part of a joint team—because the services actually will implement that—we are ensuring that the capabilities put into that network are defensible in helping to set that up.

We are not where we need to be in terms of setting all the things in place, but we have come a long ways. And I think we are making progress in that area.

If you were to ask what is the—the real issue that—that we need to address, it is ensuring that the evolving Afghan Mission Network is defensible, up and—up and operating, because it is going to cover a number of countries that are in Afghanistan.

Mr. MCKEON. Thank you.

The CHAIRMAN. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

General, welcome. Thank you for your great service to our Nation, your presence today. Again, you have had an outstanding career, and I look forward to supporting you in your new role as head of Cyber Command.

Cybersecurity, as you know, has been both a personal and professional interest of mine for—for several years now. Since serving as chairman of the Homeland Security Subcommittee with jurisdiction over cybersecurity, I have certainly paid very close attention to the cyber threats that are facing our government, our military and our citizens, and the vulnerabilities that have yet to be addressed.

I was certainly pleased to include an amendment in the fiscal year 2011 Defense Authorization Act that would enhance our efforts to secure our Federal networks and coordinate U.S. resources. And I certainly strongly support the department's moves right now to coordinate its efforts under your new command, and I believe that they found a real expert to lead this new initiative. And, again, I look forward to supporting you in your work.

General, I want to ask you a direct question. If we—the Nation were to endure a major cyber attack right now, could you defend the Nation against that attack? Do you have the authorities to defend the Nation against that attack? Obviously, we are talking about the whole of our—our cyber critical infrastructure.

As I have said—I know—because the President in his major address on cybersecurity, the first major world leader to—to make a major address on cybersecurity, said that our—our cyber assets, our critical national asset—will defend and use all assets of national power to defend it.

But my question is, again, to you. Could you defend the Nation right now against a major cyber attack? Do you have the authorities that you need?

General ALEXANDER. First, Congressman, thanks for your great support in all the cyber areas and all that you have done over the past years on this. It is been tremendous, and we appreciate it.

To answer your question directly, it is not my mission to defend today the entire Nation. Our mission in Cyber Command is to defend the Defense Department networks. And as if we are tasked by either the Secretary or the President to defend those networks, then we would have to put in place the capabilities to do that. But today, we could not.

Mr. LANGEVIN. And what would you need to do that, General?

General ALEXANDER. I think this is what the White House, Congressman, is actually looking at, is how do you form the team to do the mission that you are—that you have put on the table? How do we develop the team between Department of Homeland Security, FBI [Federal Bureau of Investigations], Cyber Command, and others to work as a team to defend the Nation in cyberspace?

And in that, what are the roles and responsibility of each member in that team? And then let us walk through in a war game—my words—how that would work? And ensure that everybody has the exact authorities and capability to do what needs to be done to protect the country.

Those are the steps that we are going through. It is under the leadership of the White House right now. Howard Schmidt and his folks are leading that to look at this. We get to participate in that, to put forward our ideas on how the country could be protected, specifically the government, the government networks, and what I will call critical infrastructure.

Mr. LANGEVIN. Well, let me press you a little bit more. If America, in fact, experienced a serious high-profile attack today against our critical infrastructure, perhaps our power grid, banking sector, or transportation, what are the rules for self-defense in cyberspace? And can you walk us through how such an attack would occur? And how would the U.S. Government work to stop it and ensure the security of our citizens?

General ALEXANDER. That is a great question. Okay, to be very direct on it, if an attack were to go against the power grids right now, the defense of that would rely heavily on commercial industry to protect it. If commercial industry had the signatures and the—and the capabilities in place to weed out that attack, then they would be successful.

The issue that you are really getting to is, what happens when an attacker comes in with an unknown capability? That unknown capability would have the ability to shut down either the banks or the power grid if it got through.

So to defend against that, we need to come up with a more, in my terms, a more dynamic or active defense that puts into place those capabilities that we would need to defend in a crisis.

That is what we are working right now in the department to do to ensure that that works and working, actually, closely with Department of Homeland Security and the White House to show how that could be done. And they are looking at that as a model to put in place and now trying to ensure that they have the authority to do that, looking at how that would all be created. And if they don't have, I think that is what they would bring forward to you.

Mr. LANGEVIN. Well, General, thank you. I know my time has run out, but these are the things that keep me up, at least. And I am very concerned about potential threats in the cyber realm facing our Nation. And I—I look forward to working with you on addressing these—these important challenges. Thank you.

The CHAIRMAN. I thank the gentleman.

Let me—let me ask this question before I call on Mr. Boswell. General, where are each of the four sub-commands physically located?

General ALEXANDER. Right now, three are at Fort Meade—or at least major portions of them are at Fort Meade. One, Air Force, is at San Antonio, Texas, collocated with San Antonio, Texas, and it will have a beachhead at Fort Meade. So I think they are all in that enterprise that allows us that capability to touch both the NSA portion and work together as an effective team.

The CHAIRMAN. Thank you.

Mr. Boswell.

Mr. BOSWELL. Thank you, Mr. Chairman. Just very short.

Good to see you again, General. Appreciate your work very much. If you have done it, why, I will just check the notes, but I got here late, but could you tie on the DNI, how they fit into this—I know as NSA you report to DNI. Tie this together for us.

General ALEXANDER. All right. NSA has a direct report to the DNI for operational intelligence means. And we do that. The DNI oversees all the threat-related collection that goes on in cyberspace, as you would expect.

General Clapper, Jim Clapper, the director of—now for DNI, absolutely in sync with where the department's going and has been a huge advocate and candidate for helping put this together, absolutely superb. I think that is going to continue to go well. I think we are building those right pieces together.

They understand and I understand the responsibilities that I have under the Title 50, back to the Intel Committee, and under Title 10, back to this committee. And I think all of those understand it, too, and know that we are—we are doing those right.

I think—I think, if I could, one of the things that this gets to, this question that you bring up that is so important for our country—note that we couldn't replicate the NSA capabilities. And so leveraging them is going to be hugely important.

And now, ensuring that we leverage them properly, that we need the civil liberties and privacy—and that we are transparent, those are going to be the keys, and where we have got to come back to you and show you how we are doing that.

Mr. BOSWELL. I appreciate that. I also—we all appreciate the investment we got in NSA, and we can't duplicate it, so that leveraging, I think, is extremely important. There is a lot of—a lot of need there, and it is—it is kind of the frontier right now, as we all know. So I wish you well and thank you for your dedication, and I appreciate those strong words you said about the in-depth you have got in the two staffs. We wish you well. And we will do our best to be helpful. Thank you.

General ALEXANDER. Thank you, sir.

Mr. BOSWELL. I yield back.

The CHAIRMAN. I thank the gentleman.

Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Speaker—I mean, Mr. Chairman, and thank you, General Alexander, for your appearance today.

I wanted—communications, logistics and intelligence operations conducted by the Department of Defense are to some extent reliant upon the public Internet. Is that true?

General ALEXANDER. Absolutely, Congressman.

Mr. JOHNSON. And could we fight a war effectively were the public Internet to fail or be compromised?

General ALEXANDER. Well, that would be very difficult. Those specific networks that we depend on were not protected, so I would put those in that category of critical infrastructure, myself.

Mr. JOHNSON. Could we fight a war in the event the global information grid were substantially or wholly compromised?

General ALEXANDER. If it is compromised, I think we could—we could fight a war. If it were destroyed, that is a different issue. And now we would—we would be back to many years ago, and we would have to look back, because much of our command and control, much of our intelligence depends on that network operating.

Mr. JOHNSON. Do we have a specific contingency plan in the event that that happens?

General ALEXANDER. That is one of the missions that we are looking at, is how do we do that? And the I.T. [Information Technology] architecture that I described earlier, one of the things that we are looking at is, how do we get that agility and flexibility to operate in those degraded environments? It is something we have got to do.

Mr. JOHNSON. Are you satisfied that the various agencies and interagency councils responsible for U.S. cybersecurity, some of which have overlapping jurisdictions or areas of focus, are arranged such that you can do your job efficiently and effectively?

General ALEXANDER. Well, I think with any new area, Congressman, you are going to have differences of opinion. I think that is a good thing. The team is coming together good. Now that we have Howard Schmidt on board as the White House coordinator, I think we are getting more folks and faster movement within the interagency.

And it goes back to a couple of the earlier questions. We do have to resolve some of these. The White House is working that right now to say, whose mission is it to do which part of this? And do we have that all right? And do you have the capabilities and authorities to do that?

Mr. JOHNSON. Yes, we have—we have seen where in our intelligence-gathering apparatus there has been silos, I guess, built and the information does not flow freely or as freely as—as we would like. And that certainly would be—not be a model that we would want to adopt when it comes to cybersecurity issues. Would you agree?

General ALEXANDER. I agree. I think it needs to be a team.

Mr. JOHNSON. Are there any structural changes that you think may accommodate that aspiration?

General ALEXANDER. I believe in the future we are going to need to make structural changes, but I don't know what they would be right now. I believe that, as we look at how we are going to operate

in cyberspace to protect this Nation and the areas that you want us to protect and the Nation wants us to protect, we then need to look at how that team is organized, how it operates, and the authorities upon which it operates.

That is one of the things the government is working hard on right now. We are working our portion of it. I think what you would then want is for those teams to come together and put that all together, and that is where the White House—specifically Howard Schmidt and his folks—need to come back, lay out those authorities, and come back to you with that.

And in that, they may come up with recommendations, but I don't know any right now that I would make.

Mr. JOHNSON. Much of the hardware used on U.S. defense and intelligence networks is manufactured abroad, some of it in China. Is that correct?

General ALEXANDER. Yes, much of computers are put together or—or built in other countries, and China is one of the big producers.

Mr. JOHNSON. Are we confident that those hardware supplies are not compromised? And is there something that we can do with respect to securing the items during the manufacturing process?

General ALEXANDER. I think there are two parts to that. One is, as we manufacture or manufacture things to a specific standard and have the capability to test that standard, that would be one part. Same for software. And, two, understand that people will always try to manipulate your system, and we have to be looking out for that and have the capability to dynamically look to that within our networks.

Mr. JOHNSON. Thank you, General. You and your associates have a big job to do, and we appreciate you for your professionalism and your—your strong will to win in cyberspace. Thank you.

General ALEXANDER. Thank you.

The CHAIRMAN. I thank the gentleman.

Ms. Shea-Porter.

Ms. SHEA-PORTER. Thank you very much, Mr. Chairman.

And thank you for being here. Last week, there was a briefing that the deputy commander of Cyber Command, he discussed an upcoming disaster response exercise that was being planned in the Department of Homeland Security and how he was working to make sure that Cyber Command was involved in the exercise. It was taking some effort to make sure that he was able to participate.

While there have been questions on integration of the services, could you please tell me how Cyber Command is working with other government agencies, such as Department of Homeland Security?

General ALEXANDER. Right. We work with the Department of Homeland Security in a number of ways. If I could, first, we, NSA, has a team there, a cryptologic support group, that we depend on largely to help in this cyber area.

Two, within the department, they—our Under Secretary of Defense for Policy has a responsibility to reach out to the Homeland Security, and we have a direct relationship to them. For the US–CERT, the computer emergency response teams that they have, for

their operations and ensure that information is passed back and forth.

So if you think about it—I am—I am giving you kind of a convoluted answer, because it actually goes on several levels. At the high level, what the departments are doing, Homeland Security and Defense, my opinion, the Secretary of Defense and the Secretary of Homeland Security have a vision for how they are going to do this and they are working towards that vision and trying to bring it.

The staffs are working together, the department staff and that. We fall under that department staff and take their lead. And at the operational level, on the networks, the US–CERT worked with our Joint Operations Center and others to ensure that information is passed on the networks about threats and stuff, and that works pretty good.

So at the—at the player level, that is going on, and we are building the others to get to issues like that cyber exercise coming up.

Ms. SHEA-PORTER. Okay. So you feel that you are a full player on the field now, that everybody recognizes how essential your mission is, and that you are well integrated?

General ALEXANDER. I think there is always going to be—for the near term, we are going to have to do a lot of work to integrate, because there is issues that as—as you would expect, of who has got the responsibility for which piece? How do we work that? I think those issues are natural. We are working those out.

I do—I would tell you that they know we are here, they are working with us. I just had a meeting earlier this week—and we had Rand Beers and Phil Reitinger there at the meeting, and we have daily VTCs [video teleconferences] with Homeland Security in this area.

That doesn't mean that we are not going to have issues about how much do we play, for example, in that cyber exercise, Defense Department issues versus Homeland Security issues, and that is probably where you will see more friction. So how much of each do you play? How—how radical do you make the exercise? And——

Ms. SHEA-PORTER. I would say that time is our enemy on this. As fast as we can move this integration, the better off and the safer we will be. So thank you for your efforts, and I yield back.

The CHAIRMAN. With no further questions, General, we are very appreciative of your being with us today. We wish you well. And it appears you have some excellent colleagues to work with. And we look forward to your testimony in the future. We are, of course, here to be of assistance to make you all the more successful.

With that, the hearing is adjourned. Thank you.

[Whereupon, at 11:22 a.m., the committee was adjourned.]

# A P P E N D I X

SEPTEMBER 23, 2010

## PREPARED STATEMENTS SUBMITTED FOR THE RECORD

SEPTEMBER 23, 2010

**Opening Statement of Chairman Ike Skelton**
**Committee on Armed Services Hearing on U.S. Cyber Command: Organizing for Cyberspace Operations**
**September 23, 2010**

Good morning ladies and gentlemen, and welcome to today's hearing on U.S. Cyber Command: Organizing for Cyberspace Operations. We will hear—for the first time in this committee since Cyber Command was established—from General Keith Alexander, the first commander of U.S. Cyber Command. He also continues to serve in his role as the Director of the National Security Agency.

General Alexander has a long record of service to the nation, and is a genuinely nice person to boot. I think perhaps the most important thing for the American people to learn from this hearing is that they have exactly the right person in charge of this new command. General Alexander is simply the best, though I would note that there are some other generals from his class at West Point who also haven't done too badly. General Alexander, welcome.

U.S. Cyber Command, or CyberCom, has been tasked with conducting the full range of activities needed for the Department of Defense to operate effectively in cyberspace. Of one thing I am confident, cyberspace will be a big part of the future of warfare. That means we can't afford to get this wrong. The establishment of CyberCom is a critical milestone for this nation's defense.

Cyberspace is an environment where distinctions and divisions between public and private, government and commercial, military and non-military are blurred. And while there are limits to what we can talk

about in this open forum, the importance of this topic requires that we engage in this discussion in a very direct way and include the public.

The threats facing the nation in cyberspace are daunting, and have been underappreciated until recently. Just within the DOD, there are more than 15,000 different computer networks including seven million computing devices on 4,000 military installations around the world. These information systems face thousands of attacks a day from criminals, terrorist organizations and more than 100 foreign intelligence organizations. DOD recently announced a new cyberstrategy to deal with that burgeoning threat.

To understand how well prepared the Department of Defense is to handle the magnitude of this threat, we need to ask some fundamental questions. Where are we today with CyberCom? Where do we want to take it in the future? And do we have what we need to get there?

An additional challenge for this Committee is determining how CyberCom fits into a broader national effort. DOD has traditionally led the way in protecting information systems, so it is natural for CyberCom to play a role beyond just protecting military networks. What that role should be, however, needs careful analysis. We know that as a nation we must do more to improve security in cyberspace and manage risk without choking off creativity and innovation. General, I look forward to hearing your testimony today on how you intend to address these important issues.

**Opening Statement of Ranking Member Howard P. "Buck" McKeon**
**Committee on Armed Services Hearing on U.S. Cyber Command:**
**Organizing for Cyberspace Operations**
**September 23, 2010**

I would like to thank Chairman Skelton for today's hearing on Cyber Command and General Alexander for joining us today. Cyber is an operational space that extends well beyond Internet searches and email messages into a world of networking, interconnected systems and pathways that can reach into individual components of critical weapons systems. The potential for harm from malicious activity reaches beyond the traditional military sphere of influence as financial systems, critical domestic infrastructure such as power and water treatment plants and personal information can all be touched and disrupted through cyberspace.

With this in mind, I look with great anticipation to Cyber Command becoming fully operational next month. The Department of Defense, in many ways, has been at the leading edge of defending against malicious cyber activity and in understanding the problems and opportunities that cyberspace presents to our nation. And I believe we have, in General Keith Alexander, the most appropriate person to lead this newly formed command under U.S. Strategic Command.

U.S. Cyber Command will be the touch-point for all things cyber within the Department and will therefore carry a heavy burden. The services have built an infrastructure—physical capability as well as policies and processes—to handle the extensive activity that must be conducted in the cyber realm. Now, General Alexander will have to ensure those efforts are brought under one vision and mission, with the goal of maintaining our military's ability to conduct its operations in cyberspace.

Let there be no doubt: this space is contested and presents a persistent vulnerability for our military, civilian and commercial infrastructures, especially as we increase our dependence on it. As then-DNI Director Dennis Blair commented in testimony to the Senate Select Committee on Intelligence on February 2nd: "We

cannot be certain that our cyberspace infrastructure will remain available and reliable during a time of crisis." In his recent Foreign Affairs opinion piece, Deputy Defense Secretary William Lynn also touched on the significant threat that exists in cyberspace.

The Department is under constant attack, and attacks will only increase in a crisis situation. Accordingly, the Department must ensure the appropriate investments in technology, infrastructure and people are being made and the appropriate authorities, processes, policies and organizations are in place to allow our nation's military to meet today's challenges. The establishment of Cyber Command meets an important step in strengthening the Department's cyber capabilities. As confirmed in the 2010 Quadrennial Defense Review, the Pentagon needs both a centralized command for cyber operations and the development of a comprehensive approach to cyber operations.

Despite this progress, many questions remain as to how Cyber Command will meet such a broad mandate. Your testimony today, therefore, will help this committee understand Cyber Command's functions and how the Department is mitigating its vulnerabilities in cyberspace.

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

23 SEPTEMBER 2010

NOT FOR DISTRIBUTION UNTIL RELEASED BY THE
HOUSE COMMITTEE ON ARMED SERVICES

Chairman Skelton, Ranking Member McKeon, and distinguished members of the Committee on Armed Services, thank you for inviting me today to represent the extraordinary men and women of the new United States Cyber Command and deliver the Command's first posture statement. Indeed, I want to begin my remarks by thanking you and your colleagues in Congress again for helping to make this Command a reality as we move forward to address threats and concerns to our nation. We have a big job in front of us, not only in terms of accomplishing our mission but also in terms of ensuring that our nation understands just what it is that you, and the White House, and the Department of Defense have charged us to do. I want to take this opportunity to explain how we look at that vital job and how we are organizing to meet its challenges. I see these remarks as an invitation to a dialogue about the roles, missions, and capabilities of the Department of Defense in cyberspace, and I am eager to hear your views on how we should be proceeding.

Before going any further, however, I also need to thank the great partners we have had, both in the effort to establish US Cyber Command and in our work of building its capabilities. Cyber Command and its early progress simply would not have been possible without the sustained leadership of President Obama, Secretary of Defense Robert Gates, Deputy Secretary of Defense William Lynn, General Kevin Chilton, and many others, including Secretary of Homeland Security Janet Napolitano, Director of National Intelligence James Clapper, Chairman Michael Mullen, Vice Chairman James Cartwright, General David Petraeus, Admiral Robert Willard, General Duncan McNabb, Admiral James Stavridis, Deputy Director Chris Inglis, Acting Assistant Secretary Cheryl Roby, and Lieutenant General Carroll Pollett. We also owe our gratitude to the White House, US Strategic Command, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and our partners in the intelligence community, law enforcement, homeland security, and industry. That list, while large, is not comprehensive, as there were significant contributions from too many others to name everyone.

My aim is to describe what is happening at US Cyber Command. I shall provide an overview of where we think we are—both in building the new Command and in the larger context of the global changes that have brought about the need to create a cyber command—and then tell you how we plan to move forward in accomplishing the mission assigned to us.

*Creating a New Command*

US Cyber Command is a sub-unified command under US Strategic Command. We are combining two entities from US Strategic Command: the Joint Functional Component Command for Network Warfare and the Joint Task Force-Global Network Operations, along with a consolidated staff that temporarily bridged these two legacy organizations. When the Cyber Command Staff reaches full operational capacity it should have around 1100 personnel, mostly military but with some civilian officials, and focused, on-site contract support. In a sense we in the Command are swapping out the engine of a race car at high speed; creating an enhanced cyberspace capability while conducting cyberspace operations in support of the Department of Defense and other departments and agencies.

Based on the Secretary of Defense's announced efficiency initiative, we are examining how we support this important program and how it might affect us at US Cyber Command. It is possible that resources saved from the stand-down of the Office of the Assistant Secretary of Defense for Networks and Information Integration will boost US Cyber Command. The Command's requirements, along with those of the rest of the Department, are being reviewed now and will be addressed in the Fiscal Year 2012 budget.

As your subcommittee on Terrorism and Unconventional Threats and Capabilities will hear this afternoon, the Service cyber components assist us in Cyber Command. Indeed, they are the organizations and the people who do much of the work of the Department of Defense in cyberspace. What we do as US Cyber Commend in many cases will actually get done through Army Forces Cyber Command, the Navy's Fleet Cyber Command, the 24th Air Force, and Marine Forces Cyber Command. We are working closely with the Joint Staff, Combatant Commands and the Services to determine the optimal way US Cyber Command will exercise command and control over the constituent units associated with these components. I look forward to reporting to you on this topic in the near future.

The National Security Agency (NSA) contributes essential expertise for our activities, both in supporting the accomplishment of our mission and in terms of day-to-day support. As you know, I also serve as the Director of NSA and the Chief of the Central Security Service (CSS). NSA/CSS's infrastructure and expertise have been crucial to our progress so far. The core of what NSA/CSS does will not change as Cyber Command grows. Those organizations will continue to lead the US cryptologic community on the signals intelligence and information assurance fronts. The professionals at NSA/CSS have a history of success and expertise, and as a customer, Cyber Command will leverage those capabilities. In our work at both NSA/CSS and Cyber Command we see how much the world is becoming networked and inter-connected. NSA/CSS more and more finds itself conducting its traditional signals intelligence and information assurance missions in the cyber domain. As Cyber Command stands up, it is vital to develop synergy with NSA/CSS in order to take advantage of NSA/CSS's longstanding competence and its outstanding capabilities—especially its deep commitment to supporting ongoing military operations and its mature processes for producing intelligence while respecting the privacy and civil liberties of US persons. Indeed, those achievements have already allowed Cyber Command to take prudent risk by focusing our efforts on building our mission capabilities now, in the light of protecting privacy and civil liberties, while letting our support functions follow. Having Cyber Command co-located with NSA/CSS will benefit the Agency now and in the long run; enabling us to build a vital partnership, leveraging intelligence to support defense and helping us conduct our respective missions in concert – while ensuring that we respect and honor our commitment to the law and the privacy of our fellow citizens.

Last, but by no means least, we also receive support from the Defense Information Systems Agency, which plans, acquires, and maintains the communications backbone that our Department of Defense's data ride on. DISA has run the Department's networks for decades, and it continues to play a significant role as we move forward. Its impending move to Fort Meade will allow for the development of closer working relationships between DISA, NSA/CSS, and Cyber Command – and it will help us ensure that future government telecommunications

infrastructure design is done in close coordination with still more organizations that are well-versed in network security.

*The Strategic Environment in Cyberspace*

Deputy Secretary William Lynn noted recently that the key to Cyber Command is its "linking of intelligence, offense, and defense under one roof." How will that actually work? Before explaining our plans for US Cyber Command, it might be helpful to describe what we might call our "common operating picture." This entails an explanation of the environment in which our Command functions and how that is changing, and a description of the actors who inhabit it with us—some of whom give us increasing grounds for concern.

Cyber Command has a unique "area of responsibility" that literally changes its characteristics and its dimensions continuously. For instance, since 2000, world Internet usage has increased by 400 percent. In 2009 there were more than 1.8 billion Internet users, and 4.6 billion cellular subscribers; together they sent roughly 90 trillion e-mails. Cyberspace in that sense is "larger" than ever. And yet, at the same time, bandwidth is broader and search engines are more powerful than ever, and so in a different sense cyberspace has become "smaller," with more and more people able to interact with each other in real-time.

The US military began thinking formally about cyber matters almost twenty years ago. Cyberspace can be tough to understand at first glance—what does it mean when machines talk to other machines, and how does that affect us here in the real world? The Joint Chiefs of Staff deemed cyberspace a "domain" within the last decade, but what does that mean when cyber is so unlike the other domains (for instance in being man-made)? The way to understand it is to grasp what cyberspace is, and what it is not.

Allow me to make one quick example. I recently bought an iPad. Its capability surpasses that of even NASA computers of twenty years ago. Yet the physical materials in that device are worth little in and of themselves. What makes those components valuable are the data they contain and the logical processes for making sense of those data. That value, moreover, was infused in that iPad through a series of steps that each represented a coming-together of hundreds or thousands of individual talents and contributions. Think of the highly specialized tools and materials that went into its manufacture, and then the millions of lines of computer code that comprise its operating system and programs—not to mention its applications—and you begin to grasp the complexity of our new world and the ways in which our economy and society have shifted to an information culture, where wealth is less and less rooted in the physical ability to manipulate objects than it is in the knowledge of how those objects work together.

The world is shifting its collective memory and sense-making capacity into digital forms. That wealth, moreover, exists in ways (note that I do not say <u>places</u> here) that are increasingly accessible by others. Time and distance are less relevant in the cyber domain than in any other. Telephones and computers and radios are essentially merging. That means our communications infrastructure is mostly computers talking to other computers. And remember that each of those

computers not only moves data, it stores data—in astronomical quantities. Our radios have become our filing cabinets, and vice versa, and they have become so small that we carry them in our pockets, and there is no going back to some simpler time.

What does that mean in military terms? The cyber domain in some ways is like the air domain, in being a realm that had no relevance for military planning until all of the sudden a new technology offered access to it. A century ago the world's militaries had to learn to fight in the air, and they had to do so all at once in the midst of a world war. We realized that no one service can possess the entire air domain or claim exclusive use of it; all the services require access, all require capability, and all contribute to the joint fight. The parallels with cyberspace seem obvious: freedom of action in cyberspace, like freedom of maneuver in the air, is crucial to the efficient employment of one's forces in all domains. Likewise, the loss of such freedom could impair the capabilities we have built in all the other domains.

Cyberspace is densely populated with billions of actors. It can be difficult to sort them into friends and enemies. Indeed, everyone who logs on to the Web puts themselves into a domain that can be used not just for productive purposes, but a domain that is simultaneously a potential area for both criminal or hostile purposes. There are no sanctuaries for the innocent. When people enter cyberspace, they can be the unwitting victims of a range of malicious actors, including states' militaries. Thefts of intellectual property can take on hitherto unimaginable scale; a conqueror once had to capture a city before his army could loot it. Now that wealth is increasingly digital, economic espionage for commercial and technological advantage is an everyday event. And it is not just theft that concerns us. More and more we see states extending their use of traditional instruments of power into cyberspace. We are increasingly seeing activities in cyberspace which carry the potential to threaten national security.

In other words, competition and even conflict in cyberspace are a current reality. US Cyber Command indeed has been "in action" every day of its brief existence. The Department of Defense networks that we defend are probed roughly 250,000 times an hour. By 2006, to cite another example, the Department determined that 10-20 terabytes of data had been remotely exfiltrated from NIPRNet, our unclassified but still sensitive network that is connected to the Internet. Furthermore, while even casual users of the Web have heard of malware to monitor, exploit, and disrupt computers and networks, there are new tools appearing that can damage or destroy systems. This recent shift toward operationalizing cyber tools as weapons to damage or destroy is of great concern to us at Cyber Command.

Conflict in cyberspace, moreover, is highly asymmetric. Minor actors can afford and deploy tools to magnify their effects; witness the recent press reports about arrests in Europe of several individuals charged with creating the so-called "Mariposa botnet"—a collection of 13 million computers slaved together for criminal purposes. The tools these actors can employ are almost anonymous—a defender can sometimes learn where an attack came from, but can be time-consuming. That means "attribution" in cyberspace is costly and comparatively rare. The "price" an adversary pays for a capability—a tool or weapon—can be slight; the cost and impact borne by the victim of his attack can be very high.

Such costs can be inflicted by a nation-state's military or by one of its intelligence services, or by cyber criminals, or simply by a software glitch. Telling one actor from another and divining actors' intentions can be very difficult. Not every event that affects our networks rises to the level of a national security threat. It is important to remember that hacking, spreading malware, and other malicious activities are crimes, defined domestically as well as internationally by the Convention on Cybercrime, and accordingly have legal consequences. Even if you spot an intrusion and you know it originated from an adversary, you usually cannot tell an intelligence operation from a military one. Is a probe of your system intended by the fellow who launched it as a precursor to an effort to map your network, to steal your data, to corrupt that data, or take down the entire network? The skills to do any one of these actions are not fundamentally different from those required to do the others. The international puzzlement and concern over the seemingly innocuous Conficker worm, which has been in millions of systems since 2008, provides just a foretaste of the disruption that malicious cyber tools can cause.

Deterrence in this field is different from any other. It will not function as it did during the Cold War, as General Chilton mentioned to you last spring. Attacks by hackers and criminals can cause "nation-state sized" effects; indeed, the accidental "release" of malware might do the same, and the problem of attributing the attack to a particular actor similarly remains difficult to impossible. We have to study deterrence anew, from a variety of perspectives, and to gain clarity on our authorities. To take a thought from Sun Tzu, we must understand the cyber environment and, the capabilities of our adversaries, and our own abilities as well. This is not going to be easy, and it is not going to yield answers soon. If we know one thing from the Cold War, it is that stable deterrence can take years to achieve, and is the product of planning, analysis, and dialogue across the government, academe, and industry, and with other nations as well. Cyber deterrence will require progress in situational awareness, defense, and offensive capabilities that adversaries know we will use if we deem necessary.

*US Cyber Command's Direction and Plans*

US Cyber Command has three main lines of operation. We direct the operations and defense of the Global Information Grid so the Department of Defense can perform its missions, we stand ready to execute full-spectrum cyber operations on command, and we stay prepared to defend our nation's freedom of action in cyberspace.

In a strict sense, none of these jobs are new. As the Department's networks expanded and became increasingly reliant on the public Internet over a decade ago, the imperative to organize ourselves better in cyberspace became obvious. We in the United States have tried several organizational arrangements for each of those three missions, and as a result of this evolution two lessons have impressed themselves on the Department's leaders. What is new is the way in which we at Cyber Command are applying these lessons. The first is the wisdom of keeping the command and control of military networks and operations with an organization possessing a global perspective on vulnerabilities, threats, and challenges to our nation; that is why US Strategic Command, within the Department of Defense, holds authority over military operations in cyberspace and delegates it to US Cyber Command. The second lesson we have

learned has been the need for a tight synchronization between the people who monitor and operate the Department's 15,000 networks and their colleagues who watch and respond to adversarial activities. In short, several previously parallel streams of expertise have to blend together continuously or leadership will not have crucial situational awareness and a full range of options.

The price we might pay for not having such synchronization can be high. An incident in late 2008 underscored this point for Departmental leadership, and also helped us to fashion a template for "operationalizing" our management of the Department's sectors of cyberspace. Operation Buckshot Yankee was our response to a very serious infection of a classified network serving US Central Command. What happened was that contaminated thumb drives were used by US military personnel in the Middle East who had no idea they were implanting malware created by one of the more than one hundred foreign intelligence services seeking to break into our systems. The resulting infection amounted to what Deputy Secretary Lynn called a "digital beachhead" on our networks that could have been dangerously exploited by an adversary if it had not been detected, analyzed, and neutralized by a combination of intelligence and military efforts. The malware involved demonstrated the skill and determination of our adversaries, and hence the urgency for increasing our preparedness for the next attempt to penetrate our sensitive systems. At the same time, our response in Operation Buckshot Yankee convinced leaders in the Department of Defense of the potential for synergy that results from combining network operations with dynamic defenses and the ability to play offense as well.

Operation Buckshot Yankee should have vanquished any notion that Department of Defense networks are not at risk. The Deputy Secretary has enumerated five principles for the Department's strategy in cyberspace, and these guide our efforts as we build US Cyber Command and launch its operations. Cyber Command is not the sole participant in any of these fields of effort, but it is a leader in collaboration with its mission partners in all of them:

- *First, remember that cyberspace is a defensible domain.* We should study cyberspace in the same way we study the other domains, to understand how the principles of the military art apply there. We must learn its topography, so to speak, along with its environmental challenges and culture, just as we would seek to learn about any other "place" where we might have to defend our nation and its interests. Let me offer an example of the work that remains to be done. The Department has learned through experience to organize its operating forces in the field not by Service but by mission, with each geographic combatant commander controlling components and task forces that operate in one or more of the domains within his region. US Strategic Command stretches this mold slightly, in controlling forces possessing global reach (and the use of which always implicates national interests). This exception, however, proves the rule in being a supplement to the work and the capabilities of the geographic commands—available to meet their needs for longer-ranged and more-powerful support. Command and control in cyberspace is still more complicated. Computer network operations can be regional and global at the same time, and can have effects approaching those of weapons of mass destruction. The devices that give us access to cyberspace exist in the physical world, and in conventional military terms we can say that they are always within the area of responsibility of some geographic combatant command—but they can create effects

that take place far away in the area of responsibility of a second command, and they might be enabled to do so by unsuspecting users and their devices located in still a third command's region. Which commander is the mission lead in such a case and is military action appropriate? Which command is supported, and which is supporting? In cyberspace, questions like this must be answered at Internet speed and must take into account our responsibilities and obligations under international law and norms. For example, the U.S. has affirmed that the international Law of Armed Conflict, which we apply to the prosecution of kinetic warfare, will also apply to actions in cyberspace. Of course, the details of this remain to be developed in light of the unique attributes of Internet technology. Indeed, in cyberspace a command can be supported and supporting at the same time, with the roles switching back and forth. The trick is to engineer a structure for operations in cyberspace that combines the necessary processes, immediate feedback, and effective controls with sufficient elasticity to respond when the first warning might be fragmentary but the risk of waiting even a few minutes for better information can be grave.

- *Make our defenses active* – In cyberspace the only "perfect" defense is the static one: to disconnect and thereby forfeit the cyber realm and its economic and social benefits to one's adversaries. That is not possible for the United States or the Department of Defense. Indeed, there is no "unplug" option for American society; our homes, businesses, schools, hospitals, government offices, and indeed our very way of life now depend on access to networks. Even if you do not own a computer, you rely on neighbors, colleagues, and institutions that do. Our cyber engagement is thereby a matter of prudent vulnerability management and risk recognition. Since security in a networked world is a system for managing that risk, we in US Cyber Command have a structured system of security measures for Departmental networks: monitoring of the Grid for situational awareness, advisories and patches and updates, anti-virus programs, firewalls, objective security assessments, automatic intrusion detection and blocking measure, active searches for malware, and forensic response teams. We manage all this with what we call Dynamic Network Defense Operations, and it is a cornerstone of our work.

- *Extend protection to our critical infrastructure* – About a generation ago the infrastructure that undergirds our society and economy passed a tipping point when computers ceased to be optional features and became essential for basic functioning. President Obama has made guarding that infrastructure a national security priority. Today our energy sources, utilities, public transportation, banking, public records, and much more are all on "the Net." Our military, furthermore, depends on unclassified networks for much of its communications and logistical functions. While automation and networking make the command and control of such systems more convenient, it adds a dimension of complexity and concomitant vulnerability that the creators of these systems never anticipated. Because of that, the legacy systems that run much of our critical infrastructure are inherently more difficult to protect and defend than modern systems being created today. No one has seriously attacked these yet—at least not in the United States—but we have seen the probing of those systems by our adversaries. We have seen enough evidence of their vulnerability due to natural disasters and accidental malfunctions—like the software glitch that contributed to the power outage across the

Northeast in August 2003—to be concerned about the potential effects of an actual attack on any piece of the networked infrastructure. The Department of Homeland Security has the daunting task to work collaboratively with public, private and international entities to secure cyberspace, and America's cyber assets, systems, and our colleagues there are moving out toward that end. But the need is great and there is no time to lose, as attacks and their potential effects would not discriminate between military and civilian users, and could come from a nation-state adversary, a terrorist group, or even a rogue individual. The Department of Homeland Security may require expert advice and consultation from both NSA and Cyber Command; both organizations stand ready to assist. Further, in the event of an attack we need to practice coordinated response efforts across government.

- *Foster collective defenses* – I like to call cyber a team sport; successful defense in any one part depends on the shared efforts of agencies, industry, allies, and mission partners who watch their own networks for problems that could affect them all. Each of us, and our colleagues, co-workers, friends, and families, are all participants—and potential targets. To avoid becoming victims, we must take positive and frequent steps to prevent that outcome. We are all part of a combined solution to a common problem. We can all do our part to understand the complexity of our new world and reduce our shared vulnerability. Many of the problems that keep us at work nights and weekends would be substantially diminished if users at their homes and offices would download and install manufacturers' recommended patches and updates. That is nothing new—many others have made the point before me. But the fact that it has to be repeated suggests something else that is different about cyberspace—it's tough to "see" security in the way we can see locks and bars and guards. Security is always inconvenient, and even more so in cyberspace because it costs time to get right and keep up-to-date—which is much of the battle right there. The cost of successful attack, however, is much higher than the expense of connecting and deploying the hardware and software to stay connected. Making security work requires common standards and terminology and the sharing of great quantities of timely information. We at Cyber Command have strong and tested military and intelligence partnerships with our allies that help us all in forming a common operating picture, and we are seeking to expand that ring of partnerships. None of us have all the authorities, capabilities, or resources to go it alone. We must work together.

- *Leverage US technological advantages* – The United States did much of the pioneering work that built the first computer data sharing networks, and many innovations in the hardware and software sectors still arise in this country. Our lead, however, has never been purely technological. I am convinced that the solutions to our vulnerabilities in cyberspace will prove to be primarily cultural and procedural. We do not necessarily need "better" technology than the proverbial other guy, in terms like bandwidth, storage, software versions, operating speeds, memory size, and so on. In any case, purely technological advantages are likely to be fewer and less lasting in our networked world. Our advantage has to lie in how we put these tools together in systems, especially systems of people, protocols, and machines that can operate reliably together at high speeds to identify vulnerabilities, share information, assess risks, devise countermeasures, and apply new solutions. Although US Cyber Command will not have acquisition authorities, we will support US Strategic Command in defining requirements. We in

Cyber Command are also participating in the Enduring Security Framework, a group of officials representing the Secretaries of Defense and Homeland Security and the Director of National Intelligence, who meet regularly with leaders from the private sector and experts in the cyber field. We envision this partnership as essential to helping the public sector address the cyber security threat. In addition, we are working with the Defense Advanced Research Projects Agency and supporting a "National Cyber Range" environment to build our capabilities in this field. Finally, another imperative is to build the capability of our "cyber workforce" in the Service cyber elements. They are essential to the accomplishment of our mission of supporting the combatant commands and national requirements. I cannot overemphasize the need for this workforce, and this capacity, to be built as soon as possible.

*Conclusion*

I thank you again for calling me before you today and giving me this opportunity to submit the first posture statement for US Cyber Command. I am convinced we have taken an important step for our nation in creating this Command, and that we have done so not a moment too soon. I have described our philosophy of actively managing the Global Information Grid—not just to defend it, but to use it as a tool to assist our warfighters, planners, and commanders by keeping their freedom of action as broad as possible—and of being as ready as we can, and when called upon, to use our own capabilities to disrupt any adversarial use of cyberspace against the United States, its interests and critical infrastructures, or other governments. I pledge that we will pull this new Command together in compliance with all of the laws governing privacy and civil liberties of U.S citizens, in accord with the directives of the national command authority, and, in conjunction with our mission partners in the Departments of State, Defense, and Homeland Security, law enforcement, the Intelligence Community, and industry and academe. We have to get this right, as I believe the security of our nation depends on it. We are working to meet this challenge so as to be worthy of your trust. With your help and counsel I have no doubt that we can succeed. 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.

## QUESTIONS SUBMITTED BY MEMBERS POST HEARING

SEPTEMBER 23, 2010

## QUESTIONS SUBMITTED BY MR. SKELTON

Mr. SKELTON. There are a number of efforts underway, in Congress and internationally, to better define legal norms and behaviors in cyberspace. DOD has traditionally been on the forward edge of thinking about these issues, so I would be interested in hearing from you about what role do you see for your command in attempting to shape the legal environment related to cyber operations? What are some of the pitfalls you see in proposals you are aware of? What components should we try to pursue more vigorously?

General ALEXANDER. United States Cyber Command (USCYBERCOM) plans and conducts operations fully consistent with all laws and regulations. Our foremost responsibility in this regard is to demonstrate our support and compliance with the law. As we conduct planning, we undertake to determine the limitations and restrictions we face, as well as any concerns, and continuously keep the policymakers and decisionmakers within the Department informed. We can best contribute to effective decisionmaking by providing quality, detailed and expert knowledge about operational considerations in and through cyberspace. We are aware of many low-level discussions across many organizations. At this juncture, we are principally supporting internal discussions sponsored by Under Secretary of Defense (Policy) (USD (P)) and the Joint Staff. In our view, the most important perspective we can bring to the table is a perspective informed through deep technical understanding of the domain and based in Combatant Command (COCOM) deliberate and adaptive planning processes. The Department, led by the Under Secretary of Defense for Policy, is conducting a review of DOD policies relating to cyberspace.

Mr. SKELTON. What service and joint training and educational institutions do you use now, or will you use in the future, for developing your cadre of cyber warriors?

General ALEXANDER. Currently, the number of fully trained, credentialed, and certified cyber personnel, military and civilian, is limited. Training and skills development and sustainment demands extensive time and effort. Our most significant challenge is to ensure that on balance, the Nation benefits from all potential talent available. USCYBERCOM currently uses several different venues for cyber training and education, to include:

- Service-specific initial occupational training and ongoing professional military education
- Computer Network Defense Course—Fort McCoy, Wisconsin
- Information Assurance Training Center, U.S. Army Signal Center—Fort Gordon, Georgia
- Basic Computer Network Operations Planners Course (BCNOPC)—1st IO Command
- Signal Corps Cyber Security Training—Fort Stewart, Georgia
- Center for Computer Network Operations, Cyber Security & Information Assurance within NSA Associate Directorate for Education and Training (ADET) College of Cryptology
- Eastern Michigan University—Michigan
- University of Maryland Baltimore County (UMBC)—Maryland
- Northrop Grumman Cyber Warrior course—Maryland
- DOD Cyber Crime Training Academy—Linthicum, Maryland
- Joint Network Attack Course (JNAC)—Center for Information Dominance, Corey Station, Florida
- Joint Cyber Analysis Course (JCAC)—Center for Information Dominance, Corey Station, Florida

Each of these courses provides a current foundation in requisite Information Assurance (IA) and Computer Network Defense (CND) skills. In addition to these Joint Service schools, agency and contract efforts, there remain extensive opportunities with significant potential: over 100 Community Colleges, Colleges and Universities which are National Security Agency (NSA)/Department of Homeland Security (DHS) Centers for Academic Excellence; Air Force Institute of Technology (AFIT) Center for Cyberspace Research; the Naval Post Graduate School (NPS); the Army's Advanced Civil Schooling (ACS) program; the National Defense University (NDU) system; the National Defense Intelligence College (NDIC); and the Advanced Technical

Intelligence Center (ATIC). The services are restructuring or developing new technical training courses and job skills that will potentially result in new occupational specialty codes throughout the services that are trained at the basic level to enter the cyber community.

Mr. SKELTON. Do you have plans to carry out any significant joint, interagency or international exercises that would test out DOD's ability to respond to large-scale attacks against DOD computer networks, similar to the ELIGIBLE RECEIVER 97 exercise?

General ALEXANDER. Exercises are a well-recognized and traditional DOD mechanism to develop and certify operational constructs. USCYBERCOM has participated in one interagency and two COCOM exercises since May 2010. It is our intention and task to participate in a robust exercise regime to support technical and operational concept development and validation; and to use these exercises as a means to develop our tactics, techniques, and procedures and identify gaps in policy and law.

Mr. SKELTON. What capabilities do you have to conduct active network operations, such as network hunting, penetration testing and other forms of red teaming? Do you have unmet needs in this area (in terms of people or tools)?

General ALEXANDER. USCYBERCOM has limited NSA and Service capabilities to leverage in hunting, penetration testing, and red teaming. We use Green Teams to respond to cyber incidents; Blue Teams that provide in-depth review and resolution of cyber events and Red Teams that emulate adversary procedures against DOD hosts to train defenders and identify vulnerabilities for mitigation. We estimate that current resources (NSA's Advanced Network Operations (ANO) and Service Red Teams) can only cover a fraction of the DOD networks. Effective hunting is absolutely essential to discovery, characterization, and mitigation of threat activity on our networks. USCYBERCOM is working with NSA and the Services to leverage the projected resource savings, both in terms of personnel and money, we anticipate from planned information technology initiatives that will enable us to recruit, train, and field more hunting teams and develop and field automated hunting and adversary data analysis capabilities to address this key shortfall.

Mr. SKELTON. In your testimony, you mentioned something called expeditionary cyber support elements. Can you explain in more detail what these are, and what role you see them playing in future CYBERCOM operations?

General ALEXANDER. COCOMs and deployed forces require the ability to leverage USCYBERCOM expertise and capabilities in planning and conducting full-spectrum cyber operations in support of their assigned missions. To directly support both Combatant Commanders and Joint Task Force Commanders, USCYBERCOM has created two complementary support elements—the Cyber Support Element (CSE) and the Expeditionary Cyber Support Element (ExCSE). Both are assigned to USCYBERCOM, but the CSE is with duty at the Geographic COCOM headquarters, and the ExCSE is deployed on orders to a Joint Task Force Commander located in an Area of Hostilities.

The CSE supports the Combatant Commanders at their headquarters through liaison, planning, and operations support primarily at the Directorate of Operations, or J3 level. However, the CSE is empowered to develop relationships and capabilities across the Combatant Command. The CSEs have played innovative and complementary roles within the COCOM Directorates of Intelligence (J2) and Directorates of Plans and Policy (J5). To enable their effectiveness, the CSE has full reach-back support to USCYBERCOM headquarters and the NSA Enterprise.

An ExCSE consists of a team of experts deployed to an active Area of Hostilities to enable, implement, integrate, and execute cyber operations. Currently, USCYBERCOM has two ExCSEs teams deployed—one in Iraq and one in Afghanistan. The teams consist of five personnel: a team chief (lead planner), a cyber attack planner, a cyber defense planner, and two analysts (cyber and intelligence). USCYBERCOM embeds these teams within the supported Joint Task Force headquarters (typically J3 Directorate—Operations) to enable the delivery of cyber effects in support of the commander's priorities.

The size, composition, and role of an ExCSE team is scalable depending on mission requirements. For example, in Iraq and Afghanistan the ExCSEs provide cyber expertise directly to the deployed headquarters' planning effort while coordinating the delivery of cyber effects through USCYBERCOM headquarters and interagency partners. In future conflicts involving full-scale operations against sophisticated cyber adversaries, the ExCSEs will scale to meet mission requirements. The ExCSE teams will continue to coordinate for global effects through USCYBERCOM but will also play a key role in coordinating planning, direction, and execution of cyber operations through an in-theater Joint Cyber Operations Task Force (JCOTF).

Mr. SKELTON. The Committee appreciates the complexity of coordinating cyber operations in various Service, Agency, interagency, international and non-governmental organizations geographically dispersed across the world. To deal with that challenge, what tools, technologies, processes or procedures do you have in place, or are planning, to facilitate collaboration across the full range of cyber operations?

General ALEXANDER. Success in the cyber domain does demand coordination amongst all entities listed in the committee's question, and in fact requires close interaction and cooperation with academia and industry. USCYBERCOM has ongoing interaction/collaboration with all of these entities and leverages NSA's existing relationships. Additionally, to continue building essential collaboration, USCYBERCOM is exchanging co-located liaisons and increasing leadership participation in interagency groups (existing and planned); information and data exchanges to build shared situational awareness; cooperative exercises and planning efforts; periodic synchronization conferences; and development of an Integrated Cyber Center.

---

## QUESTIONS SUBMITTED BY MR. MILLER

Mr. MILLER. The cyber domain has become a formidable, dangerous "fourth" domain in which warfare is not simply expected to occur but indeed is occurring. Numerous sources tell us, including the DOD, that the threat is tremendous to U.S. intellectual, utility, and financial infrastructure. We see reports every day where other nations, organization and, at times, individuals "attack" some aspect of American society whether it be governmental organizations, civilian organizations or even individual citizens. It would seem most of the work the services are involved in appears to only provide defense of the Department's IT network and specifically for their own service. Although this is important, should the Department be involved in the defense of the Nation's networks as well? I certainly understand there will be legal challenges that will need to be addressed, but are we exploring the concept of national cyber defense and not simply DOD defense.

General ALEXANDER. As exemplified by the 27 September 2010 DOD/DHS Memorandum of Agreement Regarding Cyber Security, the DOD is actively working with U.S. Government (USG) Departments and organizations (e.g. U.S. Computer Emergency Response Team, Department of State, Department of Energy, Department of Justice, and the Director of National Intelligence) to collaborate and synchronize shared situational awareness, actionable intelligence, and operations to enhance cybersecurity for the Nation. Under authorities granted to USSTRATCOM, USCYBERCOM exercises its Title 10 missions, roles and functions in accordance with U.S. laws, policies, and regulations. The authority delegated to USCYBERCOM extends only to operate, defend, and when directed, conduct full-spectrum operations for DOD or ".mil" networks.

Mr. MILLER. I'm concerned that as each service builds its own cyber entities, there could be a divergence in interoperability and a lack of interservice cooperation as each service grows in its own unique direction thereby creating a pre-Special Operations Command Special Operations type of situation. What are we doing to ensure this is not happening and ensuring there is no duplication of effort which could lead to confusion and "cyber fratricide" leading to mission degradation? Are we achieving the basic military principles of economy of force and unity of effort?

General ALEXANDER. As a sub-unified command under U.S. Strategic Command, U.S. Cyber Command is organized as a joint warfighting command supported by Service cyber components. The organizational structure of USCYBERCOM and its Service cyber components afford a joint unity of effort and economy of force for the planning, coordinating, integrating, synchronizing, and conduct of those activities in the operation and defense of specified Department of Defense information networks. USCYBERCOM and USSTRATCOM have established processes for DOD-wide cyberspace operations capability development and acquisition to ensure cooperation and interoperability for cyber offensive, defensive, and network operations in its joint force.

Mr. MILLER. In terms of domains of conflict, there is air, space, land and sea. Cyber would seem to be a new domain. Would it be wise to consider a service that would be solely dedicated to training and equipping personnel for a joint commander just as the services provide forces for their respective domains to the combatant commander? If not, why not?

General ALEXANDER. Among the principal challenges facing the DOD in cyberspace is the ability to generate capacity—recruiting, training, certifying, and retaining a sufficient number of cyber operators. The services—Army, Marines, Navy, and Air Force have structure and organizational identity to recruit and identify talent.

The current training regime is built to a Joint standard. The USCYBERCOM stand-up was a logical step in bringing similar organizational structure and alignment to this domain. USCYBERCOM's goal is for Joint Force Commanders to have the ability to plan for effects in cyberspace as an integral—not separate—part of their mission planning, execution, and assessment cycles.

Mr. MILLER. Cyber Command is intended to be a Joint Sub-unified Command reporting to STRATCOM. I would assume that each service is "training and equipping" personnel to provide forces to the Joint Cyber Command. Based on the well-documented size and scope of the cyber threat, do you all believe that Cyber Command should be its own Combatant Command? If the threat truly is a dangerous as we say, and I certainly believe that it is, why wouldn't we stand up a command that has sole responsibility to execute operations within its AOR such as any other COCOM?

General ALEXANDER. USCYBERCOM is a sub-unified command organized under USSTRATCOM. There were several studies—from outside the Department, to across the Department, and within USSTRATCOM that considered a wide range of options for "best fit" organizational alignment. These studies were undertaken with facts and informed forecasts at that time. We believe a sub-unified command was the best first step.

---

## QUESTIONS SUBMITTED BY MR. TURNER

Mr. TURNER. In the opening portion of your verbal testimony, you identified developing, training, and educating cyber professionals as CYBERCOMMAND's top challenges. Further, training, organizing, and equipping the new cadre of cyber professionals has been a common concern among policymakers addressing cyber-capabilities for our National interests. Our U.S. Deputy Secretary of Defense (DSD), William J. Lynn III, identified the "strengthening of human capital in trained cybersecurity professionals" as a significant concern. In his Foreign Affairs article, he asserted that the U.S. needs to graduate "three times as many security professionals annually as a few years ago." How do you envision the premier cyber program at Air Force Institute of Technology being optimized to educate and train professionals at/for CYBERCOMMAND?

General ALEXANDER. The Air Force Institute of Technology (AFIT) Center for Cyberspace Research offers a wide range of Certificate, Undergraduate, Master's, and PhD level programs for the cyber community. These programs, along with similar programs through the Naval Postgraduate School (NPS) and the Army's Advanced Civil Schooling (ACS) program, provide cyber professionals with the educational foundation and professional development required to be successful as they transition to intermediate and higher levels of responsibility and leadership. AFIT supplements the USCYBERCOM requirements for a cadre of trained personnel in a standardized cyber curriculum for senior enlisted, mid-level Captains and Department of the Air Force civilians. We intend to work closely with AFIT and NPS leadership to ensure their programs reflect the lessons we learn from operating in cyberspace.

Mr. TURNER. The Dayton area is home to the Advanced Technical Intelligence Center (ATIC), a classified facility focused on providing the necessary technical education for intelligence professionals. How do you see facilities such as ATIC supplementing the training need for security professionals?

General ALEXANDER. The Advanced Technical Intelligence Center (ATIC) offers a wide range of classified and unclassified, entry level/familiarization/overview courses in the intelligence or related fields. These programs could help fulfill intelligence community knowledge gaps that military educational institutions are currently unable to provide. These courses provide an effective means for gaining essential basic knowledge requirements or specific specialized training in low-density skill sets. USCYBERCOM will continue to collaborate with ATIC as well as other elite learning institutions and activities through the National Defense University system to integrate, when applicable, current training and education requirements. USCYBERCOM will continue to provide guidance on future requirements and standards. ATIC's distance learning capabilities coupled with abilities to rapidly develop training on emerging technologies could be leveraged to support cyber-related training requirements across the DOD, until the services can generate the capacity and throughput required to meet mission demands.

Mr. TURNER. As quoted by Deputy Secretary of Defense William Lynn in the *Foreign Affairs* article, "Defending a New Domain: The Pentagon's Cyberstrategy," the report, "NATO 2020: Assured Security; Dynamic Engagement," a NATO [North Atlantic Treaty Organization]-commissioned study chaired by former U.S. Secretary of

State Madeleine Albright, rightly identified the need for the alliance's new "strategic concept" to further incorporate cyber defense. The U.S. government must ensure that NATO moves more resources to cyber defense so the member states can defend networks integral to the alliance's operations. As a NATO parliamentarian, I am interested in transatlantic security and ensuring we continue to build coalition capacity around the world. It is notable that DSD Lynn emphasized the five principles of Department's strategy in cyberspace in Brussels, while also stating that NATO must build a "cyber shield" to protect the transatlantic alliance from any Internet threats to its military and economic infrastructures. A) What initiatives are in place to develop NATO partners in the cyber arena? B) When addressing cybersecurity issues involving NATO and other international allies, what are your greatest challenges? C) How can international partnerships be cultivated and improved upon in the cyber domain? D) What mechanisms does USCYBERCOM have at its disposal to share intelligence with our allies?

General ALEXANDER. DOD has an agreement with NATO for conducting Information Assurance (IA) and Computer Network Defense (CND) information exchanges and related activities. EUCOM's Network Warfare Center is the executive agent responsible for overseeing the day-to-day management of the implementation activities of the agreement and USCYBERCOM is the DOD agent responsible for providing and receiving IA/CND information with the Technical Centre, NATO Computer Incident Response Center.

The greatest challenges in addressing cybersecurity issues are the downgrading, releasing, or disclosing of classified information, which supports cybersecurity strategies. Enduring methods to maximize shared situational awareness while reducing risk to U.S. networks remain a significant challenge. Additionally, USCYBERCOM must have a means to rapidly and securely share situational awareness information and mitigation strategies.

Strategic partnerships should mutually benefit both USCYBERCOM and its foreign counterparts. At minimum, informal discussions and engagement would increase our shared understanding about activities, capabilities, and areas for cooperative development, improve cyber defense activities and reduce misinterpretation and potential escalation of malicious cyber actions. Formal partnerships may also increase shared early warning, collective self-defense, and integrated operational planning. Further, our efforts are to support COCOM theater cooperation plans.

USCYBERCOM is not an intelligence agency. USCYBERCOM leverages existing DOD and intelligence community procedures and protocols. The International CND Coordination Working Group was established and subsequently developed standard operating procedures to facilitate the exchange of information via weekly teleconferences between the respective military CND watch centers, and methods to submit requests for information regarding noted intrusion activities.

Mr. TURNER. For the purposes of a hypothetical scenario, assume Fleet Cyber Command obtains information which they believe poses a credible threat to U.S. Naval operations or forces. Further assume that Fleet Cyber Command believes this information could compromise Army or ARFORCYBER operations or forces if such information were shared beyond Fleet Cyber Command officials. How can CYBERCOM ensure that effective communication exists among organizations, and avoid the pitfalls/difficulties in integration faced by other entities within the national and homeland security infrastructure?

General ALEXANDER. Commander USCYBERCOM will lead cyberspace operations as a joint endeavor with all cyber forces, regardless of service component, fully integrated into a joint fighting force. USCYBERCOM will enable and task through a joint operations center the synchronization and coordination of DOD cyber operations. USCYBERCOM's Joint Operations Center (JOC) is linked to service network operations centers ensuring threat information is passed in a timely manner.

Mr. TURNER. Within the last decade, some might argue that the organizational structures of the separate agencies (FBI, CIA, etc.) were not effectively organized to prevent a national disaster. Of which "lessons observed" from our intelligence community should CYBERCOM be mindful, and address in its culture and organizational structure, in order to be proactive and effectively prevent future asymmetric attacks? How can our national cyber infrastructure avoid organizational bureaucratic inefficiencies and stovepiping? How does CYBERCOM culturally encourage collaboration, communication and information-sharing? With which entities throughout the DOD and government does CYBERCOM most frequently cooperate on intelligence matters?

General ALEXANDER. In recent years (2007–2008), the cyber events in Latvia, Lithuania, Estonia, and Georgia, have informed all domestic U.S. agencies and organizations of the inherent vulnerabilities within the cyber domain. USCYBERCOM continuously educates, trains, exercises, operates, and assesses operational readi-

ness to conduct full-spectrum operations. In partnership with other U.S. Government (USG) agencies, COCOMs, and DOD organizations, USCYBERCOM leverages its relationship with the NSA to develop, assess, and monitor strategic indications and warning through the capabilities and accesses developed by the intelligence community (IC) and interagency.

As exemplified by the 27 September 2010 DOD/DHS Memorandum of Agreement Regarding Cybersecurity, the DOD is actively working with the other USG Departments to collaborate and synchronize shared situational awareness, actionable intelligence, and operations to enhance cybersecurity for the Nation.

To promote shared situational awareness and information sharing, USCYBERCOM actively engages with IC and interagency organizations.

The USCYBERCOM mission requires constant interaction with IC and interagency partners. One vehicle for this cooperation is the Joint Interagency Task Force–Cyber (JIATF–C). The JIATF–C includes all members of the IC, all COCOMS (and their respective Joint Intelligence Operations Center (JIOC) elements), and multiple members of the USG interagency community (e.g., FBI, DOJ, Treasury, DHS, DOS, etc.). Many of these organizations have personnel integrated into USCYBERCOM to perform vital coordination and liaison functions dramatically enhancing the speed at which USCYBERCOM can access and share intelligence in support of USCYBERCOM's missions and goals.

Mr. TURNER. For the purposes of a hypothetical scenario, assume the 24th Air Force is headquartered and/or operates primarily out of San Antonio, TX, and that Fleet Cyber Command is headquartered and/or operates primarily out of Annapolis, MD. Further assume that a cyber attack has crippled the 24th Air Force's electronic communications capabilities. Without the ability to communicate effectively in the event of a cyber attack, USCYBERCOM and any one of its members runs the risk of being, in essence, useless. If a nation is under attack—be it cyber or otherwise—communication and rapid response are vital. A) How can USCYBERCOM ensure that the means of communication upon which it relies will not itself be compromised? B) How can USCYBERCOM maintain open lines of communication among its member when telephone, e-mail, fax, etc. are compromised?

General ALEXANDER. USCYBERCOM has four service components, including both 24th Air Force and Fleet Cyber Command. The dispersed nature of the headquarters components and global presence of cyber forces serves to mitigate this scenario. The key to sustainable mission assurance is developing and sharing a combined situational awareness. Effectively, cyber forces at all echelons, will access this common operational picture and take appropriate actions toward an effective defense posture. More broadly, as a matter of prudent military planning, USCYBERCOM and its components are developing continuity of operations plans. These plans delineate and prioritize critical mission functions in the event of short or long-term disruptions and designated locations and required functionality for rapid reconstitution of command capabilities. As our networks continue to converge, the distinction between telephone, e-mail, and facsimile will be far less discernable.

Mr. TURNER. Jurisdiction is of tremendous significance in any discussion of cyberspace. Cyberspace is the most unique medium through which an individual or group may influence or attack. The ability to conceal, obscure, or otherwise mask one's identity and geographic locale is perhaps more prevalent in cyberspace than in any medium. What challenges and processes do you envision in adjudicating or determining future jurisdictional issues, which will undoubtedly arise?

General ALEXANDER. While jurisdiction is more of an immediate concern in civilian law enforcement, it is still an issue for military cyberspace operators as well. Terrorists can now "forum shop" and choose beneficial jurisdictions from where they can launch their attacks. Cyberspace is a domain in which even one computer operator conceivably possesses a global strike capability regardless of location. It used to be that terrorists had to physically locate themselves in their target area, but that is no longer the case. The uniqueness of the cyberspace domain affords terrorists, nation-states, or international criminals the ability to strike from or through favorable jurisdictions, complicating efforts to identify, investigate, and apprehend a perpetrator. Cyberspace affords our adversaries the ability to mask the identity and source of an attack, making attribution and defense a greater challenge.

○