[H.A.S.C. No. 111–51]

CYBERSPACE AS A WARFIGHTING DOMAIN: POLICY, MANAGEMENT AND TECHNICAL CHALLENGES TO MISSION ASSURANCE

HEARING

BEFORE THE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

HEARING HELD
MAY 5, 2009

U.S. GOVERNMENT PRINTING OFFICE

57–218 WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

ADAM SMITH, Washington, *Chairman*

MIKE McINTYRE, North Carolina
ROBERT ANDREWS, New Jersey
JAMES R. LANGEVIN, Rhode Island
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
BRAD ELLSWORTH, Indiana
PATRICK J. MURPHY, Pennsylvania
BOBBY BRIGHT, Alabama

JEFF MILLER, Florida
FRANK A. LoBIONDO, New Jersey
JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
THOMAS J. ROONEY, Florida
MAC THORNBERRY, Texas

KEVIN GATES, *Professional Staff Member*
ALEX KUGAJEVSKY, *Professional Staff Member*
ANDREW TABLER, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2009

Page

HEARING:

Tuesday, May 5, 2009, Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance 1

APPENDIX:

Tuesday, May 5, 2009 27

TUESDAY, MAY 5, 2009

CYBERSPACE AS A WARFIGHTING DOMAIN: POLICY, MANAGEMENT AND TECHNICAL CHALLENGES TO MISSION ASSURANCE

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

Miller, Hon. Jeff, a Representative from Florida, Ranking Member, Terrorism, Unconventional Threats and Capabilities Subcommittee 1

Smith, Hon. Adam, a Representative from Washington, Chairman, Terrorism, Unconventional Threats and Capabilities Subcommittee 1

WITNESSES

Alexander, Lt. Gen. Keith, USA, Commander, Joint Functional Component Command Network Warfare, Director, National Security Agency, Department of Defense 6

Carey, Robert J., Chief Information Officer (DONCIO), Department of the Navy 3

Krieger, Mike, Deputy Chief Information Officer/G–6, Department of the Army 2

Lentz, Robert, Deputy Assistant Secretary of Defense for Cyber, Identity Management, and Information Assurance, and Senior Information Assurance Official, Department of Defense 5

Shelton, Lt. Gen. William L., USAF, Chief of Warfighting Integration, Chief Information Officer, Office of the Secretary of the Air Force 4

APPENDIX

PREPARED STATEMENTS:

Alexander, Lt. Gen. Keith 94

Carey, Robert J. 44

Krieger, Mike 34

Lentz, Robert 66

Miller, Hon. Jeff 32

Shelton, Lt. Gen. William L. 54

Smith, Hon. Adam 31

Page

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. Murphy 121
Mr. Smith 101
Mr. Thornberry 109

CYBERSPACE AS A WARFIGHTING DOMAIN: POLICY, MANAGEMENT AND TECHNICAL CHALLENGES TO MISSION ASSURANCE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE,
Washington, DC, Tuesday, May 5, 2009.

The subcommittee met, pursuant to call, at 3:58 p.m., in room 2212, Rayburn House Office Building, Hon. Adam Smith (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. SMITH. Good afternoon. Call the meeting to order. Sorry about the delay. Votes came at a bad time, and then I got waylaid by a conversation on my way over here, but I do want to thank all of you for being here today. Appreciate your presence on this very important topic and look forward to hearing from all of you.

I will keep my opening statement very, very brief except to say that cyber security is an incredibly important element of our national security with many, many complex pieces to it. Obviously it involves a multi-agency process; also it involves the private sector and a variety of different challenges that are very complicated and complex.

And our goal in this committee is to help work with the new administration and all the appropriate agencies to try to develop a comprehensive strategy to approach our network security needs and our broader cyber security interests—try to get us to the point where we have at least some idea of what the plan is and are working closely together on how to implement that with all the different pieces of it. And I look forward to the testimony. We have a very, very distinguished panel that will help shed some light on this issue and help let us know what the pathway forward is.

And with that, I will yield to our ranking member, Mr. Miller, for any opening statement that he might have.

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

STATEMENT OF HON. JEFF MILLER, A REPRESENTATIVE FROM FLORIDA, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. MILLER. Thank you very much, Mr. Chairman. I have a full statement that I would like submitted into the record.

[The prepared statement of Mr. Miller can be found in the Appendix on page 32.]

Mr. MILLER. I associate myself with your remarks, and as we all know, breaches in our security have taken place time and time again. The Joint Strike Fighter [JSF] Program highlights the vulnerability that currently exists today. Our charge is to help you get the job done, and that is what we are here for, so thank you.

Mr. SMITH. Thank you.

Just in connection, I had one further thought. It is not just a matter of cyber security preventing attacks. We need to look at our entire system's—our entire IT [information technology] infrastructure in terms of what we need to get out of it and how to best make that system work on a variety of different needs including, of course, making sure that it is protected from our adversaries or those who wish to do us harm.

With that I will introduce the panel. I will go—introduce all of you, and then we will just start with Mr. Krieger and work our way across the panel.

As you have noticed, there is five of you, and try to keep your testimony between five and ten minutes at the most. We don't want to go on too long before we get into the interaction. I know that is very difficult on a subject this complex, but appreciate your cooperation so we can get into the questions from the members.

So I will introduce the panel. First we have Mr. Mike Krieger, who is the deputy chief information officer for the U.S. Army; Mr. Rob Carey, who is the chief information officer for the U.S. Navy; we have Lieutenant General William Shelton, United States Air Force, chief of warfighting integration, chief information officer, Office of the Secretary of the Air Force; we have Mr. Robert Lentz, who is the deputy assistant secretary of defense for cyber, identity management, and information assurance—that sounds like a complicated job, and it is; and lastly, we have Lieutenant General Keith Alexander, who is the director of the National Security Agency.

We appreciate all of you being here. We look forward to your testimony and to the Q & A that follows.

Mr. Krieger.

STATEMENT OF MIKE KRIEGER, DEPUTY CHIEF INFORMATION OFFICER/G–6, DEPARTMENT OF THE ARMY

Mr. KRIEGER. Good afternoon, Chairman Smith, Congressman Miller, and distinguished members of the subcommittee. As the United States Army's deputy chief information officer and deputy G–6, I am pleased to appear before the subcommittee this afternoon to discuss the Army's activities to address the challenges to enhance mission assurance in cyberspace as a warfighting domain.

The Army believes that our enterprise network, known as LandWarNet, must be viewed as a critical enabler for the warfighter. This requires a change in our culture for which the Army is revising policies, management of people in the network, and enhancing technical capabilities to better detect, assess, and respond to cyberspace attacks.

The Army is transitioning to a continental U.S.-based expeditionary force. To support this force the Army is adapting our institutions and LandWarNet. General Casey recently signed a memorandum to transform LandWarNet to a new Global Network Enter-

prise Construct, or GNEC, that is more secure, economical, and seamless. General Casey also designated the Network Enterprise Technology Command, reporting to the chief information officer, as the single command for network operations of the Army's generating force networks.

The Army is implementing many new policies to improve cyber security. These policies concentrate on protecting information, defending systems, and creating an empowered workforce.

Addressing the management challenges of training our cyber warriors and protecting our network remain top priorities in the Army. The Army is reviewing the development and tracking of its overall workforce and looking to update the career management fields for conducting cyberspace operations.

Successfully mitigating cyberspace attacks and vulnerabilities requires unity of command and effort not only between the Army, other services, and the combatant commands, but within the Army staff. We have realigned organizations to streamline the command and control over the network and are creating an Army Cyber Task Force to better define and oversee cyberspace operations.

To meet the many technical challenges the Army faces, we have taken many initiatives, which include a data-at-rest encryption solution, a secure two-way wireless capability, and we are working with the defense industrial base to protect technologies used to build our future networks and major weapons systems.

In conclusion, the Army is taking action to mitigate persistent cyberspace threats. Using GNEC, the Army is addressing the challenge of changing the culture to view the network as a critical enabler for the warfighter. The Army's commitment to transforming LandWarNet will ensure commanders have the ability to control, defend, and fight the network as one enterprise.

I thank the subcommittee for affording me the opportunity to share the Army's activities to operate and enhance missions assurance in cyberspace as a warfighting domain. This concludes my remarks and I look forward to answering your questions.

[The prepared statement of Mr. Krieger can be found in the Appendix on page 34.]

Mr. SMITH. Thank you very much.

Mr. Carey.

STATEMENT OF ROBERT J. CAREY, CHIEF INFORMATION OFFICER (DONCIO), DEPARTMENT OF THE NAVY

Mr. CAREY. Thank you, Mr. Chairman.

Chairman Smith, Congressman Miller, distinguished subcommittee members, thank you for the opportunity to appear before you today. I provided a written statement and request that it be entered into the record.

I would like to use this time to briefly highlight some of our key initiatives that will ensure the Department of Navy's success in the cyberspace domain. It is a time of great change, and as the Department of the Navy chief information officer, I have the honor to work across the entire Navy-Marine Corps team, harnessing the power of information technology for our sailors, Marines, and civilians.

Our efforts in the cyberspace domain span our mission sets and mandate that we defend the information for the warfighters as well as protect the privacy of our naval team. The cyberspace domain is one in which we must prevail. The department remains on a course for interoperable, net-centric operations that will link warriors, sensors, networks, command and control platforms, weapons, and commanders, into a networked, distributed combat force.

Key to our success will be the ability to balance the polarity between the need to share information and our requirement to protect it against cyber threats. We have made great strides in the areas of policy, management, and technical challenges that are enabling us to achieve this balance.

Together with our industry partners, we have created an enterprise network structure comprised of the Navy/Marine Corps Intranet [NMCI], the department's shore-based network; Information Technology–21, for our float forces; ONE–NET [OCONUS Navy Enterprise Network], for our Navy outside of CONUS [continental U.S.] forces; and the Marine Corps Enterprise Network; as our contribution to the DOD [Department of Defense] vision of a trusted, dependable, ubiquitous network.

We have seen the power of a singe enterprise network improving access, control, interoperability, and information security, and as we move toward the Naval Network Environment 2016, our continued consolidation using the Next Generation Enterprise Network and a defense-in-depth and breadth, will further enable our ability to serve the warfighters with assured information.

Our computer network defense efforts are comprised of a broad array of initiatives to ensure a defense-in-depth, and while we are making progress, much work remains. We leverage industry best practices and standards, such as public key infrastructure encryption, data-at-rest encryption, and host-based security systems, to strengthen our cyber security.

Our brave sailors and Marines deployed far from home in harm's way are the heart and soul of our organization. What they know and how they translate that knowledge through sound decisions into action will define how successful we are. And so we are committed to providing them the information and tools they need to stay current and defend the cyberspace domain in an increasingly complex technology-based environment.

Thank you for your support of our information technology initiatives and our efforts to achieve net-centric operations and decision superiority. I am happy to answer any questions that you may have.

[The prepared statement of Mr. Carey can be found in the Appendix on page 44.]

Mr. SMITH. Thank you very much.

General Shelton.

STATEMENT OF LT. GEN. WILLIAM L. SHELTON, USAF, CHIEF OF WARFIGHTING INTEGRATION, CHIEF INFORMATION OFFICER, OFFICE OF THE SECRETARY OF THE AIR FORCE

General SHELTON. Good afternoon, Chairman Smith, Congressman Miller, distinguished members of the subcommittee. I am pleased to be here today, along with members of the DOD's cyber

leadership team, to appear before you and address our efforts to meet the challenges in the cyberspace domain.

Several years ago the U.S. Air Force recognized the growing importance of cyberspace. On December 7, 2005, we took the unprecedented step of adding cyberspace to our mission statement and placed that domain on an equal footing with our more traditional operating environments of air and space.

Since that time, we have been moving forward to organize, train, and equip our Air Force for both defensive and offensive capabilities in cyberspace or joint operations. As we have continued our study of cyberspace, we are finding that the most significant challenge we face is the constantly evolving nature of the threat in cyberspace. Threats in cyberspace move at the speed of light, and we are literally under attack every day as our networks are constantly probed and our adversaries seek to exploit vulnerabilities in our network enterprise.

I would like to thank the committee for its support and for this opportunity to highlight the outstanding efforts that the dedicated men and women of the United States Air Force [USAF] to help secure the nation and cyberspace. This domain is both highly complex and extremely challenging, but it is one that the Air Force is fully embracing.

Thank you again, and I look forward to your questions.

[The prepared statement of General Shelton can be found in the Appendix on page 54.]

Mr. SMITH. Thank you, General.

Mr. Lentz.

STATEMENT OF ROBERT LENTZ, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER, IDENTITY MANAGEMENT, AND INFORMATION ASSURANCE, AND SENIOR INFORMATION ASSURANCE OFFICIAL, DEPARTMENT OF DEFENSE

Mr. LENTZ. Good afternoon, Chairman Smith, Congressman Miller, and members of the subcommittee. I am pleased to appear before the subcommittee to discuss initiatives to enhance the department's and the nation's information assurance cyber security posture.

This is a critical priority in the Department of Defense. With information and information technology assets distributed over a vast enterprise and with diverse domestic and international partners, we know that we can not execute operations without the GIG, Global Information Grid, or the DOD network.

The GIG is where business goods and services are coordinated, where medical information resides, where intelligence data is fused, where weapons platforms are designed, built, and maintained, where commanders plan operations and control forces, and where training, readiness, morale, and welfare are sustained. Maintaining freedom of action in cyberspace is critical to the department and to the nation.

Therefore, the department is focused on building and operating the GIG as a joint global enterprise. This enterprise network approach, coupled with skilled users, defenders, and first responders, and in partnership with the intelligence and homeland security

communities, will allow us to more readily identify and respond to cyber attacks.

The DOD information assurance cyber security program is thus aimed at ensuring that DOD missions and operations continue under any cyber situation or condition, and the cyber components of DOD weapons systems perform as expected. There are many examples of current initiatives in my statement for the record. I will quickly highlight a few today.

To protect sensitive data on mobile and portable devices like laptops, we help make discounted encryption products available to all federal, state, local, and tribal government agencies and to NATO [North Atlantic Treaty Organization]. Since July of 2007, the resulting U.S. government cost avoidance has exceeded $98 million.

To address cyber security risks to the defense industrial base we have put in place a multi-faceted pilot for threat and vulnerability sharing, incident reporting, and damage assessment. For the global supply chain, the department has launched a program to protect mission-critical systems.

This year we are establishing four centers of excellence to support program executive offices and supply chain risk mitigation throughout the system lifecycle. Additionally, we are executing vulnerability assessments in accordance with the 2009 National Defense Appropriations Act.

We continue to rely on the national centers of academic excellence and IA [information assurance] education for critical cyber security skills. There are currently 94 centers in 38 states and the District of Columbia. One of the centers—the University of Nebraska at Omaha—cosponsored and hosted last year's fifth annual International Cyber Defense Workshop.

In 2008, the department helped bring cyber security to the Wounded Warrior Program. Wounded, disabled, and transitioning veterans are receiving no-cost vocational training in digital forensics, a critical technical shortfall for the nation and for the department. The program started at Walter Reed and is being expanded to other DOD and VA hospitals.

In conclusion, the DOD's CIO [Chief Information Officer] is working towards a resilient and defendable core network for the department and for the nation in the face of the daunting security challenges. We are preparing the GIG [Global Information Grid] and the GIG-dependent missions to operate under duress, and we are doing so under conditions of rising hostilities.

I am happy to take questions. Thank you.

[The prepared statement of Mr. Lentz can be found in the Appendix on page 66.]

Mr. SMITH. Thank you very much.

General Alexander.

STATEMENT OF LT. GEN. KEITH ALEXANDER, USA, COMMANDER, JOINT FUNCTIONAL COMPONENT COMMAND NETWORK WARFARE, DIRECTOR, NATIONAL SECURITY AGENCY, DEPARTMENT OF DEFENSE

General ALEXANDER. Well, that was quick, Mr. Chairman——

Mr. SMITH [continuing]. Astonished. We moved very, very quickly through that.

General ALEXANDER. I won't slow it down.

Mr. SMITH. No——

General ALEXANDER. Mr. Chairman, Ranking Member——

Mr. SMITH. We are ahead of schedule at this point.

General ALEXANDER. Well, I don't know enough to fill it up, so I will talk briefly here.

I would like to just give you a little bit of background about what NSA, the National Security Agency, but more importantly, what the Joint Functional Component Command [JFCC] for Network Warfare is doing in network operations—where we are, where we are going, and the way ahead, because I think it leverages off of what my colleagues have already brought up. It has to be a team to work this across the services, within DOD, to set up the right apparatus. So I will end on that.

Let me go back to the beginning, and if I could, just hit briefly on World War II, and in World War II, just hitting on some of the key things that happened in World War II, specifically Enigma and Red and Purple, the Japanese encryption systems and the German encryption systems. The reason I bring those up, as you may recall, the Germans had Enigma; we broke it—actually the Poles and the Brits broke it; and in 1941 Admiral Dönitz understood that it was broken and added a fourth rotor to make the decrypting of those communications more difficult.

From January to March of 1942 the United States lost 216 ships off the cost—off the East Coast, and our efforts in Europe were going down rapidly. We were able to break that collectively, with industry, Army, Navy, working together with our allies, and it changed the balance of that war.

And if you think about it, we broke their encryption, we broke the Japanese encryption, and they didn't break ours. And that was huge for warfighting.

The network that we have today has taken what was an analog network to a digital network, and a consequence of that change, going from analog to packets, is huge. It allows us to leverage things like iPhones, the iTouch—I have 11 grandchildren, and they have these little iPod Shuffles; they are hooked to the networks. They can do things at seven years old—they are googling on the network. They are linked—the same network. One network.

Great things are possible. Our military leverages that today for great good—for command and control, for integration of our intelligence with operations, with logistics, with everything we have on the battlefield. Great opportunities, great vulnerabilities.

And with those vulnerabilities comes the reason we really have to focus as a team on cyber security. The way we are approaching it today does not work.

Recently, commander of STRATCOM [Strategic Command] delegated to myself under net warfare [JFCC–NW], the responsibility for directing the defense and operations of the GIG as well as our current role for net warfare, so that we have all those missions together so that we could put the defense and the offense together for the good of the Defense Department.

As you saw in my written statement for the record, the Defense Department is considering an option to stand up a sub-unified command that would allow us to leverage the defense and the offense for the good of our forces around the world to ensure that we have the communications availability, the integrity of our communications, and the reliability that we need to conduct our missions abroad. In order to do that, the services and the joint community has to work together to support our regional combatant commands.

So I think what each of the services has said and where we are is now we are looking at the steps of what we have to put together in the sub-unified command as an option, or in a Joint Functional Component Command—how will we put these capabilities together to ensure our networks are secure and provide us freedom of maneuver in cyberspace?

So with that, a lot of work to be done is ahead of us. I think where the Defense Department is today is in a good place and moving up. We understand the problem; it doesn't mean that there aren't issues with training, with equipping, and with the tactics, techniques, and procedures that we have to do, but I do think that we have come up with a way of working together to face these and to come up with a good plan for the future.

So with that, Mr. Chairman, I turn it back over to you.

[The prepared statement of General Alexander can be found in the Appendix on page 94.]

Mr. SMITH. Thank you.

And we will—in questions we will observe the five-minute rule. Hopefully—we got great very brief statements by our witnesses—we will have time to go around more than once. But just to keep it flowing we will make sure we keep everybody to five minutes, including me.

My first question is just sort of a follow up on that last point about how coordinated the effort is in the Joint Functional Component Command. So when you look out across DOD, and certainly we have many of the key components here—Army, Navy, Air Force—and if you are in your position, or STRATCOM's position, or even a higher up, and you are going, "How secure is my network?"

How compartmentalized is that and how coordinated is that? You know, how much do you guys get together on a regular basis so that you, as the person in charge of that, or the Secretary of Defense, or somebody higher up can say with confidence, "Our network is secure and we are paying attention to the different pieces of it."

Or, I guess the better question is, to know the vulnerabilities—to know in a coordinated fashion so that it is not stovepiped, because as you know, in this situation, in many cases, you are only as strong as your weakest link into the network. How do you do that coordination within DOD?

And then I have a follow-on question about how you handle the interagency piece. But just starting in DOD, and you touched on that a little bit, but if you would get more specific about how coordinated that effort is.

General ALEXANDER. I will hit the first part and then I will let Bob and some of the others——

Mr. SMITH. Okay.

General ALEXANDER [continuing]. Pick up on that. We direct the defense of the network to the Joint Task Force–Global Network Operations. Lieutenant General Carroll Pollett, from the Defense Information Systems Agency [DISA], is the commander of the Joint Task Force–Global Network Operations and works for me in that regard, and his day-to-day guy is Brigadier General John Davis. They put out written guidance of how to defend the network—the unclassified and the classified networks.

I would like to say that our networks are secure, but that would not be correct. We do have vulnerabilities.

And the issue, and one of the things that we have wrestled with over the last six months, is a strategy for closing those vulnerabilities very quickly. I think we are making good progress on that, because the level of problems that we have had with things like Conficker and others have been greatly diminished because of the great steps that have been taken by Global Network Operations but implemented by the services.

Mr. SMITH. And what were some of those steps, if you could walk through the specifics here?

General ALEXANDER. Well, let us see. In an unclassified forum that becomes very difficult. It would be the way that you use removable media, would be a great case in point—how you have to use removable media or not use it in a network, what the restraints are, dictating those restraints, how you have your Information Assurance Vulnerability Analysis IAVA compliance out there, which means, do you have your McAfee or Symantec antivirus software up to date? Are you using the latest update? Have you scanned your system for these things? And ensuring that those kinds of things are done.

How do we tell that at a global scale? Others' mission is to look on the periphery and see if we see problems on the network.

I would like to give you one key element here I think is crucial to it. If we try to defend our networks like we do a castle—the moat—we will never be successful. We have to defend it on the network globally, because that is how it exists on the network.

And so that means we and our allies in industry and government have to work together in this enterprise. That is going to be key to our success.

Bob, and——

Mr. LENTZ. I will give you two examples, Mr. Chairman, to your question. First of all, one unclassified example of the cooperation at a technical level is the Federal Desktop Core Configuration.

The fact that we locked down the computers so tightly at our endpoint within the DOD network working with the services—in fact, the Air Force led that effort—and Microsoft, which is our most ubiquitous product throughout the Department of Defense, is locked down in terms of the stable configuration, and that has allowed us to defend the network much more effectively. I think that is a technical example.

To your first question regarding the cooperation within the Department of Defense, one of the things that—we have a DOD CIO policy that has been fully implemented is, we align every single service and agency within the Department of Defense to what we

call a computer network defense service provider, or a Computer Emergency Response Team [CERT]. So every entity in the Department of Defense, from our schools to our main military operations, are aligned to certified CND [computer network defense] service providers, and those CND service providers work together under the leadership of STRATCOM and the JTF–GNO [Joint Task Force–Global Network Operations] working in partnership with NSA and the law enforcement community part of our infrastructure to work on these cyber events. So I think that is an example of the cooperation that goes on within the DOD.

Mr. SMITH. Okay.

I will yield back the point and yield to Mr. Miller.

Mr. MILLER. Thank you, Mr. Chairman.

Could you talk about the role that you think the federal government should play in securing the networks of our defense industry partners?

Mr. Lentz.

Mr. LENTZ. Clearly, it is absolutely essential, in terms of having a robust capability in the face of the cyber attack, is, we need a partnership in every tier, from our international partners—we have found on one cyber event after another cyber event that they have insights that are very critical for us. Plus, just because of the nature of the geography, our international partners oftentimes will have an advanced warning to give us insight into cyber events.

At the domestic level, we team with the major centers across the cyber landscape, to include the counter-intelligence, the law enforcement communities, and of course, all the CERTs [Computer Emergency Response Teams]. And at the industry level, it is absolutely essential we team with the ISPs [Internet service providers], we team with Carnegie Mellon, we team with all the industry leaders in this area to gain insight into cyber events, particularly when it comes to vulnerabilities in which we have to have advanced notice in today's cyber environment.

Mr. MILLER. General? Would you like to answer?

General ALEXANDER. So the role that—just to take up where Bob left off—so one of the roles that the intelligence community and the Defense Department is going to have is, how do you make those identifications of the vulnerabilities and the signatures and how do we work those with industry and other government entities so that they know how to defend their system?

I think if you take the analogy that I was talking about, this—we are defending a castle today, but we want to defend our network and perhaps our allies' networks, then you are going to have to have an early warning capability that exists between networks to tip and cue on problems that are coming. I think that is going to be key for future problems that we face—for example, some of these robot networks, or botnets, that are out there, and things like that.

How do you defend against them? It is going to take our country and our allies to work together and tip and cue at network speed to defeat them.

Mr. MILLER. How does the DOD ensure that we—you had mentioned the word "robust"—have a robust computer network defense

and information assurance structure in place but we don't replicate across the service lines?

Mr. LENTZ. Well, I think we actually do have a very robust capability working with the services. As I mentioned, early the CND [Computer Network Defense] service provider program that we have—we have 23 different CND service providers across the Department of Defense, of which the services make up a good share of those. And each one of those CND service providers coordinate constantly in real time what is going on in cyber events.

Mr. SMITH. Mr. Marshall for five minutes.

Mr. MARSHALL. Thank you, Mr. Chairman.

I wonder what the limits of the effective partnership between DOD, or the nation generally, and business might be—the private sector might be. I was involved in an enterprise at one point that decided it was going to acquire a bunch of laptops that each individual employee would then use to enter data while they were out. We had a range of possible laptops that we could pick, and some of the more expensive laptops were less vulnerable to damage if they were dropped, if, you know, they were exposed to water, to heat, et cetera, and then there was the question of weight, and typically the ones that were less vulnerable were also heavier, and so we ultimately decided we were going to go with the lightweight one because we could, in our circumstances, not have to worry too much about things being dropped or subjected to water or heat.

I assume that for some of the applications that we might use laptops for where the Army is concerned and the services are concerned, going to go with the heavier version that can handle them. And I wonder if those—I am sure that those same kinds of decision-making differences between the private sector and the public sector exist with regard to the issues that you all deal with that are way above my pay grade. And I am wondering if you can describe where it is that your interests diverge or your objectives diverge in ways that will make the partnership more difficult.

General ALEXANDER. I will take a first whack at that, sir. Let me just give you my thought, and that is, where they converge are where it is in our nation's interest to ensure those networks exist and can function and they are reliable—our power grid, our critical infrastructure at large. We have, I think, there a responsibility to partner with industry to assure that our nation can operate in a time of crisis, and the government has some kind of role there and I think we have got to determine—and I think some of the stuff coming out of the 60-day review and other studies will look at, so how do we partner with industry to do that?

Our partnership might be giving them early warning, sharing with them threat data, and helping them secure their networks with some of the standards that Bob talked about, in terms of how you would set up your desktop configuration to active tipping and cuing to defend their networks. One of the key things that industry has done on the network is their intellectual secrets, their financial—wealth, all that is stored on the networks, their personal data. Much of that is an industry, I think, responsibility to secure, and government would support in some way.

So I think that is where it starts to diverge, as you get industry that is out there on its own—there are some things—you know, our

own personal communications from my wife to myself—that doesn't need government, and if that goes down, well then I won't buy the milk and bread tonight. I will be good.

But, you know, our personal communications aren't a national priority, so I think you are going to have that range from those things that are, how do we ensure the security of our nation, so that if a network attack blossoms into a warfare we know where that line is.

Mr. MARSHALL. There is no question a tremendous opportunity exists for synergy here and for taking advantage of the private sector's obvious interest in protecting data. I mean, literally billions or trillions of dollars are at stake, you know, besides personal private information.

And so the private sector is paying top dollar to the best possible minds to protect the infrastructure that holds access to those kinds of money flows, to that kind of private information. I am wondering where it diverges in any substantial way.

General ALEXANDER. Well, I think part of the divergence is that, you know, they are going to harden like a shell for theirs, but the government is going to operate across a global thing with our allies, so we have a global responsibility. You can harden a network for an industry within a network and almost sever it completely and have that almost ensured security.

Where we have to have an Army in the field, or an Air Force in the field, or a Navy out there, they are going to have communications that are both wireless and wired, and as a consequence they are going to have vulnerabilities that are far different than what industry might have. Now, having said that, it doesn't necessarily mean that there aren't things that we couldn't work together with or should work together with; I think there will be.

So I think you will have all the way from the far you know, all the way over here on the far right, those things that we are not worried about and even if somebody loses them, to those things that we are worried about as the national interest; and then take the other axis that you were doing, the economic access, from those things you don't worry about somebody hitting over here, perhaps, in one level of industry all the way over to the banking industry and security of those. And both of those at the far end of that—the banking industry and our national military command authority—both have to be secured with the best that we have. And I think there is great synergy here and great divergence at the other end.

Mr. SMITH. Thank you. If you have something quick, I want to make sure we keep moving to the other members. Mr. Thornberry.

Mr. THORNBERRY. Thank you, Mr. Chairman. If we are literally under attack every day and are to treat cyber as a domain of warfare, like we have treated others, it seems to me we have to have the legal, policy, and doctrine discussions as well as funding, training, equipping, and all the things that go with domains of warfare that we are serious about.

General Shelton, you mentioned the Air Force has been in front on this. Does the Air Force have a specific plan to implement what Secretary Gates talked about in quadrupling the number of people trained in cyber warfare?

General SHELTON. Yes, sir. We are moving out on adapting courses—adopting courses. There are joint courses we are pursuing that are already in place. There are new ones that are standing up.

We are changing the way we train at our training centers, both officer and enlisted, and also creating training opportunities for our civilians. So the answer is, absolutely. We are trying to expand our universe in terms of trained people in this area.

Mr. THORNBERRY. But is that down to the point where there is a piece of paper that shows, we are going to ramp up our training to meet this specific number that he talked about that has been signed off on?

General SHELTON. We aren't there yet, sir, to the actual numbers, but we do have a way ahead in terms of concept. But is it numerically in place? It is not.

Mr. THORNBERRY. I am just trying to understand how far we have gotten towards being serious—and I am not picking on you, particularly—but just how far we have gone to being serious about some of these tough issues.

General Alexander, to pick on you a little bit—not really pick on you, but——

General ALEXANDER. Thank you.

Mr. THORNBERRY [continuing]. But what are the policy and legal issues that we need to be thinking about? I mean, a lot of this is the stuff that is in you all's bailiwick, and we have got to oversee the funding and so forth, but it seems to me there are some legal policy issues that are our responsibility. What are they?

General ALEXANDER. I think one of the clear ones—what you would expect us to do is to defend our networks, and we have the right to defend our networks and to keep adversaries from getting into our networks, to secure our classified networks and all of that. And I think there is inherent right, and we have the legal framework to go ahead and do that.

Here is where it starts to break down and where I think you, with the administration and others—the discussion that we are now going to enter into. I think once the 60-day review has come up, and so now going back to the earlier question, so what is that role and responsibility primarily with DHS [Department of Homeland Security], because they will have to lead for the rest of the dot-gov networks and for that partnership with industry, so what is the legal framework for sharing threat signatures with industry that are classified? How do we do it at network speed so that it is defensible? And what is that legal framework and what is that operational framework?

And those are areas that technically are easier to do than they are to set the legal framework up, because you have industries—for example, your antivirus community. If we give them a classified signature, how do we ensure it is not given out so widely that our adversaries have it when they are a global antivirus community? Things like that we are going to have do look at. There is a whole series of issues, I think, in those realms.

Mr. THORNBERRY. Well, for example, when the Constitution says Congress has the responsibility to declare war, what does that mean when we are under attack every day? How do we deal with warfare in cyberspace?

General ALEXANDER. Well, I think the loose use of the word "under attack" and "warfare" is probably more accurately described as people probing our network. We call that, I think—others loosely call that an attack on your network, but it falls short of what I think we would legally look at, and I have got the head lawyer back there right behind me, so he will raise his hand and make sure I say this right, but——

Mr. SMITH. He was nodding his head. Let the record reflect it.

General ALEXANDER. This way, or this way?

Mr. THORNBERRY. Well, was Estonia or Georgia under attack, and was their infrastructure under attack in a way that, you know, gets closer to that declaration of war?

General ALEXANDER. No, I think you are starting to—on those you are starting to get close to what would be. The problem that you have there is who. The attribution. And so I think what you have is the inherent right to defend first, and attribute, and preferably to do those at network speed. So what we just agreed on, I think, if you agree with those two statements to do those both at network speed, is the reason that we need the defense, the exploit, and the attack to work synonymously as a team at network speed to do just that.

Because if we don't—if we leave the defend, to defend itself and they are getting hit over here and somebody says, "Hey, did you know they are getting hammered? The Air Force is getting hit on the network," we would say no, we didn't. It has happened to our industry players. And so if you are not aware of it you can't help mitigate it, you can't help attribute it.

So that partnership has to come in. I think in the legal framework it starts to go up to, when is it going from exploit to damage? And in that change is where you go from what I will call spying operations into warfare.

And there is, I think, a more specific set of terms that would define those, and—did I get all that right, Bill?

Mr. SMITH. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Gentlemen, thank you for your testimony here today.

To continue on that line, General Alexander, clearly the tools available to us in cyberspace are very powerful. I know the NSA, in particular, is very good at what we do. How far down the road are we in really setting the rules of engagement, and who and when do those decisions get made?

Clearly modern warfare has forever changed; we will never have a conflict in the future that doesn't have a cyber component to it. And where are we on that stage, you know, in terms of where we escalate to the fact—to where we would attack and cause great damage in response to an attack on our own networks? Where are the rules of engagement at this point, and who is going to make those decisions along the way?

General ALEXANDER. Well, I think if you start out within the defense community, those rules for defending, exploiting, and attacking on the networks as part of war fall within the Defense Department. I think we can easily envision—there was a Chinese PLA [People's Liberation Army] statement in 1996 that said something

to the effect, "If you want to attack the United States, attack its banking system."

Now, the issue—this complicates it and it puts us into answering your question more accurately. It gives you a understanding that it may not be the Defense Department that is attacked.

But if we assume symmetrically that they would attack us, the Defense Department, and the Defense Department would respond back, you are now into one form. The issue, I think, that realistically faces us, though, is that it would be asymmetrical. It would go against our industry, and it might be our critical infrastructure.

And then the question of the partnership between the Defense Department, Homeland Security, and the intel community has to be clear. We have to have laid out those rules and walked through that. We are walking our way down that; we are not far enough.

I think within the DOD we have laid out the legal framework for what constitutes an attack, how we defend our networks, what we do in that—specific to the Defense Department for DOD operations, for example, on the war on terror.

But that is a very limited and a very focused set. I think to really get to the heart of your question, you have to have that partnership and we have to operate seamlessly across all of those if we are going to be successful. And that is going to take some work.

Mr. LANGEVIN. In the CSIS [Center for Strategic and International Studies] report, the commission that I co-chaired and worked on with a number of others, one of the things—the conclusions—that we came up with was that the president should make clear that cyberspace and our cyber assets are a national asset and that we will use full assets of national power to protect it. Do you agree that it is time that we have, perhaps, a cyber Monroe document that lays out clearly what our response would be in terms of protecting our cyber assets?

General ALEXANDER. I do.

Mr. LANGEVIN. Let me add——

General ALEXANDER. There is four others that—you want to—I do. I think they do, too, but I don't——

Mr. LANGEVIN. Anybody else?

General ALEXANDER. But, I don't want to speak for everybody.

Mr. SMITH. I guess the follow up to that, what would be involved in making sure that that is clear? Is there an executive order that is needed? And following up a little bit on what Mr. Thornberry was asking about in terms of your authority to act—is that understood, or is there more action that is needed to allow you to have that authority?

General ALEXANDER. Well, I think what the 60-day review is looking at is taken right from your study and others and saying, "So how do we start that at the top? What is the White House role in doing that?" And I think they are going to set that up and say, "Here is the White House role," and lay that out.

So that is yet to be fully disclosed, and I think they have got a couple more steps to complete that. But my gut reaction is that they will do essentially where you are, so we have to set up a national leadership for it at the White House. Roles and responsibility to the Defense Department, DHS, our partnership with industry,

and our partnership with allies needs to be clearly documented. And I think we have to start walking down that road.

The follow-on question is, okay, so you have these—you have the legal framework that we talked about, that has got to come up. You have to have the operational framework. And I would submit that first we have got to lay out operational frameworks that will work.

There are operational frameworks that people can put on the table that just don't make technical sense, so that is where our partnership with industry really has to come to the forefront. What technically can we do to secure those networks with the Defense Department, the intelligence community, and DHS, and industry, and then how do we take that—what do we need legally to make that work? And I think we have yet to walk through those, and I think the first step will be when the White House puts out that 60-day study.

Mr. SMITH. Ask a little bit about acquisition issues, and maybe have the three individual services speak to their ability to acquire what they need technologically, because there is the challenge in the IT world that basically Moore's Law runs headlong into the acquisition process. You know, things update very rapidly, and yet it takes a couple of years to go through the ability to acquire systems.

Now, I know reforms have been made to a certain extent within IT to give greater flexibility to enable you to purchase more equipment more quickly. How well is that working, and what more do we need to do to make sure you are able to buy the equipment that you need? And just if each one of you could sort of give a little vignette from your experiences within your individual service.

General Shelton.

General SHELTON. Glad to start. You are exactly right. We have a real challenge of what I would call an industrial age acquisition process trying to operate in IT space, which is not adequate. We have vehicles that we can use to acquire IT solutions, and in many cases those are commercial off-the-shelf products or commercial off-the-shelf products that we slightly modify and adapt to our purposes. In some cases, the question is scalability, but beyond that those solutions are there.

So I think we are in reasonably good shape from the overall capability to acquire. It is that we don't often exercise that capability the way we should, so——

Mr. SMITH. Why not?

General SHELTON. We sometimes revert to the way we have always acquired. So we are forcing that inside the Air Force. We are forcing that toward much different solutions, and we are forcing an architecture that will allow much different solutions——

Mr. SMITH. Well, Mr. Carey, if you could talk a little bit about Navy's experience with the Navy-Marine Corps Intranet, which was a big transition system in terms of the software being put in place—how difficult was that to acquire? Or just more broadly within the same acquisition area, what challenges are you facing? What do you think needs to be done to overcome them?

Mr. CAREY. NMCI [Navy Marine Corps Intranet], sir, was a huge culture change to the department in the IT space. To move from a system of lots and lots of networks controlled by individual unit commanders or organizational commands through a homogeneous,

centrally-controlled network apparatus was just a huge culture change, so it took some time to get there.

The acquisition process allowed us to get there——

Mr. SMITH. Okay.

Mr. CAREY [continuing]. In a reasonable amount of time, but imagine that it is now the largest intranet in the world, so grew from having hundreds of networks—we are not subsumed by one—using the process.

Mr. SMITH. Okay.

Do you have anything you want to add?

Mr. KRIEGER. Sir, I think your discussion on the acquisition process not being agile is really a cultural issue.

Mr. SMITH. Okay.

Mr. KRIEGER. So I think within the acquisition process, both legislatively and regulatorily, the agility is there. This is a cultural change for the department. Can we deliver spiral capabilities—not a full capability—quicker and spiral it out, versus the culture has been to deliver a completed product over time?

Mr. SMITH. Well, does that also feed into sort of how personnel are rewarded and/or punished depending on how they do things? That basically there is a culture that says, "Hey, as long as I am following the process, as long as I am going through the acquisition process there I am good. If I step outside of it I am in real danger"?

Because it strikes me that it would really take, you know, creative personnel who understand IT to say, "Hey, I need this solution now. I am going to go do it, not go through the normal process as empowered."

And I can see where you might be limited within the military concept, people saying, "Look, if I do this, you know, I am not going to be rewarded for it if it goes well and I am sure as hell going to be punished for it if it doesn't go well." Is there a problem with that in terms of changing how we promote and reward behavior?

Mr. KRIEGER. Sir, I know within the Army in the current global war on terrorism, we are at the point in the Army now that when we generate a requirement from the field of JUONS [joint urgent operational needs statement], and we document it, we are delivering capability real quick now. And so I think that culture is changing, and we certainly have soldiers, and sailors, and airmen in need now, but we are discovering, culturally, that it is possible to deliver IT quicker and outside—within the system but not the traditional way that we build airplanes and ships and things. And certainly there is lots of examples in the current war where we have identified a problem, we have documented the requirement, and we have delivered spiraled-out capability.

Mr. SMITH. Thank you. I very much appreciate it.

I will go to Mr. Miller and then I will go to Mr. Conaway, who walked in right at the end of the questioning there, but we don't want to get you out of the loop there, so we will go to Miller, Conaway, and then back to the other.

Mr. MILLER. Thank you, Mr. Chairman.

One brief question to General Alexander, if you would, in reference to the new idea of the new sub-unified four-star: Will DISA and NSA be rolled into the command and how will the relationship

between DISA and ODNI [Office of the Director of National Intelligence] be affected?

General ALEXANDER. It is not clear, in my mind, that it would—it will not be rolled in, per say. I think that part—it will be leveraged in the foundation for it. I think we have to have the synergy between what NSA does for the intel community, for what NSA does for the cyber community, and those are inextricably linked.

So, specifically today, we have JFCC–NW at NSA, and as a consequence of having them there at NSA they can leverage the different offices that look globally to do their mission. I see that—we growing that connective tissue between what NSA is doing and what this command is doing.

I think there are some things that will be in common that we are going to have to put in both in the concept that is being looked at, and that is, how do we see cyberspace? An integrated cyber operations facility. What is it that you see for your defense? How do you see your network boundaries?

What do you see globally? What do our allies see? What is going on on the network? And how do you mitigate and attribute, going back to the question?

Because if you can't see it you are not doing it in real time. So how are you doing that in real time? How are you bouncing those back and forth?

So what I imagine will happen is, we will put the pieces together at Fort Meade, at least in the recommendations and the thing that is under consideration, and then look at how you build the command to specifically do cyber operations, leveraging what NSA brings in network exploitation. And I think that is the key part, is to have them coexist.

In that respect, the DNI [Director of National Intelligence] is comfortable and a proponent for it, because it does both. I think it is good for both of us and we can do both, in that regard.

The second question—the logical question that stems out of that, and what is your relationship with DHS because they need some of the same support? We see that that is a foundation that DHS can lean on—a technical foundation—while DHS takes on its missions to operate and defend the rest of the dot-gov networks.

Mr. SMITH. Thank you. Mr. Conaway.

Mr. CONAWAY. Thank you, Mr. Chairman. Since I just got here I will not replow——

Mr. SMITH. Thank you. Mr. Marshall.

Mr. MARSHALL. Thank you, Mr. Chairman. I would like to return to the line of questioning that I had when I was—just a minute ago, and it is again, where is it that you perceive the private sector's interests, motivation diverging from ours?

And General Alexander, you described, you know, a private sector company that might be able to—that had a similar interest because billions of dollars are at stake, or very, very sensitive information was at stake so they wanted to protect that information. And being able to harden itself, and its use probably more so than we could, practically speaking, given the cost associated and given the kind of uses that we have to make of information technology across the military.

But can you give other examples that would help me understand how they diverge, and would—this is a question to all members of the panel, not just General Alexander.

I know, Mr. Lentz, you were about to say something and I had run out of time.

Mr. LENTZ. Well, I can give you a couple examples of that. I think the biggest challenge we are going to have—and I think the laptop example that you alluded to in the beginning is a good example of that—when we did our data-at-rest encryption policy, we went out to industry, established a standard, we worked with industry to figure out where that bar for security needs to be and where they can meet that bar at the cost and operational effectiveness that meets both entities' standards, for them to make a profit, but also for us to be able to get the most secure capability out in the field.

We did that very quickly over the course of several months. We developed the standard, and we have 12 companies that bid competitively for that process.

The cost for a data-at-rest piece of software license would normally cost you $200 if you went and got it yourself. Because of this competitive standard-based process, we dropped the cost to less than $10 per software license. Now, that is an example where we had convergence.

Now, as the bar goes higher in cyberspace because the cyber threat is increasing exponentially, we have to work with industry to build in much more robust capability. And that is not just dealing with encryption, but all the aspects that go around hardware and software.

And that is where industry is going to have a more difficult time, because as that bar gets raised, their profits start to decrease. And that is where we have to look at the government-private sector partnership to figure out how we can get that bar raised in a cooperative way, at the same time maintain the competitive acquisition process.

General ALEXANDER. My experience with industry, though, is there is more convergence than there is divergence. They see the obvious rationale for securing the networks just like we do.

More importantly, they also see that they, in part—many of the industry folks that I have talked to said, "We need government support here." I don't think they want government compelling them to do things on the network, but I think they need government support in securing it and developing a framework—a technical framework—that is securable.

That is probably going to be impossible, so how do we get as close to that as we can? I think industry is absolutely looking for partnership with government and with our allies setting up some solution like that.

So my experience has been almost completely convergent in that regard. I have not seen—I asked one industry, I said, "Why don't we give you this problem?"

They said, "We can't afford to do it without government support." That was the only divergence.

We said, "Well, this would be one that we would throw over. Critical infrastructure—that is an industry thing. Why don't you take care of it?" And they said——

Mr. MARSHALL. So, industry interest is not broad enough to justify the cost, is in essence what you are saying, and so to the extent that we have got to have a certain level of security or capability, industry is not necessarily going to generate for us because either there are too many defeatist characters competing with one another with different products, and consequently different companies looking at those different products, or there are just not enough companies that are that interested in that level of security or capability?

General ALEXANDER. Banking industry clearly has a compelling need to create that existing secure infrastructure, and they are working hard to do that. There are things that government and industry—and that industry—could work together to make it even better. Your electrical power grid and some of your other ones are low cost when you look at the network.

So the power companies that are going to have to go out and change the configuration of their networks, that is a cost that if you take what Bob was saying, one further step, now to upgrade their networks to make sure they are secure is a jump in cost for them, and now you are going to have to work through their committees, through the regulatory committees to get the rate increases so that they can actually secure their networks.

So when you talk to the power industry, as an example, that is one where you are not going to look at, so how does government—because we are interested in perhaps having reliable power—how do we ensure that that happens as a critical infrastructure? So DHS and that critical infrastructure have to work together to walk through that.

Mr. SMITH. Thank you.

Mr. Thornberry——

Mr. THORNBERRY. Let me give the Army and Navy a chance to answer what you all's services are doing to train, equip, develop career paths for cyber warfare. Do you have cultural difficulties there, too, particularly in whether you see cyber as an enabler for the things that you are already doing or a domain of warfare on its own.

Mr. KRIEGER. Sir, you raised a very good issue, and the Army is trying to come to grips with that right now and studying it, and we have got a study going on by TRADOC [Training and Doctrine Command] to figure out what we want to do, both at the officer level and the warrant officer level and the soldier and NCO level.

The question is exactly on target. I don't have an answer yet, but that is what we are trying to figure out.

Mr. CAREY. We believe that everyone that engages the network becomes a cyber warrior at some point. If you are going to touch the network, you are involved in something that is greater than you might have actually thought. So changing that culture, as my colleagues have said, is something that we are working on very diligently right now as we move into our next generation network environment, and that we are bringing on more people to operate in this domain, both in the uniform side and the civilian side, to

allow ourselves that span of control that we don't have right now inside the department.

Mr. SMITH. Thank you.

I had one more line of questioning, but Mr. Conaway, go ahead.

Mr. CONAWAY. Well, thank you, Mr. Chairman.

A few of us are working on an acquisitions panel issues, and I was just wondering, Mr. Lentz, can we use the acquisition regulations and practices to incent defense contractors to be—their cyber warfare posture, to make sure they are compliant or that they are protected as they need to be to handle our data and handle our work? Is that an appropriate use of those?

Mr. LENTZ. Yes. We are working with AT&L [Acquisition, Technology, and Logistics] to look at the——

Mr. CONAWAY. AT&L?

Mr. LENTZ. I am sorry. The acquisition organization in DOD.

Mr. CONAWAY. Okay.

Mr. LENTZ [continuing]. To look at modifying the defense acquisition regs and the federal acquisition regs for including stronger language in there regarding meeting certain security benchmark standards in terms of protecting information that resides on their networks. That is something we are doing right now.

Mr. CONAWAY. And you think you will get pushback from the contractors on this deal?

Mr. LENTZ. No, we are not. In fact, they are asking for that language. No problem.

Mr. CONAWAY. All right.

And then, General Shelton, when you guys set up your cyber command, can you walk us through the rationale between why that was a numbered air force versus a four-star command?

General SHELTON. Sure. As we first started to look into this, we said a major command seemed appropriate because that is how we organize, train, and equip in the Air Force. But then as we thought more about it, we said, we are really about how do we operate? And the way we operate in the Air Force and present forces in the Air Force is through numbered air forces.

So if we are really all about trying to provide cyber operations for joint employment, it is more appropriate for a numbered air force. And then the organize, train, and equip aspects can be subsumed by Air Force Space Command. So that was the rationale.

Mr. CONAWAY. Okay. And you are comfortable with—the Air Force is comfortable, so far, that that was the right decision?

General SHELTON. Absolutely. Very comfortable.

Mr. CONAWAY. Thank you, Mr. Chairman.

Mr. SMITH. Just quickly—in terms of personnel, we talk in this committee each year about the challenges of making sure that you have the best and the brightest folks who understand the IT infrastructure, because it is a constantly evolving thing. Whatever the systems, it really comes down to people and their ability to adapt.

Just, you know, if anyone has initial thoughts. I don't know who would be best to comment on this, so I will throw it open to all of you. You know, how are you doing in terms of recruiting the personnel that you need to do the IT work that you need to get done?

Mr. LENTZ. I can start out, and then——

First of all, and I know, Congressman Thornberry, your interest is on target regarding the fact that within the Department of Defense we have over 90,000 personnel that we have identified working with the services and agencies that are deemed to be cyber warrior-type individuals. Now, these are sys admin, that manage the system, and network administrators that have part-time jobs both to defend the network as well as to administer, and you can't separate those functions.

Ninety thousand. We have a plan that we are 2 years into to certify all 90,000, and we right now have a goal by the end of this year to be at 45 percent. And so that is a major goal.

The other thing we are doing is we are adding highly specialized skills on top of them, in light of the cyber events that we have talked about, and that will add another layer of more highly skilled cyber warriors that will go to schools, like in Pensacola and Maxwell and Fort Gordon, possibly, to be able to get more in-depth training working with the National Cryptologic School at NSA and other institutions.

The fill rate overall—I will let the services comment on that—but what we are seeing right now is, the fill rate for those cyber warriors is a fairly good rate. We are seeing over 90 percent, in terms of those positions that we are talking about right now, which, by the way, are contractors, civilians, and military personnel.

Mr. SMITH. All right.

I guess just in general, in any——

Go ahead, General. Sorry.

General SHELTON. Sir, I was just going to say, in terms of technical expertise we have, certainly, a concern, along with everyone else in the nation, that there is just not that many people coming out of our schools that are prepared for the technical-type work. They don't have the educational background, haven't studied math, engineering science, those sorts of things. So we join the course of many—this is a real problem for us.

Mr. SMITH. Yes.

Gentlemen, do you have anything to add to that?

Mr. CAREY. All I would add is that we are all competing for that limited resource——

Mr. SMITH. Right.

Mr. CAREY [continuing]. Whether it is industry, Army, Navy, Air Force, Marines, we are all competing for that. And so there has not been a challenge that we have seen yet, but we will be ramping up for the coming months so we will have more information somewhere in the fall.

Mr. SMITH. Okay. Thanks.

And General Alexander, I just want to follow up quickly on the interagency aspect of cyber security. And I think from this panel we have got a pretty good idea what the DOD is doing. How do you interact—you touched on it a little bit—I mean, Homeland Security theoretically is the lead agency for the interagency piece of cyber security.

Does DOD sort of, you know, exist in their own world and work on their own systems while Homeland Security is dealing with the other aspects of it? What is the integration? How is that working?

General ALEXANDER. Well, for offensive operations we have a joint task force—joint interagency task force—which brings in all the players. We have great partnerships with FBI, CIA, and others, DHS. They sit on these panels—State Department—and look at the options and where we are, and I think that is well run.

Where I think there is work to be done, the U.S. CERT is growing rapidly, which is the DHS element that would actually do the computer emergency response team's job for the rest of the dot-gov, is taking that on in a way analogous to what the Joint Task Force–Global Network Ops and the CERTs under it does with the services. So there is some room to grow in the rest of the dot-gov to catch up where I think the Defense Department is today.

Within the intel community, I think they have a strong network security program so that that is running pretty good. What is lacking today is a integrated defense where you can tip and cue between the different government entities and agencies at network speed to defend elements of it, and that is one of the things we are going to have to grow, which I think DHS would leverage what the intel community and the DOD has today, both technically and the real time alerting and cuing. Think of that as a radar system for cyber security.

Mr. SMITH. I had one more question, but I wanted to see if any of my colleagues had anything further.

Mr. MARSHALL. I do.

Mr. SMITH. Go ahead, Jim.

Mr. MARSHALL. Thank you.

I am continuing the same line. So, different possibilities here—we have got a requirement that needs to be met that we have identified. Industry has already met that requirement, so we go out and we acquire either the software or the hardware and that takes care of that.

We have a requirement that has not been met by industry as well, and it is the banking industry. And the banking industry recognizes this need to secure billions and billions and billions of dollars of exposure that it would otherwise have. Or it is the up—you know, hardening the defense of the electrical grid, which has all these collateral public and private possible consequences if, in fact, there is a failure, that an attack is successful.

Could you describe—is there a difference in the way we go about trying to figure out the partnership and who carries what load in—here is the banking system. It is going to get there, and you know it is going to get there because there is just too much at stake. It is the brightest people in the world they are able to hire, and they are going to pay them big bucks, and they are going to get there.

But they would love to have us step up to the plate and pay for it. You know, that just makes more money for them. So there is obviously a give and take as we discuss with the banking system or banking industry who is going to do this.

And then, where the electrical grid is concerned, they kind of go, "Well, you know, we don't need that kind of level of security. That requirement is not one that we want to meet. We will take a chance on the grid going down and we will just send our guys out there and fix it. You know, actually, they might make some money. It might be better for us, in a sense, if the grid goes down."

Could you describe how you deal with those two different kinds of circumstances in order to figure out who carries the load? Well, at this—where we are talking about electrical grid, who winds up paying the freight, okay?

General ALEXANDER. I think DHS would have the lead in orchestrating that with the Critical Infrastructure Protection Advisory Committees that they have, the CIPACs, that go across each of those. And in the banking industry, it would be a DHS–Treasury partnership to look at how we do it with other players in the community. So I think you have got DHS in the lead.

The interesting part that you have put on the table is that there may be things that the government technically knows that would be useful to industry to secure their networks a degree beyond where they are today. How do we do that without risking some of our nation's crown jewels, but ensuring their protection?

And that is one of the things where I think the partnership between DHS and DOD is going to have to be laid out, and I think it is being worked. So there is, right now—DHS has set up a good framework for critical infrastructure protection, and they have a framework for cyber throughout that.

They work and they actually partner with DOD and the intel community in those regards, and I think they would draw on that. I don't know that anybody has come down clearly and said the different roles—I don't think they are at that point where they could define specifically the roles.

I will pass it over to Bob.

Mr. LENTZ. Well, I think that is exactly the answer. I think where DHS has set the framework up under their National Infrastructure Protection Plan, and they are working and we are supporting, as an example with the financial sector, we work through Treasury and we compare technologies and techniques and procedures that we are using, and trying to raise that bar.

And then as you work some of these other sectors, the interesting challenge is going to be, like you addressed, is going to be at some point they may say, "That is enough. I can't subsidize this level of protection any longer, especially against a nation state."

And therefore, we have to have a mutual dialogue at the highest levels of the government with industry to determine, how are we going to get that bar to a level we are all comfortable with? And that is going to be the interesting discussion in the future.

Mr. MARSHALL. Thank you, Mr. Chairman.

Mr. SMITH. Thank you.

Just one final question. Mr. Thornberry had mentioned the attacks on Estonia and Georgia, which really sort of got everyone's attention about what can go beyond, you know, some of the more basic stuff that we face. And obviously, you know, our main concern right now is data-mining—people accessing our network and pulling out information out of it as opposed to affirmatively attacking the network.

But in looking at what happened in those two countries, how vulnerable are our DOD networks to similar attacks? How confident are you that we have the, you know, system set up to withstand that type of an attack?

General ALEXANDER. I think a distributed denial-of-service attack from botnets, like you saw in Estonia, if large enough, would really hamper any network today, including the defense——

And the issue is, how do we grow a defense in depth to ensure that we don't have that? So that is where our allies and partnerships with our allies is going to become crucial.

If you try to defend it at your gateway, you surely will lose on that. And so you are going to have to have a defense in depth for that type of attack specifically.

Mr. SMITH. Forgive me. Walk me through a defense in depth, what that means exactly, in terms of what you try to do to prepare.

General ALEXANDER. So you would have—if you just look globally at the global network, instead of trying to stop all the stuff here, you might want to shut them down at the point of origin or somewhere in between, and that means that your offense and your defense are going to have to be partnered together to do that.

Mr. SMITH. Okay.

General ALEXANDER. I think that is the only way you are ever going to—I think we are going to be forced into operating like that in the future, and the consequences of that jump—the intellectual jump—is developing the tactics and techniques and procedures that I briefly discussed earlier.

Mr. SMITH. Gentlemen, anybody else want to comment on that, in terms of the security of your systems?

General.

General SHELTON. Yes, sir. Just one comment. What we are trying to do is implement some tight security on our networks, so when somebody comes onto the network we make them put a card in, we make them enter a code, and in the future probably have some sort of biometric so we know exactly who that is and we know exactly what permissions they have got, what data they have got access to, and somebody outside that realm can't have that access.

Mr. SMITH. Right.

General SHELTON. So you are defending inside as opposed to defending at the wall. That is the architecture——

Mr. SMITH. Right. And how, I mean—that is really hard with all the different people on the network. There are so many different access points to the network. But I guess that is more of a statement than a question, but you are working on it.

Anybody else?

Well, thank you very much. That was very, very informative. Look forward to working with you on this issue going forward.

Thank you all for your testimony and for answering our questions. Thanks.

We are adjourned.

[Whereupon, at 5:12 p.m., the subcommittee was adjourned.]

A P P E N D I X

May 5, 2009

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MAY 5, 2009

Statement of Terrorism, Unconventional Threats and Capabilities Subcommittee Chairman Adam Smith

Hearing on Cyberspace as a Warfighting Domain

May 5, 2009

"Today, the Terrorism, Unconventional Threats and Capabilities Subcommittee will meet to discuss how the Department of Defense operates in the cyberspace arena to support its mission and the policy, management and organizational challenges that hinder our actions. I want to thank our witnesses for attending and lending their expertise to this important discussion. We welcome you and your thoughts.

"While technological innovations have improved our ability to secure our borders, they have also exposed some security concerns to our information technology systems and the networks that support them. These concerns can be seen in the attacks in Estonia and Georgia and recent reports of a breach into contractor networks storing information on the development of the F-35 Joint Strike Fighter.

"In order to prevent similar intrusions, or more importantly, intrusions of a larger scale, we must develop a holistic approach to how we deal with cyberspace. We need to abandon an outdated mentality that views cybersecurity as a separate, discrete function that can be considered outside of or apart from operations. That means we must undertake a thorough review of our information policies and address the management and organizational flaws we uncover.

"Unfortunately, threats to our national security in the arena of cyberspace are not solely limited to government and we must also take steps to protect the private sector.

"This subcommittee has continued to stay engaged on this issue and we will continue to work with the DoD to address security concerns within the private sector, especially defense contractors.

"Our goal should not be to take control of private sector networks, but rather to look at how to bring the critical infrastructure sector within the same protected system as the rest of the federal government and continue to review and improve that system.

"Again, I thank the witnesses for being with us today and look forward to discussing this important issue."

Miller Opening Statement for Hearing on Cyberspace as a Warfighting Domain: Policy, Management and Technical Challenges to Mission Assurance

May 5, 2009

Washington, D.C. – U.S. Rep. Jeff Miller (R-FL), Ranking Member of the House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, today released the following prepared remarks for the subcommittee's hearing on the policy, management and technical challenges associated with cyberspace as a warfighting domain:

"I would like to reiterate a point I made several weeks ago during a keynote speech to a consortium of cybersecurity experts. Cyber warfare is happening now. Almost daily we see reports in the press that demonstrate the prevalence of malicious cyber activity and the growing threat it poses not just to our government, but to the private citizen as well. In the past two years, Estonia and Georgia faced cyber attacks on their national systems.

"At various times, the Department of Defense has had to shut down networks because of intrusions and, last November, had to ban the use of removable, flash-type drives because of the threat of malware transmission. Congress itself has been the target of malicious cyber activity with several committees and member offices affected. On a personal level, we are constantly bombarded by email spam and warnings of false websites and phishing scams seeking to compromise our personal information.

"The cyber threat has many faces, from the nation state using cyber space as a new intelligence front to criminal organizations seeking to steal our money and identities to the computer hobbyist who hacks for no other reason than the challenge of it; and the threat has many tools—from botnets and counterfeit chips to insider activity—to compromise our systems. In response, we need to be vigilant and persistent in our efforts to protect the information and communication on our systems.

"Assuring our systems are protected is no small challenge. Just last month, reports about the cyber breach of the F-35 program highlighted the vulnerabilities of our systems. The large amounts of data being exfiltrated, even on the unclassified level, could pose a significant security breach when viewed in the aggregate. Additionally, the same reliance on technology that gives our military forces such an overwhelming advantage on the battlefield can represent our greatest weakness if those technologies' hardware and software can be compromised.

"The Department has taken several significant steps to secure its networks and protect critical systems, but difficult decisions need to be made about what should be considered critical, and how those systems and components should best be defended. Risk management and analysis play key roles in targeting investment and efforts in information assurance, and building forensic capacity is important to help with damage assessments subsequent to intrusions. Policy, both at

the Department level and at the national and international levels, needs to be re-examined to account for the realities of the cyber dimension.

"So, we have before us today, several key players from the Department who can help explain better where the Department finds presently itself in assuring system security, what needs to be done to improve our capabilities, and how cyberspace, as a warfighter domain, needs to be incorporated into our national security strategies and policies. Of particular interest to me and this subcommittee is the continued implementation of the Comprehensive National Cybersecurity Initiative and the Department's consideration of a Cyber Command. We look forward to your testimony and to assisting the Department in this vital area."

RECORD VERSION

STATEMENT BY

MICHAEL E. KRIEGER, SES

DEPUTY CHIEF INFORMATION OFFICER/G-6

UNITED STATES ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS, AND CAPABILITIES

UNITED STATES HOUSE OF REPRESENTATIVES

SECOND SESSION, 111TH CONGRESS

INFORMATION TECHNOLOGY

MAY 5, 2009

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

STATEMENT BY
MICHAEL E. KRIEGER, SES
UNITED STATES ARMY
DEPUTY CHIEF INFORMATION OFFICER

Good afternoon, Chairman Smith and distinguished members of the subcommittee. As the Deputy Chief Information Officer and Deputy G-6 for the U.S. Army, I am pleased to appear before the subcommittee today to discuss the Army's activities to enable operations in cyberspace, and to address the policy, management, and technical challenges to enhance mission assurance in Cyberspace as a Warfighting Domain.

Securing cyberspace is a major issue for the United States as articulated in the December 2008 Center for Strategic and International Studies report. This report confirmed what the U.S. Army has already assessed – every day there are new threats and attacks against our network. I want to assure the members of this subcommittee that the U.S. Army has and continues to take action to mitigate these threats and improve our mission assurance in cyberspace.

There are many policy, management, and technical challenges to improving the U.S. Army's cybersecurity. We echo General Chilton's statement when he testified to this Subcommittee on March 17th this year, that the biggest challenge lies in changing the culture – the need to think about cyberspace, not so much as a convenience, but as a military necessity.

The U.S. Army believes that cyberspace – the enterprise network – needs to be viewed as a critical enabler for the Warfighter. In this era of Persistent Conflict, the U.S. Army is in the process of transitioning to a

Continental U.S.- based Expeditionary Force. Our ability to support a Joint Force Commander is highly dependent on having a secure global network continuously available to the Warfighter.

To change the culture, the U.S. Army is revising policies, reviewing the management of our people, and transforming how we operate the U.S. Army's portion of the DoD Global Information Grid (GIG) known as LandWarNet. The U.S. Army is also enhancing our technical capabilities to better detect, assess and respond to cyberspace attacks. We are instilling the importance of cybersecurity at all levels of command, and are making great strides to operate, maintain, and defend our network as one enterprise from the core-to-the-edge.

POLICY

To support an Expeditionary Force, the U.S. Army is fundamentally changing and adapting our institutions, including LandWarNet. On March 2, 2009, General Casey, the Chief of Staff of the U.S. Army, signed a memorandum to transform LandWarNet to deliver a global, standardized, protected, and economical network enterprise.

The U.S. Army is transforming LandWarNet to a new Global Network Enterprise Construct (GNEC). GNEC focuses on four principle objectives: (1) Operationalize LandWarNet, (2) Improve the LandWarNet defense posture, (3) Realize economies and efficiencies, and (4) Ensure Joint interoperability. These objectives will be accomplished through standardizing network operations (NetOps) processes and tools.

The U.S. Army has taken the lead on implementing many new policies to improve our cybersecurity. These policies concentrate on

protecting information, defending systems and networks, providing IA situational awareness, fostering innovation, and creating an empowered workforce. In Fiscal Year 2008 the U.S. Army led DoD on several strategic fronts to include:

- Developed and implemented an aggressive policy for encryption of Data at Rest (DAR) and Data in Motion, and currently leads DoD in the OMB mandated implementation of a DAR solution to protect sensitive information and mobile devices.
- Delivered the U.S. Army LandWarNet Information Assurance Architecture (LIAA). LIAA ensures a comprehensive LandWarNet IA Architecture that supports the DoD GIG IA Vision.
- Developed and implemented a four-phase IA compliance model and IA self-assessment checklist. This effort increases awareness, standardizes and validates IA compliance activities, and measures leader success in executing the command IA program.
- Influenced the tools selection and acquisition for DoD enterprise-wide network security solutions via our IA Approved Products List policy.
- Improved our Certification and Accreditation posture by mandating all systems be registered in the U.S. Army Portfolio Management System. As a result, the U.S. Army exceeded the Federal Information Security Management Act goal for Authorities to Operate.
- Led the execution and phased implementation of Homeland Security Presidential Directive-12 requirements for the implementation of Cryptographic Common Access Card logon.

- Partnered with OSD in support of the Comprehensive National Cybersecurity Initiative (CNCI) to draft policy to integrate Supply Chain Risk Management (SCRM) both into the procurement of Commercial Off-the-Shelf Software for the LandWarNet (and the GIG) as well as into program protection plans for major weapons systems. The intent is to improve the integrity of components used in DoD Systems, to establish a process to assess vulnerabilities, and gauge future resource requirements to mitigate the impact of supply chain risk.
- Developed a pilot process for SCRM with OSD, the other military components, and the Defense Intelligence Agency to: (1) develop a SCRM process which is scalable and relevant to meet the needs of DoD; (2) provide an initial assessment of the risk to DoD; and (3) gauge the resource and legal changes needed for a full-fledged SCRM process. The ultimate objective is to incorporate SCRM into the U.S. Army GNEC.
- Worked with the industrial base to protect the technologies used to build our future networks and other major weapons systems. In January 2008 we established the U.S. Army Defense Industrial Base Cyber Security Office (DIBCSO). DIBSCO's objective is to protect the technological superiority of U.S. Army weapons programs by managing the risks associated with the digitalization of information and the globalization of critical manufacturing capabilities. In its day-to-day mission, the DIBSCO drafts and revises U.S. Army policy and acquisition/contract procedures. These efforts maximize the protection of U.S. Army technologies within the contractor base, and are critical to current and future Warfighters.

MANAGEMENT

The U.S. Army is changing its culture by relooking how we manage our people and the network. We are updating our training curriculum to support the new cyber-skills needed to operate, maintain, and defend our network. We have realigned organizations to streamline the command and control over the network.

Recent network events have highlighted the need for a well-trained workforce capable of operating, maintaining, and defending the network. As a result the U.S. Army is reviewing the development and tracking of its highly skilled workforce, and looking to update the Officer, Warrant Officer, and Enlisted Career Management Fields for conducting cyberspace operations.

The U.S. Army has a robust training program for our individual IA professionals and Cyber-Warriors. One initiative is our Mobile Training Teams that travel to sites around the Army to execute mandatory training, and validate the knowledge and skills of the U.S. Army's IA and Cyber-workforce.

Unit training for cyberspace operations is in its formative stages. To help mature unit training, the U.S. Army conducts cyber-specific exercises such as Bulwark Defender, Unified Quest, Talisman Saber, Austere Challenge, and Global Lightning. These exercises train units to operate, maintain, and defend the network from directed professional attacks, and results in improved procedures for communicating with other Services, agencies, and Combatant Commands (COCOM). These training

exercises also provide a forum to study future joint, interagency, intergovernmental, and multinational operations.

The U.S. Army continues to change how it manages its network. Network Enterprise Technology Command (NETCOM) is now designated as the single authority to operate, maintain, and defend the U.S. Army's generating force network. The U.S. Army has reorganized its forces to support the U.S. Strategic Command (USSTRATCOM), the COCOM for cyberspace operations. In addition, we are achieving unity of effort within the U.S. Army Staff by creating an Army Cyberspace Task Force.

The U.S. Army is currently the only Component in DoD that has its NetOps command, NETCOM, reporting to the Chief Information Officer. NETCOM operates a 24x7 Global Network Operations and Security Center (NOSC) that provides the technical control to each of the Army's Theater NOSCs who support the geographic COCOMs.

When we talk about operating, maintaining, and defending the network, we are really describing Computer Network Operations (CNO). There are three disciplines within CNO: Computer Network Defense (CND), Computer Network Attack (CNA), and Computer Network Exploitation (CNE).

To improve the command and control for CND, the U.S. Army recently realigned the local network providers, known as Directors of Information Management, to NETCOM. NETCOM is also designated the CND Service Provider for the U.S. Army. Significant NETCOM functions and responsibilities include:

- Operate, maintain, and defend LandWarNet and U.S. Army global enterprise services.
- Direct, monitor, and support enterprise management across the LandWarNet.
- Execute technical control and enforce compliance across the LandWarNet.

TECHNICAL

The U.S. Army is addressing the many technical challenges we face through a number of initiatives to include:

- Selecting and deploying a DAR encryption solution for protecting sensitive data on mobile computing devices and removable media. The U.S. Army was instrumental in developing the technical requirements for the selection and subsequent award of the DOD DAR solution.
- Preventing pilfering of private or sensitive data by combing the Web for "at-risk" data through U.S. Army Web Risk Assessment Cells.
- Implementing the Information Assurance Vulnerability Management process to find, fix, report, and verify compliance with DOD mandates. The U.S. Army is using DOD automated scanning and remediation tools, innovative reporting capabilities, and increased compliance verification inspections.
- Securing two-way wireless devices and extending physical security measures to the DOD Smart Card technology. The U.S. Army has partnered with the National Security Agency (NSA) in developing the GIG IA Architecture.

- Deploying mobile wireless solutions which leverage NSA encryption devices such as SecNet 11 and SecNet 54. These devices reach back to the Warfighter Information Network-Tactical (WIN-T) in order connect back to the GIG. The U.S. Army is also deploying a Joint Tactical Radio System (JTRS) to provide secure voice and data capability at the Secret level to the Warfighter. For the future, the U.S. Army is evaluating the Secure Mobile Environment Portable Electronic Device (SME-PED) under contract with NSA. This device will deliver to the Warfighter secure voice communications at the Top Secret level and classified e-mail at the Secret level.

The U.S. Army expects that the Administration's budget request for Fiscal Year 2010 will fully support our cyberspace activities and include the resources necessary to effectively address our policy, management, and technical challenges. We are also confident that with your support, our GNEC strategy and initiatives will enhance mission assurance in Cyberspace as a Warfighting Domain.

In conclusion, the U.S. Army is taking and has taken action to mitigate the never ending cyberspace threats, and continue to improve our mission assurance in cyberspace. Using GNEC, the U.S. Army is addressing the challenge of changing the culture to view the network as a critical enabler for the Warfighter. The U.S. Army's commitment to transforming LandWarNet to an Army Enterprise will improve our network security posture as we aggressively work towards ensuring commanders have the ability to see, control, defend, and fight the network as one enterprise from the core-to-the-edge. By establishing a single focal point

for all cyberspace operations issues under the Army Cyberspace Task Force, we will provide the unity of command and effort needed to meet many of the cybersecurity issues the U.S. Army is facing today and will face in the future.

I would like to thank the subcommittee for affording me the opportunity to share the U.S. Army's activities to operate and enhance mission assurance in Cyberspace as a Warfighting Domain. Thank you.

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED
SERVICES COMMITTEE

STATEMENT OF

ROBERT J. CAREY

DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

SUBCOMMITTEE

HEARING ON

CYBERSPACE AS A WARFIGHTING DOMAIN:

POLICY, MANAGEMENT AND TECHNICAL

5 MAY 2009

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED
SERVICES COMMITTEE

Chairman Smith and members of the Committee, I am pleased to appear before you today to provide you with an overview of the Navy and Marine Corps team's views on Cyberspace as a Warfighting Capability, especially those affecting Navy and Marine Corps missions at home and abroad. In a 12 May 2008 policy memorandum, the Deputy Secretary of Defense directed the Department of Defense to use a definition of cyberspace consistent with that provided in National Security Presidential Directive 54 / Homeland Security Presidential Directive 23, which defines cyberspace as a global domain within the information environment consisting of the interdependent network of Information Technology (IT) infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. This emerging battlefield space presents new challenges to our Information Management (IM) and Information Technology (IT) systems, practices and management.

Information management and information technology have become the crucial elements supporting our warfighters. The Navy and Marine Corps rely upon our networks to deliver combat power, provide intelligence and support business operations. Internet protocol based communications permeate the battlefield. Cyberspace has become inextricably linked to the success of kinetic forces and our ability to accomplish the broad mission set of the Navy and Marine Corps. The Department of the Navy's (DON) reliance on cyberspace to conduct its missions and warfighting functions will continue to increase for the foreseeable future. A challenge we face in this domain is that information technology changes rapidly due to market forces and Naval systems change at a vastly slower pace. The need to remain current with technology and the ability to provide information to the warfighter is inconsistent with the

system development cycle times. Our effort must be directed at modernizing our approach to development in order to meet these needs.

Policy Challenges

Some challenges the Department of the Navy is focusing on are governance, policy, acquisition, role clarification and our relations with the Defense Industrial Base.

To ensure success in cyberspace, effective governance is critical. Current authorities and processes for making decisions affecting security, the design of our systems, and our portfolio of investments require adjustment to fully support cyberspace as a warfighting domain. These adjustments will improve our DON Enterprise Architecture standards and processes to better enable the exchange of information, the integration of systems and the operational management of technology resources. We also recognize the need to refine our IT asset management approach and policy to better ensure our security posture.

As the Defense Science Board (DSB) stated in their recent report on Acquisition of Information Technologies, "a new acquisition approach is needed that is consistent with rapid IT development cycles and software-dominated acquisitions." Specifically, the DSB stated the DoD needs to "develop new acquisition and requirements (capabilities) development processes for information technology systems." These must include a holistic view of our "business systems, information infrastructure, command and control, ISR (intelligence, surveillance, and reconnaissance) systems, embedded IT in weapons systems, and IT upgrades to fielded systems."

To address a portion of this new acquisition approach, the Department of the Navy is currently in the process of implementing a more proactive approach to Clinger-Cohen Act Certification. This approach will be closely aligned with our formal requirements and acquisition review and approval processes. It will ensure that Department of the Navy cyberspace investments and capabilities comply with the overarching tenets of the Clinger-Cohen Act, to:

a. implement effective information systems;
b. identify and track improvements to mission performance;
c. deploy business process improvements before investing in information technology and national security systems; and
d. accommodate the fast-paced nature of the IT industry in order to avoid outdated procurement approaches that do not take advantage of competition.

Cyberspace operations present unique and uncertain operational environments. Clearly defining the rules of engagement for cyberspace within both the uniformed and civilian domains will require careful deliberation. Law enforcement and criminal investigations, operations and related efforts, and military and intelligence functions must be well synchronized to ensure unity of effort.

Further, the implementations of the statutorily defined roles within the military departments are challenged in adequately addressing the growing cyber threat. Traditional command and control, management and acquisition all must become seamless within the IT space. Policies that control fighting, defending, information assurance and operations in cyberspace must be synchronized and consistent since all these functions occur in the same domain. Our policies need to be

synchronized to de-conflict fighting and defending operations in cyberspace. At present, the Department of the Navy faces challenges meeting the various statutory obligations while maintaining an agile posture to respond to emerging threats. In addition, the implementation of any statutory construct must be informed by a new understanding that our network environment, up to our desktops and personal electronic devices, is the new battlefield.

A final topic to address in this area is security threats to the Defense Industrial Base (DIB) who manufacture our weapons and information systems. Our networks have been under attack for more than a decade, and we must acknowledge that cyberspace is a contested domain. While we employ resources to offer a comprehensive multi-disciplinary approach to protecting our networks, we need to do more. The threat to our infrastructure and information is advanced, persistent, sophisticated, always changing, and well resourced. The challenge to the DIB is to be as vigilant and secure as the DoD and be able to maintain a security posture that enables seamless information sharing. Sustainment of this goal is impacted by the extent to which policy enables organizations to engage in an active defense of the DIB.

Management Challenges

Some challenges the Department of the Navy is focusing on are total workforce training and education, improving acquisition agility, critical infrastructure protection, and budget agility.

The Department of Defense is undergoing a significant transformation in culture, organization, structure and alignment to enable the full range of operations in cyberspace that will have broad

implications for the DON. Cyberspace management must be consistent and seamlessly linked with joint and national efforts. The DON is engaged in an intensive and comprehensive effort to improve its cyberspace governance, workforce capabilities and management approach in response.

Historically, we are oriented to acknowledge the contribution of weapons platform investments such as planes and ships to our security. Cyberspace resources must be controlled independently of the platforms they reside upon to ensure compatibility and common architectures to reduce security vulnerabilities and training cost. However, the principal management challenge arising from the emergence of cyberspace are policies governing the planning, programming and execution of our resources. Consequently, we are challenged to balance competing demands for limited resources between cyber-oriented and more traditional weapons platform investments. The cycle time associated with IM/IT moves far faster than our ability to plan, budget, and acquire, forcing potentially poor investment decisions. Further, a tighter integration of enterprise architecture, cyberspace warfighting requirements and our investment decision making process characterize the focus of our efforts.

A highly skilled workforce, trained to common DON, DoD and Federal standards is essential to meeting cyberspace requirements. The effective operation and governance of our IT will be grounded in the abilities of our workforce. Cyberspace spans multiple occupational fields, and the workforce communities must be highly synchronized to be effective. Identifying, attracting and retaining a highly qualified total workforce is an ongoing challenge which the DON is aggressively attacking through multiple strategies. The DON must also address the ability of our

current education and training development model to integrate lessons learned and the requirements of a rapidly changing IT domain. We must create a more responsive process of training development. We are investigating and leveraging all available education and training sources and processes to streamline, improve and align our training development and delivery.

Further, we must establish a culture within the Department wherein our members' understanding of their responsibilities for network security is ingrained in every single member. They must understand the ramifications of their actions on the information environment. Every action affects the security and operation of our networks which in turn affects every aspect of our warfighting environment as evidenced by our recent thumb drive issue which would have been reduced through proper adherence to network security policies. This cannot be stressed enough; the manner in which we engage every day on the network must be secure and conscientious.

Achieving and sustaining the goal of information superiority requires that we establish, maintain, and defend a secure and interoperable infrastructure. The Navy and Marine Corps rely upon the nation's infrastructure to perform their mission. Strikes against critical infrastructure can damage the economy, terrorize the population, and degrade or neutralize our Naval capability.

Technical Challenges

Some challenges the Department of the Navy is focusing on are ensuring secure access to information across the Global Information Grid, integrating Open Architected solutions, and protecting our critical infrastructure.

The DON is leveraging many technologies to improve security and lower cost. However, technical solutions delivered by industry to meet general market needs are often inadequate to meet military use in high threat environments wherein adversarial attack is presumed. Further, industry produces software products at rates sufficient to meet the needs of most users but, some software producers cannot react rapidly enough to security vulnerabilities to ensure security of our information. Investments in technology must be made to ensure we maintain the capabilities to be proactive vice reactive to security concerns. Open architecture technologies must be integrated, but security of our networks must remain the deciding factor when integrating these technologies. The Department must cooperate with industry to improve our life cycle management of our hardware and software.

In addition, there has been much discussion of using industry software to solve military problems. However, when these applications are put into military use, they have, among other issues, exploitable vulnerabilities. The DON must team with industry to ensure these applications are secure. Through activities such as vulnerability assessments and experimenting with designs, industry can engineer more secure systems that better withstand adversarial attempts to exploit them.

The size and scope of the Department presents technical challenges for networking our systems that few other organizations face. Nearly half of the Navy's ships are deployed at any given moment, making timely technology upgrades across the fleet difficult. Similarly, deployed Marine ground forces cannot be upgraded until they return to CONUS bases with robust

communications infrastructures. Multiple Information Technology architectures impact our security posture, are expensive to maintain and require separate training tracks for our cyber workforce. Addressing challenges such as security and cost containment, the Department is evolving its networking environment into a consistent, integrated naval networking environment allowing Sailors and Marines highly secure and reliable access to necessary information and services.

The DON must significantly reduce the number of points of presence (places the DON GIG connects to the DoD GIG or the Internet) and increase network security and defense resources. Additionally, asset management is essential to obtain the situational awareness necessary for network command and control and security compliance, in conjunction with consistent network architectures to facilitate cyber defense and warfighter success.

A critical emerging technical challenge is to exchange information securely with federal, state, and local departments and agencies, as well as our allies and partners. To enable information sharing across the enterprise and achieve the vision of network centric operations, data must be visible, accessible, and trusted. At present, information is locally owned and managed, which is not conducive to mission success. Additionally, providing the bandwidth necessary to facilitate sharing must be considered at the initial planning stages of any program or system.

Thank you for the opportunity to report to you the DON's views and positions on this vital issue. The Department will continue to exploit the power of information in order to transform the way

the Navy and Marine Corps fight. The assured use and protection of cyberspace is essential to our ability to deliver the Naval component of National Security.

NOT FOR PUBLICATION UNTIL RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRIORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
U.S. HOUSE OF REPRESENTATIVES

DEPARTMENT OF THE AIR FORCE

BEFORE THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
UNITED STATES HOUSE OF REPRESENTATIVES

SUBJECT: CYBERSPACE AS A WARFIGHTING DOMAIN: POLICY, MANAGEMENT AND TECHNICAL CHALLENGES TO MISSION ASSURANCE

STATEMENT OF: LIEUTENANT GENERAL WILLIAM L. SHELTON, USAF
Chief, Warfighting Integration and Chief Information Officer

5 MAY, 2009

NOT FOR PUBLICATION UNTIL RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRIORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
U.S. HOUSE OF REPRESENTATIVES

LIEUTENANT GENERAL WILLIAM L. SHELTON, USAF

Chief of Warfighting Integration and Chief Information Officer

United States Air Force

Good afternoon, Chairman Smith, Congressman Miller and distinguished members of the subcommittee. I am the Chief of Warfighting Integration and Chief Information Officer (CIO) for the U.S. Air Force and I am pleased to appear before the subcommittee today to discuss our efforts to address the challenges in the cyberspace domain.

Organizing the Force

Several years ago, the U.S. Air Force recognized the growing importance of cyberspace. On December 7th, 2005, we took the unprecedented step of adding cyberspace to our mission statement, and placed that domain on an equal footing with our more traditional operating environments of air and space. Since that time, we have been moving forward to organize, train and equip our Air Force to operate in cyberspace for joint operations.

As we moved into this new domain, we realized we would need to establish a new organization focused on developing expertise and optimizing capabilities in this arena. The Air Force decided to leverage and integrate Air Force Space Command's existing organizational responsibilities and present forces to United States Strategic Command via a new Numbered Air Force.

On February 20th of this year, the Secretary of the Air Force (SECAF) approved the activation of Twenty-fourth Air Force (24th AF), organized under Air Force Space Command (AFSPC) and a component under United States Strategic Command (USSTRATCOM), to serve as the focal point for Air Force cyber operations. Once activated, 24th AF will support USSTRATCOM and other combatant commanders to operate in, through and from cyberspace, integrated across all operating domains. The 24th AF will bring together existing Air Force cyber operational capabilities under one commander, allowing the Air

Force to better support the larger effort of USSTRATCOM's Joint Functional Component Commander for Network Warfare. Additionally, the 24th AF Commander will command and control Air Force Network Operations (AFNetOps), providing a centralized command structure for operations and defense of Air Force networks and protection of Air Force information residing on the network across the Air Force portion of the Defense Department's Global Information Grid (GIG).

The 24th AF will be comprised of three subordinate Wings: the 688th Information Operations Wing at Lackland AFB TX, dedicated to counter-information and information operations; the 689th Combat Communications Wing at Tinker AFB OK, responsible for extending and sustaining the Air Force portion of the GIG into the theater of operations in support of geographic combatant commanders; and the 67th Network Warfare Wing at Lackland AFB TX, responsible for conducting network operations in cyberspace as directed by the Commander, USSTRATCOM.

The Air Force is still in the site selection process for 24th Air Force headquarters. We are conducting an extensive review to ensure the site selected is the best possible location to ensure success of the 24th AF. Once a final location is determined, the Air Force is poised to activate 24th AF as soon as practical.

AFSPC will be the Air Force's lead Major Command to organize, train and equip our Air Force cyberspace forces. As part of this effort, significant resources and responsibilities are being administratively transitioned to AFSPC including the Air Force Information Operations Center, the Air Force Communications Agency (which has been re-designated as the Air Force Network Integration Center), the Air Force Frequency Management Agency and the 38th Engineering Installations Group. AFSPC will also assume functional responsibility for technology insertion efforts, project management, engineering and installations, communications maintenance, expeditionary communications and AFNetOps. As the Chief of Warfighting Integration and the AF CIO, I will retain the responsibilities for Air Force communications and information policy, guidance and oversight.

The National Defense Authorization Act (NDAA) of 2009 mandated the Air Force establish a Chief Management Officer (CMO) with overall responsibility for transforming business and combat support operations in the Air Force. We have made solid progress defining the role of the CMO, and recognize the clear relationship between that office and the CIO. We are currently balancing the Information Technology (IT) responsibilities and accountabilities of the CMO with those of the CIO, as directed by the Clinger-Cohen Act.

Additionally, SECAF has delegated the Freedom of Information Act (FOIA) responsibilities to the CIO. With this delegation, we instituted new processes and deployed a new interface to the public -- eFOIA. This "electronic face-to-the-public" web-based system streamlines the request process and improves tracking and overall responsiveness. As a commitment to continuous improvement and responsiveness to requests for public release of information, we reduced FOIA backlog requests by 17% in FY08, and are working on additional improvements to continue backlog reduction in FY09.

Training the Force

As we organize ourselves to operate efficiently in the cyber domain, we are tackling the challenge of increasing the size and expertise of our workforce. Issues we face include recruiting, training, incentivizing and retaining the increasingly scarce technical talent in our Nation. Despite the economic downturn, the competition for these people remains fierce. We are working hard to recruit the cyberspace warriors of tomorrow and to retain the great people we have in these positions today.

The current Air Force communications and information community is made up of over 60,000 personnel with 31,000 active duty personnel, 18,000 civilians and just over 17,000 Guardsmen and Reservists. We train about 185 new active duty communications and information officers per year, and about 155 students from the Guard and Reserve, international allies and government civilians, for a total of approximately 340 students per year. We also assign officers with relevant pre-commissioning

educational and/or life experiences to appropriate positions to leverage those skills to support this emerging mission.

Recent force reductions, combined with enabling technological change, have driven us to retool our enlisted workforce. We are consolidating 15 enlisted specialties into 11 career fields. Technology has enabled us to consolidate similar competencies into single vocations and in turn establish several new vocations focused on security and personal services delivery.

To ensure our personnel are well-trained before assuming their initial positions, we have modernized our pipeline training courses. We are considering additional training they should receive and at what point during their career they should receive it. We expanded our distance learning capabilities, and broadened our academic education program. We are updating our Professional Military Education courses to include cyber security, adding a cyber security block at Air Force Basic Military Training, and continuing to develop an advanced degree program at the Air Force Institute of Technology (AFIT) at Wright Patterson Air Force Base, Ohio. We are also working with our joint counterparts to take full advantage of the excellent cyber training capabilities at Corry Station, Pensacola, Florida.

After investing this much training in our people, we must extend our best efforts to retain them. Selective re-enlistment bonuses, as well as military benefits, are helpful in this regard. Air Force benefits compete well with industry, so we are hopeful the mission, the Air Force culture and the incentives will help us retain the best and brightest America has to offer.

The Government Accountability Office reports that a significant percentage of civilian personnel are, or will be, retirement eligible in the next 10 years. We believe our civilian workforce, who serve alongside their uniformed colleagues, is crucial to our success in this domain. A strong civilian development framework will attract new personnel to public service to fill the vacancies from the retiring workforce. We are working to identify key leadership and developmental positions and will

codify policies to manage these positions to ensure we deliberately develop people throughout their careers.

Like many others, I am concerned about the decreasing number of engineering, science and mathematics graduates from our nation's colleges. To assure our success, the Air Force will continue to need officers and civilians with technical educational backgrounds. The waning interest in science, math and technology, coupled with the rising demand for private sector IT and engineering professionals, will challenge our ability to attract, recruit and retain technically qualified military and civilian personnel. We believe this is not just an educational issue or an issue of competitive advantage. Maintaining a robust foundation of educated and trained technical professionals is a National Security issue.

Equipping the Force

The Air Force investments in IT reflect the priorities and direction of both the joint community and our Service leadership. To meet the challenges of rapidly advancing technology, we are restructuring our processes to acquire information technology. Traditional structures designed to purchase major weapons systems, with long attendant development cycles, are ill-suited for the fast-paced IT world where technologies can often be rendered obsolete in a matter of mere months. We are streamlining our processes to shorten the requirements-to-capability-delivered timeline through the use of commercially available technologies, leveraging open source technologies and exploiting opportunities to rapidly field prototype efforts.

The National Defense Authorization Act for Fiscal Year 2005 (NDAA 05) stated that defense business system modernization investments greater than $1 million must be approved by the appropriate OSD Investment Review Board and Defense Business Systems Management Committee. This was an important Act for the Air Force. Using this direction, combined with increased senior leader emphasis, we are conducting reviews of our investments. Since NDAA 05 was enacted, we have successfully certified 62 business systems. As we matured the review process, we identified

opportunities to streamline other processes. During FY07, my team developed a framework to review all statutory requirements across IT systems providing the Air Force with a single-point review of all IT systems on an annual basis.

We established a process to execute similar reviews on non-business systems. This initiative provided a unique opportunity for the CIO and acquisition community to combine reviews and eliminate duplication. This consolidation ensures all critical IT investments are formally evaluated either at an acquisition milestone, or another annual review.

This realignment also yielded other successes in IT management. We updated our portfolio investment review process to coordinate decision-making with other business enterprise management components. The new process generates an IT investment strategy that is linked to the budget cycle, and aligned to Air Force strategic objectives. Last year, we published an Air Force Instruction that formally establishes the guidelines, policies and procedures for approving and managing Air Force IT.

Today we are managing our IT certification and accreditation process to ensure that appropriate security controls are in place prior to integrating an IT system on the Air Force network. Specifically, the Air Force established robust goals for FY09: first, compliance rates of 95% or higher for certification and accreditation; second, validation of current annual security reviews, security controls and contingency plan testing; third, completion of Information Assurance (IA) Awareness training; and finally, submission of a Plan of Action and Milestones to the CIO that formalizes these policies. Compliance metrics have been developed and are tracked weekly by the Air Force Senior Information Assurance Officer who reports directly to me.

Protection of our critical information is vital and we have instituted measures to ensure the security of personally identifiable information, to include all military, civilian and public affiliation data. Restricting the disclosure of personal information is a top priority, resulting in an initiative to reduce the use of Social Security numbers. Additionally, we annually review our IT investments and identify

systems that collect or generate personal information. We use this data to ensure we have appropriate safeguards that are documented, verified and approved by me. To date, we have completed 85% of this requirement and will continue to improve this rate throughout the year.

While we have achieved much, we are committed to constantly improving our governance process to support new and on-going acquisition efforts. Partnering with our DoD acquisition team, security is a critical enabler in the development of new systems. We will no longer "bolt-on" expensive security options onto our systems; rather, we will integrate services to achieve dramatic security improvements. The AF is dedicated to improving operational effectiveness and increasing efficiency through governance and leadership. We will do this through our enterprise architecture, deliberate processes and cultural change.

With our improved processes and governance measures in place, we are now focusing our investments in a few critical areas reflecting our priorities. To help reinvigorate the Air Force nuclear enterprise, we will continue to provide dependable and secure command, control, communications and information for our nuclear forces. We are modernizing our already reliable cryptographic program to ensure the continued security of vital nuclear assets.

By partnering with joint and coalition team members, we will build networks that guarantee the security of data in any environment, while ensuring the necessary data is shared appropriately across domains. Our long-term goals are centered around our support to the joint efforts to enhance the GIG. The Public Key Infrastructure (PKI) ensures front-line security for information systems and applications on the GIG and provides critical user protection across the Department of Defense, as well as our contractors' networks. Our continued priority is to modernize and develop the proper safeguards to secure our data in both a joint and coalition environment. As we continue to deploy with our service and coalition partners, it becomes increasingly important to ensure we can communicate effectively with the entire joint and combined team, while maintaining the security of our information.

The SECAF and the Chief of Staff of the Air Force (CSAF) recently directed the Air Force CIO to take a strong and centralized approach to network management. With guidance from the Air Force Senior Acquisition Executive, Air Force Space Command and the Senior Working Group, we are developing an end-to-end IT governance policy. This combined effort, will take control of the Air Force enterprise architecture. It will create a "build-to-design" network governance structure, based on an enforceable architecture that will ensure security and reliability, while reducing development costs. This policy will also enable the AF to align network operations command and control capabilities to the joint network command and control structure to ensure both security and performance of network components.

My organization has undertaken a significant design effort to align with DOD's Net-Centric Data Strategy. We call this effort the Singularly Managed Infrastructure with Enterprise Level Security or SMI-ELS for short. SMI-ELS addresses two critical mission needs. The first (SMI) is the sharing of information across Air Force, DOD, US Government and Coalition networks. The second (ELS) is the protection of Air Force information and the infrastructure that enables the sharing of that information. SMI-ELS will provide us access to mission critical information via a secure, robust infrastructure which will protect Air Force users, information, and technical resources from both internal and external threats. To drive the Air Force to higher degrees of information and knowledge-based operations, SMI-ELS will span enterprise-level business processes such as architecture and acquisition, technical solutions networks, web services, applications, data repositories, computing infrastructure, and force transformation.

Modernization and standardization of network equipment under the Combat Information Transport System (CITS) program provides our Airmen with the necessary tools to centrally operate, defend and manage the AF network. An example I would point to is the Expeditionary Combat Support System (ECSS) which allows the AF to modernize and consolidate, or turn off, expensive, legacy logistic

systems, generating significant future cost savings. ECSS also provides accurate, timely decision support across the supply chain.

Perhaps the most significant challenge we face is the constantly evolving nature of the threat in cyberspace. Threats in cyberspace move at the speed of light, and we are literally under attack every day as our networks are constantly probed, and our adversaries seek to exploit vulnerabilities in our network enterprise. To keep pace with the efforts of our adversaries, we need a robust research and development effort to keep us ahead of those who would seek to damage our information networks. I have two particular areas of concern regarding challenges in the defense of our networks; generally both R&D topics have received national level attention through the Comprehensive National Cybersecurity Initiative (CNCI) and are being reviewed as part of the Administrations 60-day Cybersecurity review. The Air Force will ensure its R&D is consistent with these broader USG efforts, while maintaining specific R&D capabilities to ensure mission essential functions. The first is our ability to command and control our network infrastructure and have full situational awareness of the activities taking place on that network. This is an area that will benefit from government-sponsored research and development. To date, our reliance on commercial efforts poses a challenge of scalability. The scope of effort required to defend the Air Force and DoD enterprise far exceeds that of the traditional commercial customer. We are continually faced with the challenge of adapting and employing tools that are not appropriately sized for our enterprise needs. This leaves us with an incomplete view of the activities on our networks and a limited ability to execute the real-time responses required to preemptively respond to the threat. R&D efforts need to focus on developing tools that allow our cyberforce to see, know and act in the same unified way as our military forces do in every other modern battlefield domain. The second area of concern is our ability to respond to specific malicious threats, such as viruses, a problem that is not well suited to traditional R&D. While DoD conducts some organic research in response to specific cyber threats, we rely heavily on the day-to-day efforts of industry. In

most cases, this approach does not keep pace with the cyber threat; instead, it is reactive in nature. The threats can bypass defenses with minor modifications—often the case with computer viruses.

As a final thought in this area of equipping the force, we are working to assure relevant, timely and secure information to the joint warfighter engaged in combat operations overseas. In support of an urgent request from US Central Command, we deployed a capability referred to as Battlefield Airborne Communication Node (BACN). This new capability enables data translation and forwarding that connects legacy data links to emerging capabilities. BACN also increases the range for voice communications beyond line of sight through the use of radio frequency translations and repeaters, achieving both voice and data link interoperability without modifying our current equipment or aircraft. This range extension capability ensures early radio contact so we can transmit targeting information to strike aircraft like the B-1, allowing a first-pass strike, and avoiding the previously required overflight of the target area that often alerted enemy forces. The high altitude at which we operate allows us to avoid enemy small arms fire and overcome line of sight "shadows" experienced by aircraft flying low in mountainous terrain.

Since, October 2008, BACN has supported close air support, convoy, time sensitive targeting and air drop missions with great success. Based on over 700 troops-in-contact situations, we have seen a 25% reduction in the time it takes for ground units to establish communications with close air support aircraft. This improved speed of establishing communications has also enabled a 45% increase in kinetic results—bombs on target in support of our ground forces. Our efforts were not just limited to combat operations. We also provided the World Food convoy commander with "comms-on-the-move." This capability allowed the convoys to stay in continuous contact with air support and ground command channels in the complex, mountainous terrain, mitigating exposure to attacks—they no longer needed to halt movement to establish communications.

The employment of BACN directly improves joint and combined force operations. It extends ground command and control tactical communications across the region to allow the coalition to task any available air asset to respond to a troops-in-contact situation. BACN also enables the coalition to extend and unify the air picture (to include air track, aircraft orbit and targeting information) for U.S. Air Force, Army, Navy, Marine Corps and British, French and Dutch forces.

Summary

In closing, I would like to thank the Committee for this opportunity to highlight the outstanding efforts of the dedicated men and women of the United States Air Force to secure our Nation in cyberspace. I trust I have illustrated that this new domain is both highly complex and extremely challenging, but it is one that the Air Force is fully embracing. Thank you again and I look forward to your questions.

RECORD VERSION

STATEMENT BY

MR. ROBERT F. LENTZ

DEPUTY ASSISTANT SECRETARY OF DEFENSE,

FOR CYBER, IDENTITY AND INFORMATION ASSURANCE

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

TERRORISM, UNCONVENTIONAL THREATS & CAPABILITIES

May 5, 2009

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

Good afternoon, Chairman Smith, Congressman Miller, and Members of the Terrorism, Unconventional Threat and Capabilities Subcommittee. I am Robert Lentz, the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance representing the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. I am also the Department's Senior Information Assurance Officer. I am pleased to appear before the Subcommittee to discuss initiatives to enhance the Department's and the nation's information assurance/ cybersecurity posture.

Information assurance/cybersecurity (IA/CS) is a critical priority for the Department of Defense (DoD). With information and information technology (IT) assets distributed over a vast and wide-ranging enterprise and with diverse domestic and international partners actively participating in DoD missions, we know that we cannot execute operations without the Global Information Grid (GIG) – our DoD network. The GIG is not just a collection of individual networks that happen to share the same Internet access points; the GIG is how we operate; the GIG is where business goods and services are coordinated; where medical information resides; where intelligence data is fused; where weapons platforms are designed, built and maintained; where commanders plan operations and command and control forces; and where training, readiness, and morale and welfare are sustained.

Therefore, the Department is focused on building and operating the GIG as a joint global enterprise that can be depended on wherever we operate in the world and under any circumstances to include cyber attack. This enterprise network approach, coupled with skilled users, defenders, and first-responders and in partnership with the intelligence community, will allow us to more readily identify and respond to cyber attack – and still accomplish the mission.

The DoD cyber, identity and information assurance (CIIA) program is thus aimed at ensuring the following vision:

- DoD missions and operations continue under any cyber situation or condition.
- The cyber components of DoD weapons systems and other defense platforms perform as expected.
- The Department has ready access to its information and command and control channels, and its adversaries do not.
- The Defense information environment securely and seamlessly extends to mission partners.

Strategic Goals

To realize this vision, the Department has established four strategic IA/CS goals:

Goal 1: Organize for unity of purpose and speed of action. This goal focuses on how IA/CS is considered as the Department plans for and evaluates use of cyber assets or the cyber domain in Defense missions, the development and sustainment of our IA/CS

workforce, and the expansion of IA/CS capabilities and capacity through partnerships, whether they be intra-government, with academia, with information technology (IT) industries, with defense industries, or with our international and military coalition partners.

Goal 2: Enable mission-driven access to information and services. This goal addresses how the Department securely delivers the power of information to its warfighting, intelligence, and business communities.

Goal 3: Anticipate and prevent successful attacks on data and networks. This goal addresses how the Department configures and instruments the GIG with tools and technologies to prevent intrusions, detect intrusion attempts, and reduce attack surfaces to deny adversaries any opportunity or advantage.

Goal 4: Prepare for and operate through cyber degradation or attack. This goal addresses how the Department creates trust and confidence in its weapons systems, data, and networks; strengthens its IA/CS readiness; operates in a degraded cyber environment; and restores cyber capabilities.

These goals provide the means to protect and defend the GIG today and to improve IA/CS capabilities over time. We are progressing toward an enterprise information environment that can dynamically and automatically configure itself to counter any threat and facilitate any mission.

The Department has made significant advances toward the vision. We have:

- Joined forces with other federal agencies in a comprehensive national cybersecurity[1] initiative to secure government networks, protect against constant intrusion attempts, and anticipate future threats.
- Developed a DoD Information Management/Information Technology (IM/IT) Strategic Plan to further transition to net-centric operations to achieve information advantage.
- Recognized cyberspace as a global domain within the information environment, developed a National Military Strategy for Cyberspace Operations (NMS-CO), embraced a Network Operations (NetOps) construct for operating and defending the GIG, and, under United States Strategic Command (USSTRATCOM), integrated NetOps with other cyber operations.
- Stood-up and connected key cyber centers such as the National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center (NTOC), and the Defense Cyber Crime Center (DC3) as well as certified all 25 network defense centers across DoD.
- Operationalized the Joint Task Force for Global Network Operations (JTF-GNO) under USSTRATCOM.
- With industry and academia, developed the IA Component of the GIG Integrated Architecture and plans and programs for delivering key identity and IA/CS capabilities as enterprise services.

[1] The U.S. Government currently defines *cybersecurity* as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation." (NSPD 54/HSPD 23).

- Partnered with the Director for National Intelligence (DNI) to establish the Unified Cross Domain Management Office (UCDMO) to synchronize and accelerate the availability of all levels of classified/sensitive information and to protect sensitive or controlled unclassified information to include sharing with our closest partners.
- Established a cybersecurity program in partnership with the Defense Industrial Base (DIB) to protect unclassified information relevant to Defense-related research, development and procurement.
- Established DoD policy addressing the relationship between cyber offensive and defensive actions called Computer Network Defense Response Action (CND RA).
- Worked with the National Counterintelligence Executive (NCIX) and Insider Threat Advisory Group to foster collaboration on the use of insider threat IA/CS tools.
- Created a DoD Venture Catalyst Initiative called DeVenCI to aid in the invention of cutting edge IA/CS solutions.
- Developed a comprehensive IA/CS policy framework that ranges from identity protection to wireless and satellite security to workforce training and education.
- Created the National Cyber Response Coordination Group in partnership with the Departments of Homeland Security and Justice.
- Launched a comprehensive cryptographic modernization initiative.
- Established a trusted foundry program and sought ways to improve microelectronics and software assurance.

The breadth and depth of all the programs and initiatives underway within the Department is too large to cover here. However, I would like to highlight a few current enterprise initiatives within the DoD CIIA program, organized by our strategic goals.

Goal 1

In support of Goal 1 (Organize for unity of purpose and speed of action), I will highlight our efforts to establish a DoD cyber workforce, partner with the DIB in a cybersecurity pilot, and build an international IA program.

Workforce

While our long-term aim is to achieve robust machine-to-machine network defense capabilities, people will always remain our frontline against cyber adversaries. From the everyday user to cyber defenders, the DoD workforce needs to be fully trained and qualified in key areas, and appropriately deployed to leverage and protect the Department's tremendous investment in information and communications. Achieving a technically adept cyber-capable workforce is job one! Competency in multiple IA/CS skills along with extraordinary cyber expertise or "black belts" in specialty areas, plus joint exercises to foster greater knowledge throughout the cybersecurity community has become a core priority of the Department.

To this end, the Department is continuing to expand the range and quality of IA/CS training available to its workforce. The technical schools of the military services have

expanded their IA/CS curricula to meet DoD common baseline training and certification requirements. For example, the Air Force's school at Maxwell, AL, and the Navy's program at Pensacola, FL, are offering tremendous new programs. The Defense Information Systems Agency (DISA) sponsored Carnegie Mellon Virtual Training Environment provides real-time, on-line interactive IA/CS technical training to both military and civilian workforce members wherever they are in the world. The Information Resource Management College (IRMC) at the National Defense University here in Washington, DC now offers an advanced IA/CS curriculum supporting baseline standards to both DoD and federal leaders in all Departments. The military service academies and post-graduate schools are also heightening focus on IA/CS. Recently, the Army, Navy, and Air Force academies competed in the ninth-annual cyber game for cyber warriors.

The Department has a rich suite of simulation and exercise tools analogous to flight simulators that create realistic and secure environments for training and practicing IA/CS skills. This approach provides opportunities to "see" and respond to threats in a controlled environment, and rapidly build skills and experience without disrupting operational networks.

The Department has also developed IA/CS awareness training to help users and leaders to better understand their roles in defending DoD networks. The 2009 DoD IA Awareness training product introduced a new more interactive approach to teaching end users about

their critical role in securing our networks. Our compliance reports show that 2.1 million personnel successfully completed this user awareness training program. Leadership development curricula in the military service and Joint Professional Education Programs have increased emphasis on IA/CS awareness to improve operational leaders' understanding and support for CIIA requirements. Operational leadership support is critical for effective execution of IA/CS activities at all levels.

The National Centers of Academic Excellence in IA Education (CAE) are producing graduates with the right skills to achieve a world class cyber workforce that includes both defensive and offensive capabilities. The CAE and CAE-Research (CAE–R) programs reduce the vulnerability of our nation's information infrastructure by promoting IA higher education and research and by producing a growing number of professionals with IA expertise in various disciplines. Currently, there are 94 CAEs across 38 states and the District of Columbia, including five military academic institutions: the Air Force Institute of Technology, the IRMC, the US Military Academy at West Point, the Naval Post-Graduate School, and the US Air Force Academy. For many students, especially graduate students, research is their "true educational experience." We must continue to expose these students to our hardest problems. The aim of the CAE-R program is to advance IA technology, policy, and operations that enable the nation to effectively prevent or respond to catastrophic cyber events. The CAE-R designations total 23 IA research centers across 17 states and the District of Columbia.

The CAEs provide DoD with many partnering opportunities. One example is the *Wounded Warrior Training Program* for America's wounded, disabled, and transitioning veterans. Mississippi State University's Forensics Training Center, in collaboration with Auburn and Tuskegee Universities in Alabama, is providing no-cost vocational training to veterans in a critical technical shortage area – digital forensics. In the fall of 2008, the Department helped bring this training program to the Walter Reed Army Medical Center in Silver Spring, MD. The intent is to offer the program for recovering military personnel at other major hospitals across the country this year and beyond.

Currently the Department is evaluating partnerships with University of California, Davis and University of North Carolina, Charlotte for *secure software development education,* including secure coding clinics for students. The intent is for students to receive an in-depth introduction to secure software techniques, have access to the tools and methods used to fix software vulnerabilities, and understand how to use them. The partnership, if undertaken, would be a key step in providing critical and leading edge software engineering skills to students who are potential DoD or federal employees.

Defense Industrial Base

In early 2008, the Department initiated a DIB Cyber Security and Information Assurance (CS/IA) pilot program to address cybersecurity risks to DIB unclassified networks that support DoD programs. The DIB CS/IA pilot has five major components: a binding bilateral DoD-DIB company framework agreement to facilitate CS/IA cooperation; threat

and vulnerability information sharing; DIB network incident reporting; damage assessments; and DoD acquisition and contracting changes, including proposed changes to Defense Federal Acquisition Regulation Supplement (DFARS). The DoD-DIB legal framework provides the mechanism to exchange relevant threat information in a timely manner, provides intelligence and digital forensic analysis on threats, and expands Government to Industry cooperation while ensuring that industry equities and privacy are protected.

Under this program, the Defense Cyber Crime Center (DC3) is the focal point for threat information sharing. DC3, in coordination with other cyber centers, analyzes and disseminates near real-time threat information. To further strengthen near real-time information sharing and collaboration between DoD and its DIB partners, DoD is developing a secure electronic data/voice communication network called DIBNet. The DC3 also performs digital forensic analysis on reported DIB intrusion sets. These processes are labor intensive and require resources and advanced skills.

The Damage Assessment Management Office in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics orchestrates our military service damage assessment cells and is helping to standardize methodologies. Through damage assessments, the Department will be able to better determine the extent of compromised DoD information, as well as assess the overall impact of the compromise on current and future weapons programs, scientific and research projects, and warfighting capabilities.

The DIB CS/IA pilot is informing proposed changes to the DFARS for enhanced IA/CS requirements in DoD contracts.

To continue improvements in DIB network security, the Department of Homeland Security, in collaboration with the Department of Defense, is evaluating the DIB model for sharing cybersecurity information with other Critical Infrastructure sectors.

International Program

The Department has a very robust program built on trusted bilateral, multilateral, and institutional relationships with national and military representatives around the world to enhance situational awareness and capabilities to counter common cyber threats, share tactics, techniques and procedures and synchronize IA/CS strategies and policies. Shared situational awareness helps stay ahead of the threat, protects U.S. secrets and sensitive information residing on foreign networks, and protects coalition and allied operations, especially with increased ops tempo for counterterrorism activity and for peacekeeping. Cyber attacks in Estonia and Georgia have accelerated international cooperation. A common objective is to promote adoption of international standards and norms in partnership with interagency processes. This includes developing common positions for international fora, influencing standards and technology, and discussing international norms of behavior in cyberspace.

We have a number of bilateral agreements with partner countries and are aggressively pursuing more. Current activities include the International Computer Network Defense

(CND) Coordination Working Group (ICCWG), the International Cyber Defense Workshop (next one is June 2009), international civil and military participation in Cyber Storm II, (a large-scale national cyber exercise part of Homeland Security's ongoing risk-based management effort to use exercises to enhance government and private sector response to a cyber incident, promote public awareness, and reduce cyber risk within all levels of government and the private sector), and the ongoing sharing of best practices, policies, and threat information. Challenges in this area include limited classified network connectivity, over-classification of information, and difficulties in applying "write for release" practices for cybersecurity information sharing.

Goal 2

Next I will highlight two initiatives under Goal 2 (Enable mission driven access to information and services). They are identity management and assured information sharing.

Identity Management

Our identity management (IdM) initiative provides the ability to identify people and devices on our networks and distinguish among friendly, neutral, and unfriendly entities. Our Identity management capabilities are based on use of public key infrastructure (PKI) technology. Our public key certificates and the Common Access Card (CAC) provide strong, highly trusted electronic identity credentials for our people and our non-person entities (e.g., network and computer devices, phones, radios, satellites, services,

applications, etc.). The Department's PKI and IdM efforts are base-lined on the Homeland Security Presidential Directive 12/Personal Identity Verification (HSPD-12/PIV) standard for the Federal Identity Credential. Nearly all of the Department's Active and Reserve military, civilian employees and contractors utilize CACs to facilitate network, web site, and facility access. Adherence to the HSPD-12/PIV identity credential standard makes it possible for federal partners to use their PIV cards to access DoD information repositories and web servers with enhanced user security.

The Department's use of hardware-based identity credentials for access to networks and information systems has shut down known attack vectors, demonstrably decreased attacks, and elevated the security posture to our networks by denying anonymity to attackers. The use of biometrics in conjunction with PKI credentials is yielding important improvements in protection against insider threats. Identity interoperability with industry and international groups will help with secure information sharing and force protection.

DoD is involved in two premier programs leveraging standardized identity credentialing. They are the Transglobal Secure Collaboration Program (TSCP) and the Federation for Identity and Cross-Credentialing Systems. The DoD and industry have partnered through the Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs) to verify the identity of personnel and accept each other's identity credentials. FiXs currently verifies and authenticates the identities of contractor personnel seeking to enter U.S. military installations or other government controlled areas.

The Transglobal Secure Collaboration Program (TSCP) is a government-industry partnership specifically focused on facilitating solutions to the most critical issues in Aerospace and Defense (A&D) today: A key enabler for the TSCP is a common identity approach that is highly aligned with the HSPD-12/PIV credentialing program. Their interoperable identity credentials mitigate the risks related to compliance, complexity, cost and IT that are inherent in large-scale, collaborative programs that span national jurisdictions. To do business in the world today, A&D companies must balance the need to protect intellectual property (IP) while demonstrating willingness and ability to meet contractual requirements from government customers for auditable, identity-based, secure flows of information. This duality requires that security be both within organizations and across extended supply chains and partners.

Assured Information Sharing

In addition to sharing information among trusted users across organizational boundaries, the Department is working hard to enable sharing across the entire spectrum of security domains while protecting networks and information. To that end, it partnered with the DNI and established the Unified Cross Domain Management Office (UCDMO) in 2006. The UCDMO is staffed with personnel from throughout the Department of Defense and the Intelligence Community (IC); it provides centralized coordination and oversight of all cross domain activities and ensures a common approach for the implementation of cross domain capabilities within the Department and the IC. Additionally, it is working to

ensure that secure, robust and flexible capabilities are available and extensible to share information among federal, state, local and tribal entities and with mission partners and private sector enclaves appropriately. The UCDMO roadmap is aligned to the information sharing strategic plans of the Department and the IC, and it is focused on delivering needed sharing capabilities, providing return on investment, managing security risk, and promoting awareness and collaboration among the users and developers.

Goal 3

From Goal 3 (Anticipate and prevent successful attacks on data and networks) I will highlight two initiatives; network de-militarized zones and host-based security. This goal is focused on hardening data and networks in order to anticipate and prevent successful attacks on them. The most capable and motivated of our adversaries will use any means available to achieve their goals, and our strategy must address that range of tactics. To that end, we invest in intelligence and perimeter-hardening to anticipate and prevent successful attacks, but we also design and configure systems to ensure that attackers are easy to find and/or contain should they pierce perimeter defenses.

De-militarized zones

Network de-militarized zones (DMZs), are to perimeter defense as a moat is to a castle. The DMZs obviate the need for most DoD assets to ever have to touch the Internet. Instead, those DoD applications, such as email, which must face the Internet are housed within a special containment zone. Within that zone inward-bound traffic can be

carefully scrutinized for viruses and other malware. The DMZ controls can also enforce white-listing, that is, only allowing traffic from trusted addresses to enter the enterprise, and perhaps most importantly, by acting as a proxy for all communication to the untrusted world, can deny adversaries reconnaissance knowledge of the structure of DoD networks. The Department has vastly reduced the number of its Internet access points, the first step in moving toward an enterprise-wide DMZ architecture, and is identifying outward-facing applications for placement in the zones.

While DMZs harden the network at entry points, host-based security provides a line of defense at each computer. Host-based security significantly reduces the risk of cyber attack at the individual computer by preventing malicious code and unauthorized applications from running. It also provides a consistent way to do configuration and management across all DoD networks.

Host-based security

Host-based security includes, but is not limited to host firewall, host intrusion detection, host intrusion prevention, system compliance profiling, rogue system detection, application blocking, and Information Condition (INFOCON) baselining. Under USSTRATCOM's direction, the Department is rapidly implementing host-based security across the enterprise. It is now deployed within approximately 40% of the host processing environment, and should be deployed to a majority of our systems by early 2010. Coupled with this, we are widely deploying the Federal Desktop Core

Configuration, a pivotal industry/government cooperative venture, beginning with ubiquitous Microsoft products, to make computers more stable and defensible. We are also widely deploying data-at-rest protection.

As is evident from these highlighted projects, safeguarding our networks against adversary attack today requires close partnership between information assurance experts and information technology (IT) providers. The DMZs are as much about network architecture as they are about specific tools for content filtering, and host-based security is a suite of software which is installed on commodity computing hardware; it is not a stand-alone IA device that plugs in to a computer or network. This convergence of IA/CS and IT poses challenges for governance and training, but it promises some new and much more efficient ways to secure our networks.

Our DoD research labs are particularly interested in new IT paradigms that change the game for defense, and I will close this section by discussing two of them, virtualization and cloud computing, which together and separately may revolutionize how we think about and secure our networks.

Virtualization

The DoD enclaves today look mostly like traditional local area networks; each user has a physical device on a desk linked back to one or more servers. Some user data lives on the desktop machine and some resides on servers, with the desktop patched periodically

to close security holes and implement new configuration guidance. With virtualization, the necessity for coupling together specific logical and physical assets goes away. For example, each user's environment (data and computing tools) can be stored and maintained as a digital file or image in a central control area. When a user needs their environment, it can be "incarnated" into any compatible physical platform. So tomorrow, instead of scanning physical components for current state and applying patches to bring the component into compliance, we may, instead, proactively repair and refresh the stored images and only incarnate the good ones. Doing this cleverly and often will make it harder for adversaries to sustain the footholds they gain through phishing attacks to persist in our networks.

Cloud computing

Cloud computing builds on these ideas to offer a virtual computing fabric with almost limitless and infinitely definable processing and storage capacity. In the future, many enterprises will choose not to invest in their own IT departments, but will pay as they go, relying on ability to access commercial computing services in the cloud. For many DoD applications, the commercial cloud will be too risky, but a private cloud could bring us many benefits. Besides the obvious economic benefits of scalable, on-demand computing, a private cloud also gives us the ideal platform with which to provide the virtual monitoring and provisioning described earlier. A cloud is also an ideal place from which to make capabilities available to the whole enterprise. While, in the DoD, we have encountered challenges moving towards a service-oriented architecture (SOA), in the

private sector, companies like Google and Salesforce are basing their business models on an insatiable public hunger for software and applications as a service. Emulating their delivery mechanisms within our own private cloud may be key to how we realize the true potential of net-centricity.

Goal 4

Finally, I will highlight three initiatives under Goal 4 (Preparing for and operating through cyber attack or degradation) which provides a foundation to leap beyond traditional IA/CS approaches. They are supply chain risk management, assurance in defense system acquisitions, and network resiliency.

Supply Chain Risk Management

While the global marketplace provides the Department increased opportunity for innovation in information and communication technologies (ICT), it also provides increased opportunity for malicious actors to manipulate ICT products and services to gain unauthorized access to otherwise closed-off technologies and services – what we call supply chain risk.

Threats to the ICT supply chain can affect both software and hardware products. Software design, development, testing, distribution, and maintenance frequently can be done less expensively offshore, but puts technology within easy reach of malicious actors. At the same time, the growing complexity of software and microelectronics

makes discovering vulnerabilities extremely difficult. Security of the ICT supply chain can also be compromised by untrustworthy or counterfeit ICT components. We are particularly concerned about the semiconductor industry which has increasingly moved toward offshore or foreign-owned semiconductor component production. This trend creates an increasing threat to the US as the potential for unauthorized design inclusions to appear on integrated circuits used in military applications increases.

As early as 2003, the Department promulgated a Defense Trusted Integrated Circuits Strategy. The Trusted Foundry Program, initiated in fiscal year 2004, leverages a contract with IBM to aggregate purchases of leading edge semiconductors with state-of-the-art features for use in defense applications. As part of the contract, IBM upgraded their facilities and implemented enhanced security procedures, creating the Department's first Accredited Trusted Integrated Circuits Supplier. In 2004, the Department tasked the NSA to stand up a new office to manage this contract and expand the ranks of suppliers capable of providing trusted integrated circuits. In response, NSA created the Trusted Access Program Office and implemented a trusted integrated circuits supplier accreditation program, now overseen by the Defense Microelectronics Agency.

The Trusted Foundry Program is funded at approximately $80M/year through equal investments from the Services and NSA as well as from direct program payments for chip processing and services. In 2008, the Trusted Foundry served over 80 program customers and processed 412 unique integrated circuits designs. The Trusted Supplier

Accreditation program continues to expand and there are now 21 Accredited Trusted Suppliers providing a full range of services enabling the department to draw on a fully accredited end-to-end trusted supply chain for integrated circuits.

Building on the Trusted Integrated Circuits Strategy, the Department continued to work supply chain risk issues both internally through DoD software and systems assurance efforts beginning in 2004, and within the interagency through the Committee on National Security Systems. Its strategy is holistic: System prioritization allows the Department to apply resources first against our most critical systems; an approach to driving assurance activities into the systems engineering process, to identify critical sub-systems and components, and to mitigate vulnerability through engineering design; a supplier assurance process to increase knowledge of counterintelligence threats posed by the suppliers' chain; a technology strategy to improve vulnerability detection capability, and a collaborative effort between DoD and industry to identify standards and best practices. This approach was validated by a September 2007 Defense Science Board study "Mission Impact of Foreign Influence on DoD Software," and informed subsequent efforts within DoD and the interagency.

The Department now co-leads an interagency effort with the Department of Homeland Security to develop a multi-pronged, US Government (USG)-wide approach to global supply chain risk management for hardware and software ICT. This effort brings to bear a range of USG capabilities to address national security risk to USG systems and

networks from globally developed and maintained ICT through sharing of technical risk mitigation techniques, development of new acquisition guidance, work with industry on the promulgation of commercial standards, and enhancement of IT and software assurance capabilities. The Department has recently issued policy for managing supply chain risk to ICT within DoD critical information systems and weapons systems in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23. Additionally, the policy establishes Department-wide responsibilities for meeting the assessment and reporting requirements of §254 of the Fiscal Year 2009 National Defense Authorization Act.

The Department is incrementally developing a supply chain risk management (SCRM) capability, beginning with pilot activities in fiscal years 2009-2010 and progressing to full operational capability by fiscal year 2016. These pilots are a joint effort led by the Deputy Assistant Secretary of Defense for CIIA. Each of the military services and DISA has identified pilot programs to test SCRM engineering and procurement processes and mitigations and share best practices. The Department is also partnering with the IC in evaluating the risk to the Department posed by commercial entities conducting business with the individual components of the Department.

Ultimately the goal of the SCRM pilots is to position supply chain risk management decision-making very early in the system lifecycle. Early identification of risk facilitates

mitigation through system design and ensures that ICT products purchased for use on DoD systems and networks are sufficiently trustworthy for their intended purpose.

Assurance in Defense System Acquisitions

Complementary to the SCRM efforts are the DoD CIO's responsibilities for overseeing the integration of IA/CS into major defense system acquisition programs to ensure compliance with statute, and consistency with DoD policies, standards and architectures. Under Subtitle III of Title 40, United States Code (formerly the Clinger-Cohen Act of 1996), the Department conducts formal reviews of the acquisition IA strategies of all Major Automated Information Systems (MAIS) and Major Defense Acquisition Programs (MDAP) prior to approval of all acquisition milestone decisions. The acquisition IA strategy sets the stage for early, effective, and efficient implementation of IA into the system.

The Department emphasizes the early identification of IA/CS requirements for all IT acquisitions, including weapons systems and command and control systems. An IA/CS controls-based approach is employed that mandates a comprehensive set of protection requirements based on the sensitivity of the information and the importance of the mission that the system supports. The specific IA/CS technical solutions that satisfy the individual IA/CS controls must be certified as effective and secure before implementation into the systems. Leading-edge networking programs are required to comply with similarly leading-edge information security requirements from NSA to ensure that new

capabilities are protected. Finally, the system as a whole is subjected to a rigorous independent security review and an overall risk management decision prior to allowing it to operate. The Department is working to streamline the fielding of ICT commercial solutions, accelerate the certification and accreditation process, and achieve greater reciprocity of IA/CS risk management processes and decisions across the Department and federal government.

A particular challenge in this area is acquisition time. Our reliance on globally sourced ICT means our adversaries have access to the same technologies we do; however, our ICT and IA/CS acquisitions must follow the same rules as for weapons systems, constraining our ability to respond quickly. We need more agile ICT and IA/CS acquisition processes. Acquiring automated information systems without a production component is significantly different from acquiring a weapons system. For weapons systems we concentrate on key risk areas like technology maturity and producing large numbers of custom hardware in economic quantities. In contrast, for automated information systems we concentrate on reducing risk in areas like process reengineering, enterprise architectures, information assurance, and integration of multiple commercial off-the-shelf applications.

The challenges of information technology acquisition were studied by the Defense Science Board as directed in the fiscal year 2008 National Defense Authorization Act. The results of their study were recently released (April

2009) and recommended changes to our acquisition processes, for the rapid acquisition and continuous upgrade and improvement of IT capabilities. A process that is agile and geared to delivering meaningful increments of capability in approximately 18 months or less.

DoD has recently instituted a new rapid intergovernmental acquisition process that develops multiple competitively-awarded Blanket Purchase Agreements (BPAs). In partnership with the General Services Administration (GSA), this process provides BPAs in six months for heavily discounted IA/CND products available for federal, state, local, and tribal government agencies.

Network Resiliency

Denial of service against critical elements of the physical and application layer of the networks and cyber attacks effecting the integrity and confidence of information flowing to users and decision makers is increasingly a major source of risk, as shown by recent undersea communications cable cuts or threats by software worms like Conficker. The Department's Guidance of the Development of the Force (GDF) for 2010-2015, signed May 2008 states, "All DoD Components will reduce the risk of degraded or failed missions by developing doctrine/tactics, techniques and procedures and planning for, implementing, and regularly exercising the capability to fight through cyber or kinetic attacks that degrade the Global Information Grid."

In support, we have a series of cyber resiliency and mission assurance initiatives that are focused on reducing risks to missions should our networks, enterprise services, or information be compromised or degraded. They include:

- Exercising military operations under a severely degraded cyber environment.
- Improving prioritization for recovery and continuity of operations planning.
- Strengthening network command and control capabilities.

While the Department is aggressively enhancing the security of the GIG and promoting IA/CS nationally and internationally, the threats in an information-centric world are dramatic. Conducting counterterrorism operations, global peacekeeping, homeland security and preparing for escalated warfare make it imperative that IA/CS be viewed not as an IT expense but as a critical enabler of all national security and defense capabilities. To this end, the Department sees its participation in the Comprehensive National Cyber Initiative (CNCI) as imperative. The Department leads or co-leads several CNCI initiatives:

- Initiative 3, with the NSA supporting Department of Homeland Security efforts to secure the .gov domain.
- Initiative 7, with the Department and the DNI co-leading an effort to secure the classified networks.
- Initiative 8, with the Departments of Defense and Homeland Security developing the conceptual foundation for building the USG cyber workforce of the future and reinforcing the skills of the current workforce.
- Initiative 11, previously discussed under SCRM.

Summary

In conclusion, the Department has a strong IA/CS vision, strategy and supporting program. We are working toward a resilient and defendable core network for the Department and for the nation. The ASD(NII)/DoD CIO is managing a diverse portfolio to lead the Department toward Net Centric operations and aggressively working to get ahead of the daunting security challenges facing the Department.

Statement for the Record

Lieutenant General Keith Alexander

Commander

Joint Functional Component Command for Network Warfare

Before the

House Armed Services Committee

Terrorism, Unconventional Threats, and Capabilities

Subcommittee

5 May 2009

(U) Introduction

(U) Chairman Smith, distinguished members of the committee, thank you for the opportunity to discuss the military's cyberspace mission and some of the challenges we face executing the responsibilities assigned to us by United States Strategic Command (USSTRATCOM).

(U) Background

(U) As you are all well aware, our economy, the nation's critical infrastructure, and many of our military operations depend on unfettered access to cyberspace. Cyberspace has clearly changed the way we interact as a global community. More than that, it has influenced business processes, the management of critical infrastructure, and human interaction in ways that were not foreseeable just 15 years ago. However, this advancement in technology comes with vulnerabilities for our nation that have not been adequately addressed.

(U) The vast array of electronic devices populating the global information infrastructure today remain the functional tools of cyberspace, and any of these devices, or the underlying software, can be used for both beneficial or malicious purposes. As cyberspace continues to evolve and grow in complexity and importance, our nation must vigilantly maintain technological dominance and freedom to maneuver within this global domain. This statement will focus on the latter in an attempt to provide this Committee insight into how the DoD is organizing to operate in the cyber domain, how we operate in the environment and some initial thoughts regarding deterrence.

(U) JFCC-NW Organization Overview

(U) As the Commander, Joint Functional Component Command for Network Warfare (JFCC NW), it is my responsibility to support USSTRATCOM's mission to plan, coordinate, and conduct offensive and defensive cyberspace operations. Executing this mission requires assembling and maintaining a force capable of adapting to, and operating in, a complex and continually evolving and expanding environment. Unlike the land, sea, air and space where the laws of physics do not change, cyberspace is a man-made creation that continually changes and evolves – operating effectively in this kind of environment requires that we leverage the expertise from a wide variety of disciplines. Moreover, we must close the seams between information assurance, network operation and defense, intelligence collection and offensive operations. Recently the Commander, USSTRATCOM, placed the Joint Task Force – Global Network Operations (JTF-GNO), which directs the operation and defense of DoD's networks under my operational control in order to better integrate and synchronize defensive cyber operations. This necessary initial realignment is a significant step towards the establishment of a command that is organized to operate and defend vital networks and project power in cyberspace.

(U) The next steps in this transformation will require a more substantial reorganization, which is one reason why the DoD is considering the establishment of a new sub-unified command for Cyber, under USSTRATCOM, that would be headquartered at Fort Meade. The creation of a single, sub-unified cyber command would provide the DoD with a command comprised of forces and capabilities better aligned to conduct cyber operations and capable of evolving to meet and overcome challenges presented by operating in cyberspace at the speed of cyber.

(U) Operating in Cyberspace

(U) Maintaining freedom of action in cyberspace in the 21st Century is as inherent to U.S. interests as freedom of the seas was in the 19th Century, and access to air and space in the 20th Century. This is especially true since the United States is committed to leading international and domestic efforts to ensure the security of global information infrastructures upon which cyberspace depends; maintaining the capabilities to use cyberspace as a medium to deter, deny, or defeat any adversary seeking to harm U.S. national and economic security; while ensuring actions are undertaken in a manner that protects our Constitutional liberties. The ability to operate freely within cyberspace poses a number of unique challenges.

(U) The rapid expansion and global dependence upon cyberspace required the Defense Department to evolve its warfighting doctrine to include cyberspace as a viable domain on par with the domains of the land, sea, air and space. As I have mentioned, cyberspace is unlike the other warfighting domains, it is a man-made technological phenomenon solely reliant upon human activity. The Department of Defense defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers." [1]

(U) The uniqueness of cyberspace can best be described by three attributes: volume, speed, and convergence.

(U) Perhaps the characteristics of volume and speed are best known, as the truly unprecedented volumes of data and speed at which communications occur in cyberspace are demonstrated daily. More than the speed of the communications, the rate of change of cyberspace, and the applications that use it, is continuous, making this domain ever evolving. However, the convergence of communications devices being driven by cyberspace is fueling an integration that has far reaching consequences, both positive and negative, that must be appreciated if one is to understand this domain.

[1] See Deputy Secretary of Defense Memorandum, Subject: *The Definition of Cyberspace*, May 12, 2008 (The Department of Defense holds this definition is consistent with the definition of cyberspace provided in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), which states that cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.).

(U) The integration taking place in communication devices is easy to see in our daily lives. What were once separate communications means such as telephones, cell phones, television, radio and computers are increasingly being combined into single devices, allowing us to watch video or send email on our cell phone or use the telephone over the Internet. Fundamentally, this is only possible because of a much greater integration occurring behind the scenes, the increasing merger of what were once separate communication networks into one network-of-networks. Accordingly, what were once distinct networks carrying the communications of our adversaries, allies and ourselves have also merged into one network-of-networks – "cyberspace".

(U) And while it may be hard to believe for something that has become so important and so much a part of the fabric of our lives, cyberspace largely "happened." It was not planned or designed to serve the purposes for which it is being used today. And while the concept to make it easier for people to communicate by connecting networks was conceived and given life in the United States, it resulted in a global domain that knows no geographical boundaries, is largely unregulated and impossible to fully secure. There is no one entity, be it from the private sector or from the community of nations, "in charge" of cyberspace, which means that there is no one entity that can change cyberspace to eliminate the negatives while keeping the benefits. Thus, cyberspace is a perfect environment for United States adversaries to thrive and a domain that the United States must vigilantly protect.

(U) Deterrence Strategies

(U) Robust information assurance and securing vital networks must be our first priority. Our people play an important role in preventing unauthorized access to the critical systems in cyberspace. The cyber security training provided to our service men and women, and the civilian and contractor workforce is inadequate and must be improved.

(U) Secondly, the defense of our networks must be accountable to the highest levels, and managed as such. It is imperative that all commanders enforce measures to ensure the readiness of networks managed by personnel under their purview. Our adversaries are taking advantage of this lack of assiduousness and discipline that ultimately costs hundreds of millions of dollars in lost information and work hours.

(U) Finally, we must leverage the power of automated security protocols to effectively manage these threats we face every day. For example, deploying a host based security system will provide a level of security that potentially will operate at the speed of the network, and centrally update systems to a trusted baseline.

(U) Conclusion

Cyberspace is a uniquely complex domain absolutely vital to the nation. For the Department of Defense to operate freely within the cyber domain it must devote sufficient

resources and personnel to ensure mission success. This includes creating an organizational construct that aligns and synchronizes forces so that they are able to operate and defend the military's network and project power at "network speed".

Traditionally, military action is an option of last resort that should complement deterrence strategies. Within the DoD, deterrence can be partially achieved through the creation and maintenance of a cyber force capable of freely operating within cyberspace.

Thank you for providing me with this opportunity and I will try to answer any questions that you may have.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MAY 5, 2009

QUESTIONS SUBMITTED BY MR. SMITH

Mr. SMITH. Knowing that our IT adversaries are becoming more complex, what steps is the Army taking to protect our wireless communications?

Mr. KRIEGER. The Army places tremendous focus on Transmission Security (TRANSEC) in order to protect our wireless communications from detection and interception. To mitigate this increasingly adept and complex threat we maintain rigorous Certification and Accreditation programs for our IP based networks; including routine network scanning for unauthorized wireless access points and systems. Technical mitigation strategies are used to reduce the probability of detection and interception of our FM tactical communications systems. Encryption is used on our FM and IP networks using NSA approved type 1 encryption while traversing the wireless spectrum. Additionally, the Army is leveraging OSD's cooperative program with major defense contractors to identify and remediate efforts to exploit wireless communications network vulnerabilities.

Mr. SMITH. What is the process for remediating a hardware or software vulnerability identified during an information assurance vulnerability assessment? Are there institutional processes and funds available, or are you forced to "take this out of hide."

Mr. KRIEGER. The Army participates in the DOD Information Assurance Vulnerability Management (IAVM) program which identifies and resolves discovered vulnerabilities in systems and platforms. It requires the completion of four distinct phases to ensure compliance. These phases are: (1) vulnerability identification, dissemination, and acknowledgement; (2) application of measures to affected systems to make them compliant; (3) compliance reporting; and (4) compliance verification. This program includes Information Assurance Vulnerability Alerts (IAVAs), Information Assurance Vulnerability Bulletins (IAVBs), and technical advisories. The Army Global Network Operations & Security Center (A–GNOSC) is the Army's focal point for coordinating the mitigation efforts for identified vulnerabilities across the Army. While institutional processes are used and some centralized support is available, the Army still is required to "take out of hide" resources in order to mitigate information assurance risks.

Mr. SMITH. What are you doing in the Services and OSD to develop a career cyber force?

Mr. KRIEGER. The Army is evaluating the current force and comparing it to the requirements of the proposed cyber force. Once the analysis is completed, the Army will develop a management program to meet the requirement.

Mr. SMITH. What incentives are available to recruit and retain the types of individuals you would like to attract to the military cyber corps? Are there other incentives that you would like to be able to offer, but do not currently have the authority to provide?

Mr. KRIEGER. The Army continually reviews its incentives for recruiting and retaining individuals who have critical skills. The Army manages its resources to achieve the best possible outcome. If given additional resources the Army could increase its ability to offer more incentives to achieve better outcome.

Mr. SMITH. What kinds of leap-ahead technologies do you believe we need to be investing in?

Mr. KRIEGER. Technologies which can provide the Army with a superior advantage to prevent, detect, analyze, and respond to threat events at network speed.

Mr. SMITH. The outsourcing of NMCI resulted in an outsourcing of much of the brains of the Navy, especially with regards to technical and architectural designs and senior-level technology management. What is the Navy doing to rectify that situation?

Mr. CAREY. Although NMCI caused a shift in responsibility for core network operations to industry, the Navy and Marine Corps retained a significant amount of technical, architectural and technology expertise supporting other networks, including afloat, overseas, in-garrison, medical, educational, and research and development networks. One of the principal concepts of the Next Generation Enterprise Network (NGEN) program is to restore the decision-making, design control and oversight to the DON. A modest recruiting campaign for network talent will com-

mence in Fiscal Year 2010, and we have established a comprehensive training and education strategy embodied in our IT of the Future program. As the DON implements the concepts of the Naval Networks Environment 2016, prioritized decision making, design control and oversight positions will be filled by members of the government workforce.

The DON will also partner with other organizations, including the Defense Information Systems Agency (DISA), the Defense Advance Research Projects Agency (DARPA), and other DOD Services and Agencies for analysis, best practices and lessons learned. Finally, private sector design development and technological expertise will continue to support government workforce decision making and oversight.

Mr. SMITH. What is the process for remediating a hardware or software vulnerability identified during an information assurance vulnerability assessment? Are there institutional processes and funds available, or are you forced to "take this out of hide."

Mr. CAREY. The DON fully supports the IAVA process and a tool by which we can improve our network security posture. Institutional processes are in place if vulnerabilities are found during a vulnerability assessment. This guidance can be found on the DISA Information Assurance Support Environment page located at http://iase.disa.mil/index2.html. Specific actions are provided in the DISA IAVM Handbook. The DON provides additional guidance within our IA Policy document and our IA Manual.

When a vulnerability notice has been issued by the JTF–GNO/NetDefense, the DOD Vulnerability Management System (VMS) sends email notices through command channels to the individuals responsible for the affected assets. Notices are also sent to all IA Managers and organizational oversight users. The VMS notice directs users to access the JTF–GNO/NetDefense Web Page to obtain detailed information on the specific vulnerability.

Funding for routine hardware/software support is part of the annual IT support budget for most programs. If an upgrade is required that is outside the scope of the support contract, then funding for these "previously unknown" vulnerabilities must be found using the DON process for conducting budget trade analyses.

Mr. SMITH. What are you doing in the Services and OSD to develop a career cyber force?

Mr. CAREY. DON is working closely with DOD leadership and the other Services to determine the scope, missions, functions and tasks relevant to the cyber workforce. We are working with operational organizations including the National Security Agency (NSA) and the new U.S. Cyber Command to determine DON roles and responsibilities and to implement the DON command and control necessary to support cyber operations. We are also exchanging information on manpower, personnel, training and education requirements and solutions development with DOD and the other Services to leverage work done by others as we determine the best means of meeting DON cyber missions.

The Secretary of the Navy has issued policy that designates the Under Secretary of the Navy as the DON Chief Cyberspace Officer, with the DON CIO and the DUSN as his chief advisors for CND/CandA/CNE. The document also directs the Chief of Naval Operations and the Commandant of the Marine Corps to establish organizational constructs for cyber operations and to maximize training and education efficiency in cyberspace career fields. Additionally, the policy directs DON CIO to work directly with DOD and DON cyberspace leadership to develop workforce policy and guidance and to work with the Assistant Secretary of the Navy for Manpower and Reserve Affairs to track and measure the effectiveness of cyberspace manpower, personnel, training and education efforts.

Both the Navy and Marine Corps headquarters staffs are working to document cyber manpower, personnel, and training and education requirements. This team includes professionals from each of the communities that supports cyber operations and reports to the Chief of Naval Operations or the Commandant of the Marine Corps.

The Navy is the executive agent for the Joint Cyber Analysis Course attended by personnel from all Services. Additionally, the DON participates in the DOD Information Workforce Improvement Program which provides Joint opportunities for Information Assurance training and certification.

Mr. SMITH. What incentives are available to recruit and retain the types of individuals you would like to attract to the military cyber corps? Are there other incentives that you would like to be able to offer, but do not currently have the authority to provide?

Mr. CAREY. The Navy has the authorities available to recruit and retain cyber professionals. In the execution of attracting and retaining cyber professionals we will leverage accession and retention incentives where appropriate. Accession bo-

nuses, critical skills retention bonuses, scholarship for service, fellowships and post-graduate education all remain important tools that can be utilized to recruit and retain our cyber corps.

Mr. SMITH. What kinds of leap-ahead technologies do you believe we need to be investing in?

Mr. CAREY. The DON will seek to invest in and deploy emerging technologies that enable collaboration and increase the security of our networks. New technologies and capabilities, such as IPv6, self-forming wireless mobile networking (for people on-the-move, IP sensor networks, etc.), and Web 2.0 tools present opportunities worthy of investigation.

The DON must also explore the use of virtualization and cloud computing. Many organizations both within and outside the DOD are examining the use of "private clouds" to reduce costs, increase security and lessen the environmental impact of IT. Additionally, we must focus on Identity Management and Attribute Based Access Control as they increase security and enhance information sharing.

New technologies are becoming available at a rapid pace, and while our unique position requires that we be selective in which tools we implement, we continuously look for ways to increase security, promote collaboration and improve the mission effectiveness of our operating forces.

Mr. SMITH. What is the process for remediating a hardware or software vulnerability identified during an information assurance vulnerability assessment? Are there institutional processes and funds available, or are you forced to "take this out of hide."

General SHELTON. Remediation of hardware or software vulnerabilities is dependent upon type and severity of the vulnerability identified. Every organization conducting an information assurance vulnerability assessment requires local operating instructions governing remediation steps for that particular organization and for specific vulnerability levels. Institutional processes for remediating discovered vulnerabilities are defined in United States Strategic Command's Secure Configuration Compliance Validation Initiative and are inherent in the assessment tool used. No additional funds are needed because on-site vulnerability assessment personnel and system owners work together to remediate identified vulnerabilities.

Mr. SMITH. What are you doing in the Services and OSD to develop a career cyber force?

General SHELTON. The Air Force is establishing dedicated officer, enlisted and civilian cyber operations career fields to meet Joint and Service cyber missions. Additionally, we continue to participate in robust inter-Service dialogue and OSD efforts to develop DOD-wide cyber career force guidance.

Mr. SMITH. What incentives are available to recruit and retain the types of individuals you would like to attract to the military cyber corps? Are there other incentives that you would like to be able to offer, but do not currently have the authority to provide?

General SHELTON. The Air Force has many incentives available to support recruiting and retention, to include enlistment and reenlistment bonuses, undergraduate and graduate education benefits, and education with industry opportunities. At this time, we believe existing authorities and incentive programs are flexible enough to support cyber recruiting and retention efforts.

Mr. SMITH. What kinds of leap-ahead technologies do you believe we need to be investing in?

General SHELTON. Cyber technologies are a pervasive set of technologies that cannot be developed in isolation from the entire national enterprise. Communication is the foundation of effective national governance and current and future warfighting capabilities. As a result, cyber leap-ahead technology development is not being done in isolation by the Air Force. Future technologies could include self-generating communication networks that adapt to network attacks, advanced computing including quantum computer architectures and optical networks for its ability to transmit very large volumes of data over long distances. Additionally, information fusion and multi-level security could enable early detection of cyber attacks.

Mr. SMITH. In an age of increasing outsourcing and globalization, can you describe the threat to the software and hardware supply chain? What are we doing to mitigate the risks to the global supply chain?

Mr. LENTZ. While globalization has many economic benefits, it also provides increased access and opportunity for malicious actors to manipulate information and communications technology (ICT) products and services to gain unauthorized access to otherwise closed-off technologies and services. The multi-tiered, global nature of our ICT supply chain means that the government has suppliers that it may not know and may never see. With less insight into their security practices and less control over how they conduct their business, the global supply chain may make the

U.S. Government (USG) more vulnerable to a sophisticated adversary who can use security gaps in the global supply chain to alter or steal data, disrupt operations, or interrupt communications.

Threats to the ICT supply chain can affect both software and hardware products. Software is growing exponentially in size and complexity, which creates assurance challenges. In addition, software design, development, testing, distribution, and maintenance can also be done more inexpensively offshore in easier reach of malicious actors. Security of the ICT supply chain can also be compromised by untrustworthy or counterfeit microelectronic components. The semiconductor industry has increasingly moved toward offshore or foreign-owned semiconductor component production. This trend creates an increasing threat to the U.S. as the potential for unauthorized design inclusions to appear on integrated circuits used in military applications increases. Furthermore, counterfeit ICT products have the potential to fail unexpectedly and prematurely, which may cause the mission critical systems in which they are used to malfunction.

The national security concern regarding the global marketplace is that software or microelectronic circuitry may include deliberately-inserted malicious logic or "malware" that an adversary might slip into a computer system to steal or corrupt data or disrupt the system. The malware might act immediately, or it may be designed to lie dormant until it is activated by a future signal. Buried in the millions of lines of code that comprise the modern computer application, such malware is difficult to detect with malware protection applications, and no one may be aware of its existence until after the damage is done.

DOD approaches supply chain risk management (SCRM) through a defense-in-breadth strategy—a multi-faceted risk mitigation strategy that seeks to identify, manage, mitigate, and monitor risk at every stage of the system or network lifecycle, from product design to system retirement. DOD is actively working to ensure that policies and processes are put in place to raise awareness of the risk, empower acquirers to make informed decisions when they procure and integrate ICT products and services, and arm acquirers with practices and tools necessary to mitigate risk when ICT products are used across the government.

DOD is incrementally implementing SCRM through pilots in fiscal year (FY) 2009 and FY 2010 and will be fully executing SCRM by FY 2016. In addition, the Department is analyzing existing regulatory and legislative authorities to provide guidance on the use of SCRM in procurement planning and decision making, and to recommend proposed clarification of DOD authorities to reduce litigation risks associated with managing supply chain risk during acquisition. DOD is also collaborating with industry to develop standards and best practices that recognize security challenges in commercial global sourcing. Finally, under the Comprehensive National Cybersecurity Initiative, DOD is working with other federal agencies to develop a multi-pronged, USG-wide approach to global supply chain risk management where best practices, risk mitigation techniques, and lessons learned are shared and the overall risk posture of the USG is enhanced.

Mr. SMITH. How might we better utilize acquisition regulations and contracting clauses to better enforce the cybersecurity posture of our defense contractors?

Mr. LENTZ. DOD plans to publish an Advance Notice of Proposed Rulemaking (ANPR) in the near future to obtain public input on needed changes to the Defense Federal acquisition Regulation Supplement with regard to safeguarding and cyber intrusion reporting of unclassified DOD information within industry. The establishment of minimum safeguarding requirements for unclassified DOD Program Information on defense Industrial Base (DIB) partner networks will identify cyber security as a standard practice, and address vulnerability to compromise, loss, or exfiltration of unclassified DOD Information.

Mr. SMITH. What is the process for remediating a hardware or software vulnerability identified during an information assurance vulnerability assessment? Are there institutional processes and funds available, or are you forced to "take this out of hide."

Mr. LENTZ. The Department's Information Assurance Vulnerability Management (IAVM) Program is specified in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 Change 2, dated 26 Jan 2006. This policy provides reporting and compliance guidance for publishing Information Assurance Vulnerability Alerts (IAVAs) for all Combatant Commands, Services, Agencies, and Activities (CC/S/As). IAVAs address immediate threats to the Departments Global Information Grid. IA vulnerabilities, whether they be in the form of IAVAs or found during routine evaluations, are tracked in a Vulnerability Management System (VMS) managed by the Defense Information Systems Agency. In support of this policy, each CC/S/A must report acknowledgment, mitigation, and expected correction date to the VMS database. All systems must either be patched or have an approved Plan of Action and

milestones (POA&M), for mitigations to be implemented. Vulnerability assessments not only address cyber vulnerabilities, but also identify out of date software, physical security problems, and system configuration issues, etc.

In addition, DOD Instruction 8510.01, "DOD Information Assurance Certification and Accreditation Process (DIACAP)," dated 27 November 2007, identifies detailed life cycle support requirements for information systems and addresses high-level procedures related to the Protect; Monitor, Analyze, and Detect; and Respond phases of the computer network defense lifecycle. In support of this policy, the Program Manager or System Manager for DOD information systems is responsible to plan and budget for IA controls implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

While there is generally no separate funding set aside for vulnerability mitigation and related actions by CC/S/As, system mitigation efforts are considered and funded as a normal part of the CC/S/A network defense operations resources and budgeting process. Ensuring adequate life cycle sustainment resources are available is a planning, programming, budgeting, and execution process role of the CC/S/A as identified in the DIACAP. In order to facilitate standardization of vulnerability mitigation capabilities and to leverage the use of common tools, DOD currently has an enterprise software license providing tools that enable automated vulnerability scanning and remediation.

Mr. SMITH. What are you doing in the Services and OSD to develop a career cyber force?

Mr. LENTZ. The DOD is currently working with the Services, Agencies, Joint Staff, and STRATCOM to develop baseline cyber workforce standards. The current model for these standards is the DOD 8570.01–M "Information Assurance Workforce Improvement Program". The basic requirements for developing a career cyber force include:

- Defining baseline position descriptions based on functions
- Identifying positions in manpower databases
- Specifying baseline training and or certification requirements aligned to the functions performed by the positions
- Continuous education, training, and participation in exercises to maintain and expand skills

Mr. SMITH. What incentives are available to recruit and retain the types of individuals you would like to attract to the military cyber corps? Are there other incentives that you would like to be able to offer, but do not currently have the authority to provide?

Mr. LENTZ. Current incentive authorities available to provide cyber qualified members:

- Enlistment and reenlistment bonuses
- Accelerated promotion opportunities
- Recognition programs such as special patches or badges for Cyber qualified personnel
- Specialized training and education opportunities

The DOD IA Scholarship Program is a proven retention tool for Cyber security military personnel. Since the program's inception in 2001, DOD military personnel have pursued master's or PhD degrees in IA related disciplines. Graduates are working full time in strategic positions across the Department. All of the Services have participated to some capacity.

Other potential incentive authorities for consideration:

- Authorize specialty pay for cybersecurity certified personnel
- Authorize specialty pay for cyber warfare qualified personnel (once defined)

Mr. SMITH. What kinds of leap-ahead technologies do you believe we need to be investing in?

Mr. LENTZ. The philosophy explored by leap-ahead is that, while some progress on cybersecurity will be made by researching better solutions to today's problems, some of those problems may be too hard to solve; we need rather to leap over them by finding a way to make them irrelevant. This latter approach we call *changing the game,* as in "if you are playing a game you can't win, change the game!" Most of today's research, development, technology and engineering (RDT&E) efforts are focused on "playing today's game better." But, since our adversaries have an advantage in today's cyber "game," we advocate investment in RDT&E that moves us away from having to play that game, in other words, moves us towards a cyber environment where our security does not depend on the solution of today's intractable problems. To understand this paradigm shift, we can look at three areas which can

yield game change in a reasonable time frame and which would be very useful to the DOD.

1) Today's game: eliminate vulnerabilities which enable penetration;
Tomorrow's game: reduce consequences of penetration

Today users and their applications are our front line of defense against adversaries. Malware enters our systems through vulnerabilities in the applications with which we access the Internet, or is invited in by users who unwittingly download malicious attachments onto enterprise systems. Though we struggle to keep browsers patched and users aware of the latest spear phishing attacks, it is impossible to keep up, so in the new game we worry less about eliminating every vulnerability, but place an emphasis on technologies which mitigate the effects of the attacks which vulnerabilities enable. For example, using the technique of virtualization, we can create a temporary or "non-persistent" computer-within-a-computer for our risky browsing and email sessions. User mistakes don't hurt us because attacks which enter through the virtual computer never touch our mission network. Other ideas in this vein include advanced key management techniques to enable ubiquitous encryption of mission data and prevention of exfiltration of intellectual property (adversaries may get in, but they can't see anything); also a network operating system to instantiate access policy at any level of the architecture and prevent adversaries from escalating privileges (adversaries may get in, but they can't do anything).

2) Today's game: check for maliciousness;
Tomorrow's game: know what to trust

Today we spend a lot of energy testing digital content to determine whether it is trustworthy. Virus-checkers and content filters attempt to ascertain by inspection whether applications and data are safe to place on our systems. Root-kit detection tools try to tell us if our computers have themselves been compromised. All of these tools are generally only as good as the catalog of attacks they have seen before. Again, it is impossible to keep up, so in the new game the emphasis is on roots of trust, or what it is that we can know for sure about our IT assets. Using new hardware constructs like the Trusted Platform Module and techniques of measurement and attestation, we can begin to have a means to monitor and restore the integrity of computers throughout their deployment life. Other useful avenues along these lines include provenance technologies for associating integrity and authenticity proofs with all types of digital content and events; also unspoofable identity authentication to eliminate masquerades. These approaches allow us to trust our assets because we know they are good, rather than because we haven't proven that they are bad.

3) Today's game: avoid damage;
Tomorrow's game: fight through and recover quickly from damage

Today we have a large investment in perimeter defense not only to keep adversaries from learning our secrets, but also to prevent their tampering with our data and command and control systems. We have COOPs and mirrored data centers designed for recovery from physical damage. We have learned, though, that perimeter defense does not always work, and that attacks on the integrity or available of our assets look very different from flood damage or electrical blackouts, so in the new game we emphasize the ability to maintain operations in the face of attack. Virtualization can help us again here. Virtualization obviates the necessity for coupling together specific logical and physical assets. For example, each user's environment (data and computing tools) can be stored and maintained as a digital file or image in a central control area. Should those environments be lost or compromised, they can easily be "reincarnated" into any compatible physical platform. We may also choose to prophylactically refresh stored images periodically just in case. Other promising paths include "battle mode" where assets are stripped down to an easier-to-guarantee austere functionality, and self-healing to bootstrap back up.

The new paradigms described above take us to a future where we are not so vulnerable to the asymmetric advantage enjoyed today by the remote network attacker. Each of the new games takes advantage of technology which seems to be emerging on the near horizon to mitigate our need to depend on things that are too hard for us to do.

Mr. SMITH. The Secretary of Defense recently placed the Joint Task Force for Global Network Operations under the operational control of JFCC–NW. Why was that important and how does it make our DOD systems more secure?

General ALEXANDER. Earlier, the Department of Defense established two separate military cyber component commands under U.S. Strategic Command—one dedicated to defensive cyber operations (JTF–GNO), the other to building an offensive capability (JFCC–NW). However, neither of these entities was fully resourced and their

separation inherently precluded the type of dynamic defense and agile, fluid maneuvering needed to secure our equities in cyberspace. In recognition of this, the decision was made in November of 2008 to consolidate these two components. The contested cyber environment clearly demands an ability to seamlessly integrate and synchronize cyber offense with cyber defense—at network speed. Further, it requires a unifying construct with the focus, scope of responsibility and authority to succeed in this mission space. Unifying command and control along the full range of capabilities will streamline operations, improve situational awareness and ultimately provide a much more robustly and reliably defended Global Information Grid.

Mr. SMITH. What are the pros and cons of establishing a sub-unified Cyber Command under STRATCOM? How would this be different from the current structure?

General ALEXANDER. The decision to establish a sub-unified Cyber Command was made in the Office of the Secretary of Defense (OSD) and is best answered by OSD.

Mr. SMITH. What role do you have in helping define the S&T requirements for cyberoperations?

General ALEXANDER. Joint Task Force–Global Network Operations (JTF–GNO) and Joint Functional Component Command for Network Warfare (JFCC–NW) have a cadre of military, government, and contractor personnel who directly support cyber operations planning, define cyber capabilities requirements, prototype and/or manage funding, on behalf of U.S. Strategic Command, related to cyber capabilities, technical assurance and risk assessment. Collection of Combatant Command requirements is a proactive endeavor, conducted and maintained via a JWICS-based intellipedia wiki website known as the Collaborative Environment (CE).

In general, these requirements require long term solutions and extensive intelligence efforts software and hardware research development, as well as test and operational fielding. Emergent operational needs or enabling requirements are also identified by cyber operators, crisis planners and Combatant Commands, sometimes in "real time." Emergent requirements may drive more future S&T efforts but the standing Combatant Command requirements are the primary drivers for the ongoing S&T efforts which are funded through a Call for Proposals process. This also provides a direct linkage to the Service and Agency research laboratories, which are the primary developers of capabilities. The National Security Agency (NSA), JFCC–NW and JTF–GNO provide collaborative operational and technical inputs to U.S. Strategic Command's Integrated Priority List gap analysis effort to ensure both budgetary and S&T awareness of areas requiring attention.

Mr. SMITH. What is the process for remediating a hardware or software vulnerability identified during an information assurance vulnerability assessment? Are there institutional processes and funds available, or are you forced to "take this out of hide."

General ALEXANDER. As a routine matter, the remediation process for hardware and software vulnerabilities that are identified during an inspection are usually mitigated by the associated vendor. Each vendor provides fixes for products with active support for lifecycles. These fixes are provided to the users of those products at no additional costs to the user as long as they are within the supported lifecycle. In many instances Agencies will purchase an additional support agreement for specific products for technical guidance or warranties for newly purchased products. During the purchase of those products, vendors will recommend a support agreement for their product for an additional fee or on an as required basis (hourly rate). This agreement will normally provide the user with an account or support contact to access the required update or technical support information

Most large software companies (i.e. Microsoft, Cisco and Oracle etc.) will provide fixes for vulnerable software Operating Systems and applications that are still supported by the vendor at no additional cost to the user. Open source applications are usually updated/upgraded as vulnerabilities are identified by any associated developer that has technical knowledge of the affected code and is normally provided at no additional charge. At any given time a vendor patch has the ability to break something. In this case the vendor will try to provide an appropriate fix for their product however; if this is a special case you may need a Technical Support Agreement with the vendor to troubleshoot your problem which may incur an additional cost.

However, there are other significant costs associated with investigation, analysis and remediation of compromised systems outside of the normal life-cycle arrangements. This question is best answered by the individual services and agencies as they are in the best position to discuss the budgetary impact of those activities.

Mr. SMITH. What are you doing in the Services and OSD to develop a career cyber force?

General ALEXANDER. Developing cyber forces is a Service organize, train, and equip responsibility, and they are best positioned to address individual Service career field development efforts.

A lot of planning work is being done within all the Services, regarding identification of new skills needed to perform emerging missions. We must also leverage the unique contributions of universities and research institutions as well as private enterprise to ensure U.S. forces are always on the cutting edge.

The Secretary of Defense has directed all the Services to maximize the facility at the Center for Information Dominance in Corry Station, Pensacola (the Executive Agent for Cryptologic Computer Network Exploitation and Defense training) to acquire the technical skills required for cybersecurity missions. (Those with more analytic work roles receive their training at Goodfellow Air Force Base.) It is expected that graduates of both programs will be assigned to places where they can practice what they learned, gain mission experience in several sectors of Computer Network Operations, and participate in more advanced training fielded by the Services and the Crytologic Training System.

Mr. SMITH. What incentives are available to recruit and retain the types of individuals you would like to attract to the military cyber corps? Are there other incentives that you would like to be able to offer, but do not currently have the authority to provide?

General ALEXANDER. Recruiting will be one of our top priorities. Unfortunately, very little is available today as the Services do not currently recruit specifically for cyberspace forces. However, as we move forward, there are a number of recruitment and retention incentives we would recommend.

We will encourage Service "cyberspace branches" to operate independent of recruiting operations within their Service, with subject matter experts interviewing and testing candidates from within the ranks. We should provide recruiters with sufficient knowledge of the cyberspace career opportunities in DOD to address basic questions of potential recruits. We should enhance recruiting organizations with cyber mentors, test materials, and military cyberspace points of contact. And just as importantly, we must use DOD and Service public affairs resources to aggressively promote a professional cyberspace field. In addition, we should also consider the implications of total force recruitment, leveraging our Reserve and National Guard components, to identify colleagues as potential members of the DOD workforce while also identifying and considering the cyber-related talents they may bring from their civilian employment.

Once we've begun to recruit highly motivated candidates with the potential to succeed in the cyberspace workforce, we will continue to seek and leverage a wide variety of incentives and career options to retain them. Individual services should seek to introduce incentives based on their ability to attract and retain personnel can develop monetary and other incentives that are widely used across DOD. Incentives such as additional skills pay, performance and re-enlistment bonuses, special schooling and certifications, as well as advancement in specialized fields (e.g., nuclear power incentive pays) will have to be considered. We should seek to recruit DOD civilian cyber specialists from our military personnel and allow them to benefit from military retirement benefits while continue to advance their careers as government civilians. We should consider a "cyber branch" model that allows us to affect assignment tempo for exceptionally talented performers, thus allow cyber specialists to continue to work their specialties. To keep our world-class force, we need to provide non-traditional means to routinely update cyber skills and develop inter- and intra-Service competitions to identify and reward the best of the best. Finally, we should continually emphasize the uniqueness of the work, access to some of the world's most advanced cyber technologies, and the critical importance of this mission to both DOD and the nation.

Mr. SMITH. What kinds of leap-ahead technologies do you believe we need to be investing in?

General ALEXANDER. The following are examples of current investments:

- **Knowledge Management Systems (KMS).** An integrated and automated requirements database; a tools and tactics repository; and an Analyst Workcenter interface with an information warfare planning system.
- **Common Cyber Operational Picture (COP)**: Automated combination/deconfliction of germane real-time exploitation and attack warning and characterization along with real-time situational awareness of defense measures; functionally tailorable to facilitate information sharing with different U.S. agencies and allies.
- **Attribution Science**: Anti-anonymizer technologies (how to both create them and defeat them); hardware and software signatures; and tactics techniques and procedures (TTP) for operational uses.

- **Internet Governance.** Thorough research of: 1) the next generation Internet Protocol version 6 (IPv6), which is prevalent in many universities and R&D environments and is quickly emerging in many foreign sectors. 2) the ".tel" internet domain, the online equivalent to the phone directory, which is the most significant innovation in the domain name system since the advent of .com.
- **Network Traffic Interdiction Capabilities**: Capabilities facilitating interdiction of targeted traffic in transit across the global network.
- **Automated network re-configuration and Computer Network Defense applications.** Requires all of the above technologies to be applied and integrated in real-time.

QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. Define a cyber warfighter, or cyber warfare professional as he exists today.

Mr. KRIEGER. "Cyber warfigher" and "Cyber Warfare Professional" are still fluid terms; however, the terms can include professionals who perform duties under three categories: Computer Network Attack (CNA), Computer Network Exploit (CNE), or Computer Network Defense (CND)/Network Operations (NETOPS).

Mr. THORNBERRY. Describe what you envision for the cyber warfighter of the future in terms of education (undergraduate/graduate or high school only, too), training, career path, rank structure, capability, mission, responsibilities, organization, etc.

Mr. KRIEGER. Army's education, career path and management of future cyber warfighters is being developed using standard paths through our personnel management system for officers, enlisted and Department of the Army Civilians to ensure that our workforce meets the Army's needs in the Cyberspace field. The Army follows the Federal Information Security Management Act (FISMA) and Department of Defense Training and Certification mandates which require Information Security Certifications and all levels of our Information Security Professional Corp.

Mr. THORNBERRY. Given the limited pool of individuals with the necessary technical skills, as stated recently by Gen Shelton, and the growing cyber personnel requirements articulated by Secretary Gates, what is the plan to recruit, organize, train, and equip prospective and current cyber warfare professionals? Is it joint or by service? Please explain.

Mr. KRIEGER. The Army conducts ongoing reviews to ensure it is manned, trained and equipped to meet the Army's operational missions and increase the pool of eligible candidates that meet the standards for occupational skills which are deemed critical. The Army works diligently with Joint Staff and other services to combine its training and other efforts wherever possible to make sure that the needs of the Department of Defense are integrated wherever possible to increase efficiency and effectiveness.

Mr. THORNBERRY. In your opinion should the cyber warfighter be trained by service branch, jointly, jointly with service specific trailer courses, or somehow else? Why?

Mr. KRIEGER. The Army fights as a Joint/Coalition force and therefore supports Joint training to the maximum extent possible, but recognizes the peculiarities of each individual service. Joint training allows services to train to a single standard and leverages the one-time investment in infrastructure, training curriculum and reduces duplication. The Land, Air, Sea, and Space domains each have unique characteristics and challenges while working in and through the cyberspace domain. Functioning effectively in each of these domains require different equipment sets/characteristics, training/education and operational principles. As standardized and/or unique joint mission requirements are identified, specific joint trailer courses will allow the services to focus the skill sets of the personnel to satisfy that particular mission.

Mr. THORNBERRY. In the current overseas contingencies, please describe to what extent, if any, has U.S. Strategic Command (USSTRATCOM) taken an active role supporting U.S. Central Command?

Mr. KRIEGER. USSTRATCOM along with the Army Service Component Command has played a very active role in the development of Computer Network Operations tools supporting USCENTCOM. USSTRATCOM was integral in mitigating Computer Network Defense/Information Assurance issues in support of Operation Iraqi Freedom and Operation Enduring Freedom. USSTRATCOM recently marshaled resources to mitigate capacity degradation stemming from breaks in undersea cables, restoring service with no significant operational impact. USSTRATCOM's main focus over the past year has been on establishing common standards, procedures,

and discipline to better secure military networks. This benefits all warfighters, to include USCENTCOM, who are dependent on Cyberspace to conduct operations.

Mr. THORNBERRY. Irrespective of service branch, does USSTRATCOM's cyber warfighters possess the skills necessary to ensure all secure battlefield communications? Please explain.

Mr. KRIEGER. Gen Chilton, Commander USSTRATCOM, stated in Congressional Testimony to the Senate Committee on Armed Services, on 19 March 2009:

"The provisioning of adequate cyber forces to execute our assigned missions remains our greatest need in this mission area."

The Army is aware of this requirement, and has been very proactive in training, equipping and manning USSTRATCOM and its Functional Components with requested cyber warfighters to secure the internet and battlefield communications. Consistent with the National Military Strategy for Cyberspace Operations, the Army has made progress toward defining Service level requirements and advocating for Service cyberspace workforces. We understand the demands, and have moved aggressively to grow our cyber expertise; organize and orient against threats; and improve the technical and manpower capabilities our Joint Warfighters and interagency partners require for the cyberspace fight.

Mr. THORNBERRY. How is responsibility between USSTRATCOM, NSA, and DISA clearly defined in theater?

Mr. KRIEGER. Currently, USSTRATCOM operates through two subordinate component commands: Joint Functional Component Command for Network Warfare (JFCC NW) and Joint Task Force for Global Network Operations (JTF–GNO). Both commands have implemented a more responsive command and control structure reliant on centralized orders and decentralized execution. Tightening the relationship between JFCC NW and JTF–GNO this past year has led to a better, more responsive capability to defend our military networks. But, we have found the need for closer coordination and clearer delineation of responsibilities at the national and theater levels, and are moving to form USCYBERCOM. This new organizational structure will enable DOD-wide leadership to address computer security incidents and network compromises enhancing timely threat identification and mitigation through unity of effort, both within theater and globally.

Mr. THORNBERRY. Should the Department of Defense establish a "Cyber Agency" at the same level of the National Security Agency (NSA) and Defense Information Services Agency (DISA)? Why or why not?

Mr. KRIEGER. Army stands ready to support the strategy defined by Department of Defense leadership.

Mr. THORNBERRY. To what extent is the cyber domain being integrated into other domain and domain awareness initiatives (i.e. battlespace, maritime, air, space)? Please describe.

Mr. KRIEGER. The U.S. Army Training and Doctrine Command established an Integrated Capabilities Development Team (ICDT) chartered to integrate cyberspace operations into full spectrum land domain operations. This ICDT is developing a Cyberspace Operations Concept of Operations (CONOPS) which will articulate how the Army intends to fight in the Cyberspace domain which incorporates lessons learned from Operation Iraqi Freedom (OIF), Operation Enduring Freedom (OEF) and our National Training Centers which stresses integration. The CONOPS describes how the Army will use the other domains to support land component Battle command in terms of cyberspace awareness. This CONOPS will form the basis for future Army analysis and capability development efforts.

Mr. THORNBERRY. Define a cyber warfighter, or cyber warfare professional as he exists today.

Mr. CAREY. While all who engage the network to perform their missions are members of the cyber workforce, we consider a cyber warfare professional as an officer, enlisted member or civilian trained to work in an interdisciplinary domain including networks, computer applications and services. These professionals work in information operations, computer network defense, attack, and exploitation aspects of network operations, which must be aligned from end to end with the Intelligence Community. They will work as a cohesive unit, combining Intelligence and Operations to perform information assurance in protecting, monitoring, analyzing, detecting and responding to threats on the network, and manage information by retrieving, caching, compiling, cataloging and distributing it. The management mission also includes information technology system acquisition and architecture development and compliance.

Mr. THORNBERRY. Describe what you envision for the cyber warfighter of the future in terms of education (undergraduate/graduate or high school only, too), training, career path, rank structure, capability, mission, responsibilities, organization, etc.

Mr. CAREY. The DON will recruit cyber workforce personnel from multiple educational levels, hiring experienced personnel and developing the cyber skills of others through career path education and training. The DON will recruit from high school, vocational school, junior college, undergraduate and graduate programs. DON cyber personnel will be educated and trained through a blended approach of traditional schoolhouse instruction, on line, and commercial vendor instruction including cyber and information assurance certification and licensing programs, joint education, on-the-job training and qualification, and team and unit tactical training. A key element of this program will be standardized training (applicable to positions regardless of the military or civilian status of the person performing the work in the position) and education curricula to support a core capability that is fungible across the contractor/civilian/military workforces.

Rank and grade structures for military and civilian personnel will follow current structures, and it is expected that cyber workforce personnel will be required at all rank and grade levels. Career path development is still in progress as the missions, functions and tasks of the DON cyber structure are developed, but it is expected that there will be military career paths leading to the most senior enlisted and officer ranks. Civilian personnel will be able to follow paths leading to, and including Senior Executive Service positions.

The DON cyber workforce will be capable of supporting all DON missions. Within the cyber arena they will provide Computer Network Defense (CND), Network Operations (NETOPs), Information Assurance (IA), Computer Network Attack (CNA), Computer Network Exploitation (CNE), and All-Source Intelligence support; telecommunications, and management functions including design and development, strategic planning and investment, policy and planning, and acquisition.

Cyber workforce responsibilities will be split among military, government civilian and contractor support personnel as required. Decisions on workforce structure, the number of inherently governmental activities, and the scope of in-sourcing and outsourcing will be finalized following the establishment of the Department of Defense and the DON Cyber Command structures, missions, functions and tasks.

Mr. THORNBERRY. Given the limited pool of individuals with the necessary technical skills, as stated recently by Gen Shelton, and the growing cyber personnel requirements articulated by Secretary Gates, what is the plan to recruit, organize, train, and equip prospective and current cyber warfare professionals? Is it joint or by service? Please explain.

Mr. CAREY. The Department of the Navy (DON) is developing plans to recruit, organize, train, and equip military and civilian cyber warfare professionals. The first step being taken is to determine the specific skill sets needed for cyber warfare. The DON will also develop career options to support recruitment, retention, and development of personnel with the needed skill sets. The DON is looking at ways to modify career paths and improve training to prepare the current workforce to meet the cyber challenge. The Navy along with the other services will continue to leverage training and educational opportunities by sharing resources at the Center for Information Dominance, Joint/National-sponsored schools, and post-graduate schools. The task of equipping this force will follow closely the training model for the near term, primarily leveraging Joint/National capabilities.

Mr. THORNBERRY. In your opinion should the cyber warfighter be trained by service branch, jointly, jointly with service specific trailer courses, or somehow else? Why?

Mr. CAREY. Cyber warfighters must be thoroughly trained, employing both formal education and on-the-job training tracks within both their respective Services and the Joint environment. This is essential, due to the nature of cyber warfare and the need to be able to defend the Global Information Grid and its Service components. Foundational education and training should take place within the Service framework, and experienced personnel should take that knowledge into the Joint operational and training environments, facilitating DOD-wide synergies. When possible, DON cyber workforce development plans should include participation in forums including not only DOD, but also other Federal and private industry workers. Increased familiarity with non-governmental and inter/intra-agency organizations' tactics, techniques, and procedures will increase the overall efficiency and effectiveness of cyber operations supporting national security objectives.

Mr. THORNBERRY. In the current overseas contingencies, please describe to what extent, if any, has U.S. Strategic Command (USSTRATCOM) taken an active role supporting U.S. Central Command?

Mr. CAREY. The Department of the Navy Chief Information Officer respects the direction and authority of the Secretary of Defense and his assignment of Title 10 and UCP authority to CDR USSTRATCOM.

Service network operations centers (NOSCs) are under CDR USSTRATCOM's operational control. JTF–GNO orders Service NOSCs to perform network operations and defense. USSTRATCOM, through the CENTCOM AOR DON Network Operation Centers' direct reporting relationship to the Joint Task Force–Global Network Operations, is very active in providing direction on network operations and defense and ensuring computer devices and networks are compliant with published IA Vulnerability Alerts (IAVAs), Communications Tasking Orders (CTOs), Operations Directive Messages (ODMs), etc. These efforts mitigate vulnerabilities and eliminate (or reduce) the instance of infections. This work is a major challenge in the forward tactical environment where forces frequently rotate every six months to one year, bringing with them personnel who have various (often limited) levels of network administration skills. Additionally, the Commander, USSTRATCOM and his staff have traveled to the CENTCOM AOR, visiting the Defense Information Systems Agency and Service NOSCs in search of ways in which U.S. Strategic Command can better support the current overseas contingencies.

Mr. THORNBERRY. Irrespective of service branch, does USSTRATCOM's cyber warfighters possess the skills necessary to ensure all secure battlefield communications? Please explain.

Mr. CAREY. The Department of the Navy Chief Information Officer respects the direction and authority of the Secretary of Defense and his assignment of responsibilities to USSTRATCOM. However, it should be noted that most technical work in the battlefield/AOR is performed by Service-specific personnel/organizations, and not USSTRATCOM personnel.

Mr. THORNBERRY. How is responsibility between USSTRATCOM, NSA, and DISA clearly defined in theater?

Mr. CAREY. The Department of the Navy Chief Information Officer respects the direction and authority of the Secretary of Defense and his assignment of Title 10/50 and UCP authorities to CDR USSTRATCOM, NSA, and DISA. The in-theater responsibilities of USSTRATCOM, NSA, and DISA are outlined in Chairman, Joint Chiefs of Staff Directives and Instructions, including interactions with COCOMs and the Services. NSA responsibilities are also found in U.S. Signals Intelligence Directives (USSIDs).

Mr. THORNBERRY. Should the Department of Defense establish a "Cyber Agency" at the same level of the National Security Agency (NSA) and Defense Information Services Agency (DISA)? Why or why not?

Mr. CAREY. The Department of the Navy Chief Information Officer respects the direction and authority of the Secretary of Defense in his establishment of the USCYBERCOM. The SECDEF memo of 23 June 09 stated it best when it said that the "Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners." The DON supports the establishment of U. S. Cyber Command, which presently appoints the Director, National Security Agency the Commander, U.S. Cyber Command, making the integration of activities easier. The Director of the Defense Information Systems Agency (DISA) is tasked to provide network and information assurance technical assistance to USCYBERCOM as required. The Joint Task Force–Global Network Operations (JTF–GNO) and the Joint Functional Component Command for Network Warfare are merged into the new Cyber Command, bringing together the strengths of both of these commands. The DON believes that functional reporting relationships between the cyber operating forces, USCYBERCOM and the Military Departments and Services must be established to ensure efficient and effective command and control of these vital assets.

Mr. THORNBERRY. To what extent is the cyber domain being integrated into other domain and domain awareness initiatives (i.e. battlespace, maritime, air, space)? Please describe.

Mr. CAREY. In May 2008, the Department of Defense published the following definition of cyberspace: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." This definition is almost identical to that which was developed by the Department of Homeland Security and the National Institute of Standards and Technology.

The Information Technology Reform Act of 1996 (Clinger Cohen Act) defines IT as: "Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information." The term information technology includes computers, ancillary equipment,

software, firmware and similar procedures, services (including support services), and related resources.

Given these terms of reference, Cyberspace (IM/IT) is present in all domains. The ability to operate within cyberspace is vital to the DON's mission. Achieving an appropriate balance between the need to collaborate and share information and the need to protect information will be key to our success.

The DON has established a DON Enterprise Architecture framework or "blueprint" to enable the exchange of information, integration of systems and management of resources to support cyberspace domain capabilities across all mission areas (surface (sea and ground), sub-surface, air and space). Further, to support system development and integration, the DON mandates use of the Defense Information System Registry (DISR) as its authoritative standards source. The DON established a governance structure to ensure adherence to the DON EA framework and standards in system development supporting the cyberspace domain.

Mr. THORNBERRY. Define a cyber warfighter, or cyber warfare professional as he exists today.

General SHELTON. Cyber warfighters are skilled professionals working to deter and prevent cyberspace attacks against vital U.S. interests, ensure our freedom of action in cyberspace, respond to attacks and reconstitute operations, develop persistent cyberspace situational awareness and defeat adversaries operating through cyberspace.

Today, these personnel are drawn primarily from communications, intelligence and engineering specialties, often returning after a single assignment. While initially adequate, cyberspace has emerged as a dynamic and technically demanding warfighting domain of strategic national importance. The Air Force recognizes this and has committed to establishing dedicated officer, enlisted and civilian career fields to meet emerging demand and address recruiting, training, retention and force development challenges.

Mr. THORNBERRY. Describe what you envision for the cyber warfighter of the future in terms of education (undergraduate/graduate or high school only, too), training, career path, rank structure, capability, mission, responsibilities, organization, etc.

General SHELTON. Cyber warfighters are skilled professionals working to deter and prevent cyberspace attacks against vital U.S. interests, ensure our freedom of action in cyberspace, respond to attacks and reconstitute operations, develop persistent cyberspace situational awareness and defeat adversaries operating through cyberspace.

Today, these personnel are drawn primarily from communications, intelligence and engineering specialties, often returning after a single assignment. While initially adequate, cyberspace has emerged as a dynamic and technically demanding warfighting domain of strategic national importance. The Air Force recognizes this and has committed to establishing dedicated officer, enlisted and civilian career fields to meet emerging demand and address recruiting, training, retention and force development challenges.

Mr. THORNBERRY. Given the limited pool of individuals with the necessary technical skills, as stated recently by Gen Shelton, and the growing cyber personnel requirements articulated by Secretary Gates, what is the plan to recruit, organize, train, and equip prospective and current cyber warfare professionals? Is it joint or by service? Please explain.

General SHELTON. Growing and developing cyber forces is a DOD-wide challenge. Recognizing this, the Services are cooperating with each other, Joint Staff and OSD to develop new approaches and more effective solutions for recruiting, acquisitions, training and retention.

Mr. THORNBERRY. In your opinion should the cyber warfighter be trained by service branch, jointly, jointly with service specific trailer courses, or somehow else? Why?

General SHELTON. Initial training of cyber forces should be conducted by the Services, with joint post graduate training reserved for specialized tasks.

Mr. THORNBERRY. In the current overseas contingencies, please describe to what extent, if any, has U.S. Strategic Command (USSTRATCOM) taken an active role supporting U.S. Central Command?

General SHELTON. Congressman, I would respectfully ask that this question be directed to the Commander of U.S. Strategic Command, General Chilton, who can provide you with the most up-to-date and accurate information regarding his command's support to U.S. Central Command.

Mr. THORNBERRY. Irrespective of service branch, does USSTRATCOM's cyber warfighters possess the skills necessary to ensure all secure battlefield communications? Please explain.

General SHELTON. Congressman, I would respectfully ask that this question be directed to the Commander of U.S. Strategic Command, General Chilton, who can provide you with the most up-to-date and accurate information regarding his command's ability to secure battlefield communications.

Mr. THORNBERRY. How is responsibility between USSTRATCOM, NSA, and DISA clearly defined in theater?

General SHELTON. Congressman, I would respectfully ask that this question be directed to the Commander of U.S. Strategic Command, General Chilton, the Director of NSA, Lieutenant General Alexander, and Lieutenant General Pollet, the Director of DISA, who can provide you with the most up-to-date and accurate information regarding the division of their responsibilities in theater.

Mr. THORNBERRY. Should the Department of Defense establish a "Cyber Agency" at the same level of the National Security Agency (NSA) and Defense Information Services Agency (DISA)? Why or why not?

General SHELTON. Currently, it is the Secretary of Defense's intent to establish a U.S. Cyber Command as a sub-unified command under U.S. Strategic Command. The Air Force is standing up the 24th Air Force in order to present Air Force cyber forces to this command. The Air Force stands ready to respond to any cyber-related requirements from the Department.

Mr. THORNBERRY. To what extent is the cyber domain being integrated into other domain and domain awareness initiatives (i.e. battlespace, maritime, air, space)? Please describe.

General SHELTON. Secretary Gates' decision to stand-up USCYBERCOM indicates the importance the Department of Defense places on this domain. The Air Force also recognizes the criticality of cyberspace to Joint and AF operations and is standing up 24th Air Force to focus on this key area. The integration of cyberspace operations with other operations happens at Joint and Service levels. For the Air Force, this integration will occur at 24 AF with USSTRATCOM/USCYBERCOM and at Air Operations Centers (AOC) supporting Combatant Commanders (CCDR). When CCDRs rely on reach-back cyberspace operations, Airmen in the 24 AF and AOCs will facilitate integration of applicable AF capabilities.

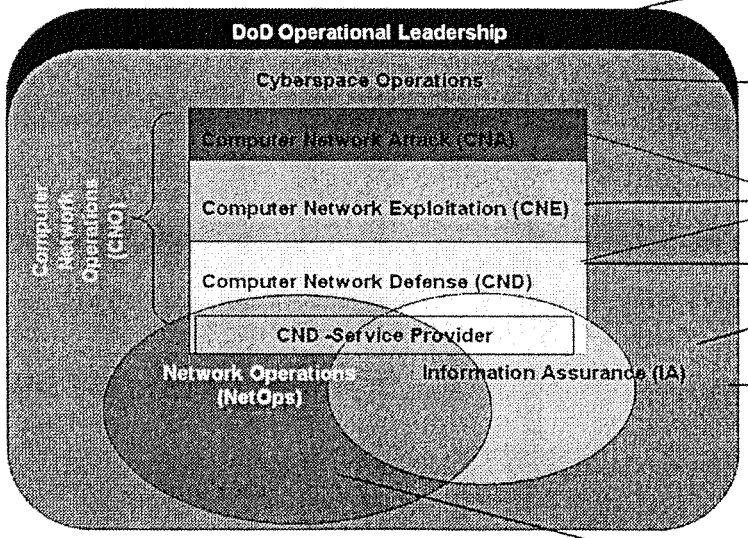
Mr. THORNBERRY. Define a cyber warfighter, or cyber warfare professional as he exists today.

Mr. LENTZ. The Cyber warfighter is evolving from a variety of military specialties such as Intelligence, Communications, Information Technology, and Information Assurance. The primary roles currently identified for Cyberspace Operations include military, civilian, and contractors performing:

- Computer Network Operations (CNO) Execution, consisting of:
  - Computer Network Attack (CNA)
  - Computer Network Exploitation (CNE)
  - Computer Network Defense (CND)
  - Network Operations (NetOps)
  - Information Assurance (IA) Computer Network Defense Service-Providers

The "Cyber-warfighter" is a relatively new concept. The Department is developing the concept of operations. This includes the structure, missions, career progression and general responsibilities of the developing Cyber workforce. The diagram below suggests notional thoughts on the integration of the various components of the Cyber workforce.

IA/Cybersecurity Workforce Overview



Integrate cyber and IA content into professional military education

Provide special cyber ops training for planners

Training provided by services/NSA

IA/Cybersecurity exercises

DoD 8570.01-M "IA Workforce Improvement Program" - identify, train, certify, continuous education, and exercises

IT Workforce Training Programs

Mr. THORNBERRY. Describe what you envision for the cyber warfighter of the future in terms of education (undergraduate/graduate or high school only, too), training, career path, rank structure, capability, mission, responsibilities, organization, etc.

Mr. LENTZ. Cyber Warfighter Education and Training will depend on how the position/person supports cyber warfighting. We anticipate the cyber warfighter of the future to reflect the following basic education and training qualifications:

Military Officers: Receive professional military education in conjunction with cyber specific training so that they can conduct cyber warfare in their role as leaders and managers.

Education:

- Bachelor or advanced degree preferably in information systems related program
- Service officer basic professional education
- Service intermediate professional education
- Service/Joint Warfare Command and Staff College

Training:

- Common foundational cyber warfare skills at career start
- Functional mission specific cyber warfare skills at mid-career
- Senior strategic leadership training across the cyber warfare domain
- Baseline IA/IT commercial certification

Government Civilian Cyber Warfare Managers: May receive DOD education in conjunction with cyber training so that they can apply cyber to their role as managers.

Education:

- Bachelor or advanced degree preferably in information systems related program
- National Defense University (NDU) Information Resource Management College (IRMC) professional development programs or certificates.

Training:

- Component-specific policy, processes, and requirements
- Cyber related continuous training
- Component-specific/sponsored cyber courses
- Baseline IA/IT commercial certification

Contractors performing cyber warfare management roles should meet the same/equivalent education and training as their government counterparts. DOD unique training or equivalent should be available to contractors.

Military Operators (hands-on/technical): We anticipate these individuals will receive cyber warfare training along with their military and technical education for their role as operators.

Education:

- High school/community college
- Rank/Grade appropriate professional education

Training:

- Basic and advanced cyber related occupational specialty training
- NetOps/IA certification depending on position requirements
- Operational and exercise training

Government Civilian Operators (hands-on/technical): Receive cyber training, which they apply along with their technical education to their role as operators.

Education:

- Community college/baccalaureate degree in information technology field

Training:

- NetOps/IA certification depending on position requirements
- Operational and exercise training

Contractors performing cyber warfare technical roles should meet the same/equivalent education and training as their government counterparts. DOD unique training or equivalent should be available to contractors.

Mr. THORNBERRY. Given the limited pool of individuals with the necessary technical skills, as stated recently by Gen Shelton, and the growing cyber personnel requirements articulated by Secretary Gates, what is the plan to recruit, organize, train, and equip prospective and current cyber warfare professionals? Is it joint or by service? Please explain.

Mr. LENTZ. There are several steps required to recruit and train personnel into the cyber workforce. The Services and Agencies are specifically responsible for accomplishing these tasks in compliance with DOD policy (which is still evolving for cyber warfare and its workforce). Based on current processes, the following actions must be accomplished by the Services and Agencies to develop a Cyber Workforce:

- Define their cyber workforce (what are the position requirements)
- Identify their position requirements
- Document manning requirements/table of organization
- Program and budget to fill the documented positions.
- Develop recruiting requirements/quotas
- Identify recruitment incentives to attract potential cyber warriors
- Recruit personnel with qualifications/potential to learn required skills
- Provide baseline training for specific job/positions skills
- Provide Continuous training via on-line, classroom, or exercises

The DOD is currently working with the Services, Agencies, Joint Staff, and STRATCOM to develop baseline cyber workforce standards. The current model for these standards is the current DOD 8570.01–M "Information Assurance Workforce Improvement Program".

Organizing and equipping the cyber warfare professionals is a function of mission capability requirements defined by the Chairman of Joint Chiefs of Staff and executed by the Services and Agencies.

Mr. THORNBERRY. In your opinion should the cyber warfighter be trained by service branch, jointly, jointly with service specific trailer courses, or somehow else? Why?

Mr. LENTZ. The cyber warfighter should be primarily trained to meet DOD and service level baseline requirements established by the Services under Title 10 authorities. Such training should be augmented by applicable joint specialized training.

Efforts are underway by the Joint Staff to finalize the cyber joint mission task list and to develop a joint learning continuum for cyber training. This should form the basis for joint specialized training.

At both the DOD and joint level, there is a significant emphasis on joint training exercises for the cybersecurity workforce. Exercises are focused on attack detection, diagnosis, and reaction at military speeds.

Mr. THORNBERRY. In the current overseas contingencies, please describe to what extent, if any, has U.S. Strategic Command (USSTRATCOM) taken an active role supporting U.S. Central Command?

Mr. LENTZ. Joint Functional Component Command for Network Warfare (JFCC–NW) and Joint Task Force–Global Network Operations (JTF–GNO), which are two USSTRATCOM components, are actively engaged in support of U.S. forces in the USCENTCOM area of responsibility.

In today's battlefield, our networks are a critical force multiplier. Both JTF–GNO and JFCC–NW work closely with USCENTCOM leaders and staff, in Tampa as well as forward in theater, to ensure vital warfighting networks are robust and defended.

Mr. THORNBERRY. Irrespective of service branch, does USSTRATCOM's cyber warfighters possess the skills necessary to ensure all secure battlefield communications? Please explain.

Mr. LENTZ. Commander, USSTRATCOM met the DOD's 2008 Information Assurance (IA) workforce certification goal to certify 40% of their Information Assurance/Cybersecurity workforce by December 31, 2008. Overall, the Department's information assurance workforce personnel certification rate as of December 31, 2008, was 23% (for its approximately 84,000 IA positions), with a target date of December 31, 2010, for certification of the remaining IA workforce.

Commander, USSTRATCOM has "cyber-warfighters" from a variety of military specialties such as Intelligence, Communications, Information Technology, and Information Assurance with the skills necessary to direct the DOD's Global Information Grid operations and defense. USSTRATCOM provides direction to the Services and organizations to secure their portions of the defense information environment including battlefield communications. The "cyber-warfighter" skill requirements are evolving and DOD is developing the structure, missions, career progression and general responsibilities of the cyber workforce.

Mr. THORNBERRY. How is responsibility between USSTRATCOM, NSA, and DISA clearly defined in theater?

Mr. LENTZ. Joint Functional Component Command for Network Warfare (JFCC–NW) and Joint Task Force–Global Network Operations (JTF–GNO), the two USSTRATCOM components for which I am responsible, maintain a close and collaborative partnership with NSA and DISA. NSA maintains a robust forward pres-

ence in Iraq and Afghanistan to provide both cryptologic and information assurance support to deployed forces. These capabilities support both JFCC–NW and JTF–GNO in their respective missions of providing support for offensive and defensive cyber operations. DISA's mission to build, provision and engineer the backbone of the military networks also serves as a key enabler for JTF–GNO's ability to direct the operations and defense of these networks.

We use liaison officers and support elements embedded within each organization to help ensure our activities are mutually supporting and to avoid conflicting objectives. While each organization has distinct responsibilities, functions and authorities as defined by law and DOD regulations, connective tissue between these organizations is naturally bolstered by the relationships which exist between the Director, DISA dual-hatted as Commander, JTF–GNO, my role as both Director, NSA and Commander, JFCC–NW and since November 08, the relationship established by the SECDEF's decision to place JTF–GNO under the operational control of JFCCNW. It is critical that we continue to maintain and strengthen this connective tissue between our organizations in order to optimize agile cyber support for combatant commanders and DOD as a whole.

Mr. THORNBERRY. Should the Department of Defense establish a "Cyber Agency" at the same level of the National Security Agency (NSA) and Defense Information Services Agency (DISA)? Why or why not?

Mr. LENTZ. Cyberspace is critical to joint military operations, and we must protect it. To do this, the Department of Defense needs to ensure it has the right balance of integrated cyber capabilities. Our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to national security. To effectively address this risk and secure freedom of access in cyberspace, the DOD requires a command possessing the required technical capability and which remains focused on streamlining cyberspace operations. The Secretary of Defense has recently recommended the officer serving as Director of the National Security Agency be nominated as Commander of USCYBERCOM. In his role as the commander of USCYBERCOM, he will report to the Commander of USSTRATCOM.

Mr. THORNBERRY. To what extent is the cyber domain being integrated into other domain and domain awareness initiatives (i.e. battlespace, maritime, air, space)? Please describe.

Mr. LENTZ. The cyber domain is integrated with the other domains and provides supporting capabilities that enable command, control, communications, computing, and information (C4I) processes. The cyber domain is an essential enabler for virtually all functions, including mission operations, information sharing and mission-related data processing.

Domain awareness for the cyber domain is a difficult challenge. At this time, cyber domain awareness capabilities are not completely integrated with domain awareness capabilities for the other operational domains. Cyber domain awareness is routinely included in daily status briefs to commanders, providing a rough awareness of key cyber issues to warfighting commanders. However, cyber operations and incidents are difficult to model and present in visual form, and they are generally not depicted in warfighting common operational pictures.

Mr. THORNBERRY. Define a cyber warfighter, or cyber warfare professional as he exists today.

General ALEXANDER. Cyber professionals are a cross-disciplinary team of highly-trained individuals that bring together diverse skill sets to conduct cyberspace operations. Their mission includes operation and defense of Department of Defense Global Information Grid. Technical expertise and roles cover the span of traditional military planning, intelligence preparation, command and control, operational assessment, requirements development, and operationalization of capabilities; all done in an ever-changing mission space. Cyber warfighters are directly supported by experienced intelligence analysts familiar with the larger cultural and operational contexts, expert language analysts, network analysts, cryptologists and operational planners, to name a few. These experts, be they military or civilian, work together in real time to effectively operate in cyberspace.

Mr. THORNBERRY. Describe what you envision for the cyber warfighter of the future in terms of education (undergraduate/graduate or high school only, too), training, career path, rank structure, capability, mission, responsibilities, organization, etc.

General ALEXANDER. DOD's Cyber force must be continuously educated and mentored, sharpened by experience and drilled to operate in a dynamic environment. I envision a total force solution, active and reserve components, military and civilian, appropriately supported by contractors to build the cyber warfighters of the future. They will arrive with high school diplomas, undergraduate, and graduate de-

grees. Our training and education programs will fill the skill gaps to create increasingly skilled and adaptable personnel who will either specialize in specific cyberspace capabilities or develop broad-based experience to lead and manage future cyberspace operations. Continual specialized training will be necessary because the mission space encompasses an enormous number of different systems and software and is constantly being updated and reconfigured. Mentoring and growing leaders must be done as we do in other specialized fields to ensure experience is distilled to the next generation of planners and operators; a challenge for the nation as well as the military. On the learning continuum, a cyber warfighter will progress from the most basic of tasks through the most complex, by attending formal training, having work assignments that provide the opportunity to perform various missions, and participating in formal education programs.

The Secretary of Defense has directed all the Services to maximize the facility at the Center for Information Dominance in Corry Station, Pensacola (the Executive Agent for Cryptologic Computer Network Exploitation and Defense training) to acquire the technical skills required for cybersecurity missions. (Those with more analytic roles receive their training at Goodfellow Air Force Base.) It is expected that graduates of both programs will be assigned to places where they can practice what they learned, gain mission experience in several sectors of Computer Network Operations, and participate in more advanced training fielded by the Services and the Crytologic Training System.

Specific plans regarding rank structure, responsibilities, and organizations are all under development. The future cyberspace warrior must be adaptive and flexible with the ability to fulfill multiple roles that quickly adjust to changing conditions within the cyberspace domain and the joint warfighter's requirements. Of special importance will be the ability to shift though all missions required for steady state and surge requirements. It is important that individuals be assigned to organizations that are flexible enough to meet the complex challenges of the environment in which they will operate. While a specific organizational construct remains in development, the capabilities should be centered on cyberspace operations that support joint warfighter requirements.

Mr. THORNBERRY. Given the limited pool of individuals with the necessary technical skills, as stated recently by Gen Shelton, and the growing cyber personnel requirements articulated by Secretary Gates, what is the plan to recruit, organize, train, and equip prospective and current cyber warfare professionals? Is it joint or by service? Please explain.

General ALEXANDER. In anticipation of this need, we have been hard at work over the past year identifying the necessary individual technical skills for future cyberspace missions and the training required for those skills.

We currently conduct this training at both Corry Station in Pensacola, Florida and Fort Meade, Maryland and are working through resource requirements to meet future demand for trained and ready cyberspace forces.

While we were developing training, we've also worked closely with the Services and national community to determine future force number requirements for the Department that included initial estimates for the expected end strength in a "total force" approach.

We envision that the future cyberspace forces will be a total force approach of both Service and joint—the Services will organize, train, and equip cyberspace forces that will be presented to joint warfighters. Additionally, there will be a joint force that provides day-to-day support to USCYBERCOM missions as directed by Commander, USSTRATCOM. Using common force training and skills baseline, the services will generate forces that will rotate back and forth between the joint community and Service unit assignments.

We must also leverage the unique contributions of universities and research institutions as well as private enterprise to ensure U.S. forces are always on the cutting edge.

Mr. THORNBERRY. In your opinion should the cyber warfighter be trained by service branch, jointly, jointly with service specific trailer courses, or somehow else? Why?

General ALEXANDER. There is clearly a need for Service and Joint training for the cyber warfighter as well as more robust leveraging of the scientific and technical expertise found in our universities, research institutions and private enterprise. The complex and dynamic nature of the operational environment should dissuade us from adopting a one-size-fits-all approach. As in other military disciplines, we must train individuals with the basic skills they will need to operate and adapt in this domain: technology, analytics, cryptanalysis, languages, intelligence, operational planning and effective command and control. The Services play an enormous role here. There is a great deal of work being done by the Services to determine how

they can best organize, train and equip forces for the combatant commanders. The Services, of course, also need much of this same expertise to effectively operate, secure and defend their networks and communication systems.

Joint training is also critical; we must train how we fight. Part of the reason Secretary Perry first created the Joint Task Force–Computer Defense Network in the late 1990s was because he realized then, as we do now, that unity of command and unity of effort is as essential in cyberspace as it is in the physical domains of air, sea, land and space. All we have learned in the intervening years led Secretary Gates to direct the creation of U.S. Cyber Command. It is only by focusing the talent and resources of the Services and forging and training Joint teams with interoperable equipment and unifying doctrine that we will be as effective in this domain as we are in the physical domains.

Mr. THORNBERRY. In the current overseas contingencies, please describe to what extent, if any, has U.S. Strategic Command (USSTRATCOM) taken an active role supporting U.S. Central Command?

General ALEXANDER. Joint Functional Component Command for Network Warfare (JFCC–NW) and Joint Task Force–Global Network Operations (JTF–GNO), the two USSSTRATCOM components for which I am responsible, are actively engaged in support of U.S. forces in the USCENTCOM area of responsibility.

In today's battlefield, our networks are a critical force multiplier. Both JTF–GNO and JFCC–NW work closely with USCENTCOM leaders and staff, in Tampa as well as forward in theater, to ensure vital warfighting networks are robust and defended. We also plan, synchronize and execute cyberspace operations to deny a widely disbursed adversary the ability to easily use the Internet to orchestrate complex operations that target our forces, friends and allies. Of course, these commands also engage in deliberate planning in support of other long-term USCENTCOM priorities.

The bright, energetic people assigned to these organizations are committed to this mission. They work to build the relationships with USCENTCOM that are so vital to the kinds of sophisticated, synchronized operations conducted by U.S. forces and Coalition partners. We must build the same kind of robust relationship with the other Combatant Commanders and ensure our operational planning and activities are well integrated with the other global missions for which USSTRATCOM is responsible.

Mr. THORNBERRY. Irrespective of service branch, does USSTRATCOM's cyber warfighters possess the skills necessary to ensure all secure battlefield communications? Please explain.

General ALEXANDER. Let me begin by saying that no commander can guarantee battlefield communications will always get through or that they won't be intercepted by an adversary. The military, by definition, must be able to operate in a degraded environment. Yet, it is imperative that we ensure availability and security of communications. The Department of Defense has come a long way since the President first assigned U.S. Strategic Command the mission to defend DOD networks in 2002. In Joint Task Force–Global Network Operations and Joint Functional Component Command for Network Warfare, U.S. Strategic Command has highly-motivated, well-trained personnel engaged in the 24/7/365 defense of our vital networks. But we must do more.

Over the years, the Secretary of Defense has provided U.S. Strategic Command with the authority to direct the operations and defense of defense networks, known as the "Global Information Grid" or "GIG." We have established command and control that begins to enable the coordinated security configuration and defense of globally dispersed military networks. We also established baseline standards for network configuration, readiness standards and incident response. Service and Joint training are based on these collaboratively developed standards.

However, even with well-trained and engaged personnel, the challenges are great. The Internet's open architecture is one of its principal strengths, but it is also its principal vulnerability. To defend national interests, DOD's GIG must be reliable, resilient and its individual components and date must be secured. We must be able to operate at "network speed" to be effective. Without greater machine-to-machine interfaces, we cannot hope to dynamically configure systems to contain and defeat the threat of malicious traffic on a real-time basis—a necessity in this era's battlefield environments. Achieving much greater unity of effort throughout the Department as well as information sharing and collaboration with our Intelligence Community, Law Enforcement and Homeland Security partners as well as leveraging the expertise of universities, research institutions and private enterprise is also essential. We must continue to evolve training and operational exercises to ensure all personnel can appropriately and quickly leverage the diverse skill-sets needed to secure and defend military networks in this dynamic domain.

Mr. THORNBERRY. How is responsibility between USSTRATCOM, NSA, and DISA clearly defined in theater?

General ALEXANDER. Joint Functional Component Command for Network Warfare (JFCC–NW) and Joint Task Force–Global Network Operations (JTF–GNO), the two USSTRATCOM components for which I am responsible, maintain a close and collaborative partnership with NSA and DISA. NSA maintains a robust forward presence in Iraq and Afghanistan to provide both cryptologic and information assurance support to deployed forces. These capabilities support both JFCC–NW and JTF–GNO in their respective missions of providing support for offensive and defensive cyber operations. DISA's mission to build, provision and engineer the backbone of the military networks also serves as a key enabler for JTF–GNO's ability to direct the operations and defense of these networks.

We use liaison officers and support elements embedded within each organization to help ensure our activities are mutually supporting and to avoid conflicting objectives. While each organization has distinct responsibilities, functions and authorities as defined by law and DOD regulations, connective tissue between these organizations is naturally bolstered by the relationships which exist between the Director, DISA dual-hatted as Commander, JTF–GNO, my role as both Director, NSA and Commander, JFCC–NW and since November 08, the relationship established by the SECDEF's decision to place JTF–GNO under the operational control of JFCC–NW. It is critical that we continue to maintain and strengthen this connective tissue between our organizations in order to optimize agile cyber support for combatant commanders and DOD as a whole.

Mr. THORNBERRY. Should the Department of Defense establish a "Cyber Agency" at the same level of the National Security Agency (NSA) and Defense Information Services Agency (DISA)? Why or why not?

General ALEXANDER. On 23 June 2009, Secretary of Defense Gates directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish a subunified U.S. Cyber Command (USCYBERCOM). Since that time, a STRATCOM-chartered CYBERCOM Implementation Team, with membership from NSA, DISA, JFCC–NW and JTF–GNO, have been working to produce a plan which would outline the mission and operating framework for this command. Both DISA and NSA will play critical roles in the Command's ability to successfully operate and defend our military networks.

Mr. THORNBERRY. To what extent is the cyber domain being integrated into other domain and domain awareness initiatives (i.e. battlespace, maritime, air, space)? Please describe.

General ALEXANDER. Cyberspace operations are being integrated with operations in other domains through a myriad of efforts. These include developing joint doctrine to inform warfighters of extant capabilities, tactics, techniques, and procedures; developing cyber force constructs and associated training; integrating cyberspace operations within joint force exercises; ensuring cyberspace operations are included in combatant command plans; and developing initiatives which inform cyber users by examining culture, conduct, and capabilities. Although still in initial stages, initiatives to provide decision-makers with holistic views of the cyberspace domain, similar to the Maritime Awareness Initiative, are being addressed. Much remains to be done; however, the increasing national focus on cybersecurity is encouraging and will provide impetus to DOD and interagency efforts to increase awareness of this critical domain.

QUESTIONS SUBMITTED BY MR. MURPHY

Mr. MURPHY. We have heard a lot about how our government's resources are organized to address the threat posed by cyber hackers, but if we want to direct our efforts most effectively, it's also important to know how the hacker community is organized. What do we know about the culture of hackers, what motivates their actions, and what political, economic and social forces shape their behavior? It would seem that the answers to these questions should inform some of our decisions on how best to organize ourselves.

General Alexander, I understand that a small office at the NSA—the Institute for Analysis—has done some innovative work to address these questions about the culture of hackers. Can you briefly describe, in an unclassified manner, this work and how it is contributing to our cyber security efforts?

General ALEXANDER.

Background

The **Institute for Analysis (IFA)** is an NSA-sponsored program launched in October 2004 with the intent of 1) reaching out to and engaging external world-class

experts in addressing internal intelligence analytic problems in an unclassified setting and 2) learning from and applying new or unique analytic processes, methodologies, techniques, and associated tools developed in the "real world" to improve the overall health of analytic tradecraft at NSA. The primary vehicle used by the IFA is a "challenge problem" which is essentially an unclassified "analog" problem that stands in for/represents the actual classified analytic problem identified by mission elements. IFA also facilitates networking between external experts and analysts and also develops and offers new analytic methodology training courses to analysts. Since 2008, IFA has been able to increasingly share these opportunities with other Intelligence Community partners.

The Challenge

In early 2008, an analyst from the NSA/VCSS Threat Operations Center (NTOC) brought the issue of understanding hacker cultures to the IFA as a potential challenge problem. The analyst understood that hacker scenes evolve and continue to evolve. In an effort to best focus his time and resources, the analyst wanted to know if there was a way to better understand the culture of hacker groups and therefore better understand the potential for a group of hackers to pose a significant national security threat. Specifically, he wanted to know the answers to the following questions:

- *What motivates hackers?*
- *How do they learn, team up, and execute attacks?*
- *How do their strategies and operations differ from country to country?*

NTOC analysts have a solid understanding of the technical elements associated with hacking, but they wanted to know more about the sociological and "cultural" aspects. The challenge therefore was to strengthen analysts' understandings of the human side of hacking: what motivates hackers; where do they go to learn new techniques; how do they find out about new technologies; what self-identified hacker communities have emerged; and finally, what the relationship was, if any, between relatively benign "tinkering networks" and truly malicious hackers?

What makes this a difficult problem was that virtually all hacker scenes are animated by a culture of secrecy and anonymity. Many hackers, and especially those who are likely to be of most interest to the USG, do not wish to have their activities and habits documented.

Project Scope

There were three specific goals built into this challenge question, as follows:

1) Systematically identify subcultures within the global hacker scene, and the key traits that distinguish them from other hacker subcultures, with a focus on teaming/interaction, learning, technology use, and motivations with the intent of developing the ability to "strategically segment" these subcultures to identify other hackers of potential interest;
2) Identify how these scenes vary from region to region (or along other lines, e.g., by generation, motivation, etc.) with potential concentrations on Russia, China, and/or the Middle East. This would allow analysts to differentiate the threat matrix by region or other factors;
3) Research and analyze how these scenes have changed over the past decade and may continue to change going forward. This will enable analysts to better anticipate strategic or tactical surprises that may emerge from the hacker scene.

Two substantive limits were also identified, as follows:

1) This project focused on the culture of hackers and the hacking scene, not on the wider issue of cybercrime, writ large. That is to say, the analysts were interested in understanding the habits of those who like to break into secured computer systems, whatever their motives, rather than on criminality which just happens to take place on or via the Internet. Clearly criminals of one sort and another may well adopt innovations and techniques that emerge from the hacker scene for their own purposes but that was not the main focus of the challenge problem;
2) Open source research would focus on the dimensions of the hacking scene that are *most* pertinent to national security: penetration of government systems, disruption of critical infrastructure, significant intellectual property theft, etc. This scoping excluded, for example, spambots, the hacking of consumer electronics, defacement of websites, etc., except insofar as such activities connected in some tangible way to national security.

Challenge Results

Specific results of this challenge problem provided detailed descriptions of hacker cultures in two areas of interest to NTOC as well as a framework that allowed

NTOC analysts to rapidly identify, characterize, and categorize hacking activities based on potential threats to national security. The framework in particular has already been integrated into NTOC operations and has resulted in a quantitative increase in reporting on adversarial capabilities, including capabilities previously undiscovered using more conventional techniques. According to NTIOC management, this framework has also resulted in a significant savings of time, measured in man-*years,* in the "discovery" process.

○