[H.A.S.C. No. 112–146]

# DIGITAL WARRIORS: IMPROVING MILITARY CAPABILITIES FOR CYBER OPERATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

HEARING HELD
JULY 25, 2012

U.S. GOVERNMENT PRINTING OFFICE
75–668 WASHINGTON : 2013

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

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MAC THORNBERRY, Texas, *Chairman*

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

JAMES R. LANGEVIN, Rhode Island
LORETTA SANCHEZ, California
ROBERT ANDREWS, New Jersey
SUSAN A. DAVIS, California
TIM RYAN, Ohio
HANK JOHNSON, Georgia
KATHLEEN C. HOCHUL, New York
RON BARBER, Arizona

KEVIN GATES, *Professional Staff Member*
MARK LEWIS, *Professional Staff Member*
JAMES MAZOL, *Staff Assistant*

# CONTENTS

## CHRONOLOGICAL LIST OF HEARINGS

2012



**WEDNESDAY, JULY 25, 2012**

**DIGITAL WARRIORS: IMPROVING MILITARY CAPABILITIES FOR CYBER OPERATIONS**

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS



WITNESSES



APPENDIX

# DIGITAL WARRIORS: IMPROVING MILITARY CAPABILITIES FOR CYBER OPERATIONS

---

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
*Washington, DC, Wednesday, July 25, 2012.*

The subcommittee met, pursuant to call, at 3:35 p.m. in room 2119, Rayburn House Office Building, Hon. Mac Thornberry (chairman of the subcommittee) presiding.

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

Mr. THORNBERRY. The subcommittee will come to order.

We welcome our witnesses, guests, and members to this hearing in the Emerging Threats and Capabilities Subcommittee on "Digital Warriors: Improving Military Capabilities in the Cyber Domain."

There is widespread agreement that cyberspace is now a domain of warfare, and many people regard it as the most difficult, perplexing national security challenge we face. Certainly the laws, policies, and organizations have not kept pace with the evolution of technology. But if cyberspace is important to our country's security and if it is a domain of warfare, our military services, on whom we rely to protect and defend us, must be prepared to operate in cyberspace as well. That preparation involves a number of issues, including organizational structure, recruitment and retention of qualified personnel, training, rapid acquisition, among others; and it is those issues which we want to examine in today's hearing.

Before turning to our witnesses, let me yield to the ranking member, Mr. Langevin, for any comments he would like to make.

[The prepared statement of Mr. Thornberry can be found in the Appendix on page 37.]

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

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses for appearing here today. It is a pleasure to see all of you again and to have you join us for what I believe is going to be a critically important hearing.

I agree with the chairman. There is no more critical task in today's environment than safeguarding the Department of Defense's networks. The cyber domain, as we all know, has become an integral part of every action DOD [Department of Defense] undertakes,

whether offensive or defensive. And as operating environments grow ever more complex, we need joint forces that are manned, trained, and equipped to conduct the full spectrum of operations in support of, and in some cases supported by, what we think of as traditional military forces.

The Congress and the country as a whole have been struggling with what cybersecurity means to us as a Nation. We are grappling with how to protect our systems and our privacy at the same time, and I am proud to be a part of that robust discussion. I have held drafts of legislation and cosponsored others, and now it looks as if something actually may be moving over in the Senate, which I am pleased to hear. Let's hope so.

And I hope that today we will hear your thoughts on what sorts of additional authorities you may need and how the proposed legislation may or may not affect those needs, as well as your thoughts on the delegation of authorities within the executive branch. Most importantly, I hope that we hear about how you are finding and retaining the sort of people that you need today and in the future and being able to hold onto them.

This, I believe, is the fundamental challenge that faces all of us. It is often said that the root strength of our military is the quality of our people, and nowhere is that more true than in your organizations.

As you think about growing your forces, what thought have you given to where the people are going to come from? How will you keep them, promote them, educate them, and continue to challenge them even when outside organizations are keen to lure people with those skill sets away to the private sector? And I know some of you are probably already facing that dilemma right now.

So, lastly, I need to take a minute to talk about a topic that would be irresponsible to avoid. We all know that we are facing significant fiscal challenges in the coming years, even without the threat of sequestration looming. So cyber-related activities are faring reasonably well so far, but nothing is immune, and even noncyber-specific cuts could have an impact on your commands as personnel resources are reduced or research and development funding are decreased. Those are just two examples.

So as you look ahead, how do you factor in the possibility of even more austere fiscal environments? This is a tough question but one that I believe we have to face in order to responsibly address the complex challenges in the future.

So, with that, I want to thank you again for being here.

Mr. Chairman, thank you for holding this hearing. I know your commitment to the issue of cybersecurity. And I enjoy working with you and appreciate your organizing this hearing today.

I yield back.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 38.]

Mr. THORNBERRY. I thank the gentleman, and I share his cautious optimism that the Senate may actually pass something. We will see.

Again, let me welcome our witnesses. We have before us Lieutenant General Rhett Hernandez, Commander, U.S. Army Cyber Command; Vice Admiral Michael S. Rogers, Commander, U.S. Fleet

Cyber Command, and Commander, U.S. Tenth Fleet—I made that as hard as possible to say—Lieutenant General Richard P. Mills, Deputy Commandant, Combat Development and Integration, and Commanding General, U.S. Marine Corps Combat Development Command; and Major General Suzanne Vautrinot, Commander, 24th Air Force, and Commander, Air Force Network Operations.

You all have significant titles. I suspect the responsibility and the challenge is commensurate with the length of the titles.

Thank you for being here. Without objection, your full written testimony will be made a part of the record. We would appreciate if you can summarize your comments for us today.

General Hernandez.

**STATEMENT OF LTG RHETT A. HERNANDEZ, USA, COMMANDER, U.S. ARMY CYBER COMMAND, U.S. ARMY**

General HERNANDEZ. Thank you, Congressman.

Chairman Thornberry, Ranking Member Langevin, and distinguished members of the subcommittee, thank you for your support and for the opportunity to appear before you today. I am pleased to be here with my fellow Service component commanders, and I am honored to represent the Army soldiers and civilians. Their great work enables our Army's ability to operate every day and adds to our Nation's security. I am proud to serve with them and really amazed at what they have accomplished since October 2010.

The Command has been hard at work increasing Army capacity and capability, defending all Army networks, and conducting cyberspace operations in support of U.S. Cyber Command. We all know the cyber threats are real, growing, sophisticated, and evolving. Today, a wide range of actors are capable of exploitation and disruption of our networks, with a growing potential for destructive capabilities tomorrow. And all of this could impact our freedom to operate.

To meet these threats, Army Cyber Command and its supporting units are engaged daily in conducting cyberspace operations critical to the Department of Defense, Cyber Command, and Army missions. Our work is guided by the Department of Defense's strategy for operating in cyberspace; and the Command helps prevent conflict by maintaining credibility based on capacity, readiness, and modernization. It helps shape the environment by sustaining strong relationships with our military allies in other nations and builds their capacity and capability and, when required, supports winning decisively, with the Army's operational level force organized to conduct cyberspace operations, and daily we provide trained and ready forces to Cyber Command in support of their mission.

We have completed a wide range of work and continue to pursue other initiatives to train, organize, and equip the Army to conduct operations in cyberspace. Strong training, leader development, and education programs are essential to conducting cyberspace operations. We have established a world-class, cyber-opposing force that provides realistic training, requiring commanders to defend and operate in a contested and degraded cyberspace environment.

We continue to deploy dedicated information operations and cyberspace capabilities to Army and joint forces, and we are sup-

porting combatant command cyber support elements, while providing expeditionary cyber support elements to commanders for contingencies and during exercises.

A significant organizational milestone occurred for the Command on 1 December, 2011, when the Army activated its first dedicated cyber brigade at Fort Meade. The 780th Military Intelligence Brigade is organized to support Cyber Command and combatant commanders in their conduct of cyberspace operations.

The Army has a wide range of capabilities being leveraged today to operate and defend as well as support offensive operations. We continue to respond to Cyber Command and combatant commanders' requirements and have rapidly produced capabilities to support missions.

While technology plays an important role in the cyberspace domain, cyber warriors will determine our success. A team of cyberspace professionals able to quickly act across a full range of mission sets is who will make the difference. We must continue to recruit, develop, and retain a skilled professional workforce.

While there is still plenty to do in this new domain, Army Cyber Command has made great progress and remains focused on providing trained and ready forces able to conduct cyberspace operations. We will provide depth and versatility in cyberspace to the Joint Force and with our cyberspace capability provide options and flexibility for commanders and national decisionmakers to ensure the Army remains America's force of decisive action and that Army Cyber Command remains second to none.

I want to thank you for inviting me here today. I look forward to your questions and our continued relationship and would welcome your visit to Army Cyber Command. Thank you.

[The prepared statement of General Hernandez can be found in the Appendix on page 40.]

Mr. THORNBERRY. Thank you.

Admiral.

**STATEMENT OF VADM MICHAEL S. ROGERS, USN, COMMANDER, U.S. FLEET CYBER COMMAND, AND COMMANDER, U.S. TENTH FLEET, U.S. NAVY**

Admiral ROGERS. Thank you.

Chairman Thornberry, Ranking Member Langevin, and distinguished members of the subcommittee, thank you for holding this hearing today and the opportunity to sit shoulder to shoulder with my cyber teammates in the other Services.

As the Navy's Component Commander to U.S. Cyber Command and the second echelon command within the Navy subordinate to the Chief of Naval Operations, Fleet Cyber Command directs cyberspace operations in defense and support of Navy and joint forces. The Department and the Navy continue to mature cyberspace operations by growing the workforce, exercising the processes, and developing the capabilities we need to support cyber operations. Our progress has been, and will continue to be, guided by the Department's overall strategy for operating in cyberspace; and I would like to take this opportunity to highlight a few items that I think highlight some of the progress as well as some of the challenges we have experienced in the last year.

That progress has been an iterative one, and we continue to refine concepts and doctrine, but there are two significant achievements I think in the last year that will help us as we move our efforts forward.

First, the approval and implementation of the Transitional Command and Control Concept of Operations, which provides the Services and the Geographic Combatant Commanders a standard baseline for how we are going to execute cyberspace operations by documenting the command and control relationships, the missions, and the functions that we will be executing.

Secondly, U.S. Cyber Command's Operational Directive, which specifies the standard tasks and mission responsibilities for each of the Service components before you today, which will provide initial insight into how U.S. Cyber Command intends to use us as components, which in turn will provide a foundation for how we will generate Navy capacity to support them.

In addition, the strength of our efforts over the last year have been from our workforce, which continues to be a source of strength. And, at the same time, the events of the last week remind us just how great that workforce is.

Unfortunately, Fleet Cyber Command and Tenth Fleet suffered the loss of a petty officer in Aurora, Colorado, on Friday in a movie theater in a way that none of us would have ever expected. I had the opportunity to see Petty Officer Larimer's family in Chicago over the weekend after the tragedy, and I will tell you if we had more Petty Officer Larimers in the world, there is no challenge that we couldn't handle. But he is symbolic of the broader workforce that we have.

And, to date, our recruitment, our development, and our retention, although it remains a challenge, has in fact exceeded our expectations. We hope that is what continues, and we are working hard to make sure that is the case.

We also have taken a hard look over the last year about how we are going to train the force of the future, establishing summer internships with the Naval Academy and ROTC [Reserve Officers' Training Corps] midshipmen with the Navy Cyber Warfare Development Group, as well as our cyber defensive operations.

In addition, we have established a cyber warfare engineer career field designed to enable direct accessions from recent college graduates who bring deep cyber expertise to the table.

In addition, to develop our sailors and civilians, we have developed and begun implementing a tiered cyber training strategy that tailors cyber training based on an individual's particular roles and responsibilities.

We have also created a Navy Cyber Manpower 2020 Task Force to plan and execute the steps necessary, we believe, that will develop a comprehensive near to midterm cyber manpower strategy.

We have also worked hard in the last year to strengthen our networks and to reduce our exposure and our vulnerabilities, and those efforts continue. We emphasize cross-communication between our large network programs, both afloat and ashore; and we are actively engaged in developing concepts with the Department of a joint information environment which will be comprised of information technology infrastructure and enterprise services. These in-

vestments that we have made in network consolidation and deployment of enterprise services have already provided us with greater situational awareness of our networks, which is a key element of our ability to defend them.

In summary, sir, I would like to close by emphasizing that our success to date in the maritime domain and the joint operational environment depends on our ability to maintain freedom of maneuver and deliver effects within cyberspace. And to ensure we maintain our edge, the Navy will continue to drive advancements in Navy cyberspace operations guided by the initiatives set forth both by the Department and the joint commander we support at U.S. Cyber Command.

I thank you for this opportunity, and I look forward to answering any questions you might have. Thank you, sir.

[The prepared statement of Admiral Rogers can be found in the Appendix on page 51.]

Mr. THORNBERRY. Thank you.

General.

**STATEMENT OF LTGEN RICHARD P. MILLS, USMC, DEPUTY COMMANDANT, COMBAT DEVELOPMENT AND INTEGRATION, AND COMMANDING GENERAL, USMC COMBAT DEVELOPMENT COMMAND, U.S. MARINE CORPS**

General MILLS. Chairman Thornberry, Ranking Member Langevin, Congressman Conaway, it is an honor to appear before you today. On behalf of all the marines and their families, I want to thank each of you for what you do and your continued support in all things military.

I will keep my comments short, as my written statement has been made a part of the official record.

Protecting cyberspace is a national security priority. Your Marine Corps understands that and recognizes that fact. Indeed, while Marine Forces Cyber Command is just 3 years old, Marines have been conducting cyber operations for well over a decade. We clearly understand that cyberspace, the convergence of network systems brought about by so many disciplines, is absolutely integral to our everyday lives, our national well-being, and has become a key aspect of today's warfighting. Around the world, and particularly in the United States, cyberspace is part of all that we do. Smartphones and social media, to efficiencies throughout our vast critical infrastructure, it all depends on the grid.

Yet with all these positive advances come risks and vulnerabilities. We know that Department of Defense systems are attacked millions of times each day. Indeed, the Marine Corps Enterprise Network is also attacked hundreds of thousands of times each day. The critical infrastructure in the United States is highly vulnerable to cyber attack.

As the Nation's expeditionary force in readiness, the Marine Corps is preparing to meet these threats by increasing capacity for network operations, by increasing our ability to conduct defensive cyber operations, and, when directed, to conduct offensive cyber operations. Ensuring the stable cyber domain means that we will ensure our stability of our weapons systems, our command and control systems, and indeed our national industrial assets.

Today's dynamic global environment demands that the maritime forces be flexible and scalable, thus allowing operational commanders the ability to configure the sea base to optimize the employment of appropriate size and capable forces to accomplish a mission, whatever that mission may be, from humanitarian assistance to major combat operations. Therefore, our cyber operations must be tailored to provide flexibility to the Marine Corps, to the Joint Force, and indeed to the Nation. We need to meet emerging missions, enhancing the requirements to support distributed operations today.

Since my predecessor, Lieutenant General George Flynn, testified before this committee some 2 years ago, the Marine Corps has made great strides in expanding the capability and capacity of Marine Forces Cyber Command. We have increased its workforce as well as our cyber-related Military Occupational Specialties. In the future, we plan to increase our cyber workforce by approximately 700 marines and civilian marines through fiscal year 2016. I am very proud of our cyber marines and our civilian marines. They work diligently every day to defend and protect our cyber domain.

In addition to the progress we have made in developing our cyber workforce, we have made great strides in securing our network architecture. The Marine Corps has already standardized its security boundary architecture through its implementation of the Marine Corps Enterprise Network, and we are working with the Joint Information Environment framework to comply with developing shared security architectural standards. Indeed, as we assume full control over our network transport and enterprise services, we will collapse our remaining legacy networks, which will then reduce our management footprint and our costs, while achieving greater compliance and consistency, again throughout the Marine Corps Enterprise Network.

We are taking a very deliberate and joint approach to cyber requirements. We continually strive for the right balance in supporting the requirements of both U.S. Cyber Command and our own Service requirements.

Gentlemen, I appreciate the opportunity to discuss this important project, and I look forward to our questions.

Thank you.

[The prepared statement of General Mills can be found in the Appendix on page 62.]

Mr. THORNBERRY. Thank you.

General.

**STATEMENT OF MAJ GEN SUZANNE M. VAUTRINOT, USAF, COMMANDER, 24TH AIR FORCE, AND COMMANDER, AIR FORCE NETWORK OPERATIONS, U.S. AIR FORCE**

General VAUTRINOT. General Thornberry, Ranking Member Langevin, Congressman Conaway, and distinguished members of the subcommittee, thank you for the opportunity to represent the exceptional men and women of Air Forces Cyber before this panel. It is an honor to appear before you alongside my Service counterparts and to share our progress in responding to U.S. Cyber Command and our Nation's mission requirements.

In Air Forces Cyber, through continued support from General Shelton at Air Force Space Command and General Alexander at U.S. Cyber Command, we have made great strides towards normalizing and operationalizing cyber capabilities to match the rigor and discipline of its air and space counterparts. I have been privileged to witness firsthand cyber airmen fulfilling our commitment, the commitment we pledged to you 2 years ago, to provide global vigilance, reach, and power by doing what airmen do best, innovate. This culture of innovation is foundational and has been vital to overcoming the myriad of challenges associated with conducting cyber missions. I would like to share a few examples of this culture in action.

In addition to the remotely piloted aircraft mission assurance, which I described in my written remarks, we have also collaborated with U.S. Transportation Command and employed our specialized U.S. cyber teams to search within the .mil networks to assure the mission by proactively discovering vulnerabilities before they can be exploited. General Fraser's Command worked with our teams inside the tanker airlift control center to initially map that mission network to the architecture. Then, in phase two, the operators proactively searched for the network and leveraged capabilities to identify, pursue, and mitigate threats impacting the critical system interfaces that are essential to mission success, an activity in the military which we seek to support in defense of the Nation.

For mission assurance, a combatant command's prioritized defended asset list determines where this focused capability will be employed, in effect, the cyber high ground. These teams are operational and have been deployed to protect against adversaries' actions per Cyber Command tasking.

Mission capabilities and applications are critical, but increasing the capacity to expand those capabilities in support of joint operators is just as important. I recently attended a graduation ceremony at Hurlburt Field, Florida, where our Intermediate Network Warfare Training course, which is our schoolhouse for a wide range of cyber operators and one of ten in-residence and seven online courses, graduating over 7,000 students a year. As a result of this course, young cyber warriors like Lieutenants Andrew Cook and Stephanie Stanford are now experts in their field and carry unique certifications that only 6,800 people in the world have attained.

Operationalizing cyber training and certification, our commitment 2 years ago, a reality today. Likewise, high school and college students around the country have been exposed to science, technology, engineering, and mathematics through successful programs such as Cyber Foundations, the Air Force Association's CyberPatriot initiative, as well as the National Collegiate Cyber Defense Competition. These programs have been truly groundbreaking in that they get our next generation of cyber professionals excited about and committed to a cyber career. These professionals are key to U.S. Cyber Command's mission and the Nation's defense.

We grieve the loss of one of those cyber warriors, Staff Sergeant Jesse Childress, in the Aurora shooting; and we join our sister Service, Fleet Cyber, in grieving the loss of Petty Officer Larimer. We are grateful for their service.

Having new capabilities and expanding capacity, along with academic, industrial, interagency, and international collaboration is what will move this Nation forward and make Jesse and John proud.

Air Forces Cyber has improved our collaboration with our sister Services, other government agencies, academic and industry partners to share situational awareness and increase capabilities and capacity, which is the first essential step towards transitioning to a more predictive and proactive defense. From across the Air Force, we have synchronized materiel command acquisition and engineering professionals, research lab and test specialists, and 24th Air Force's real-time cyber development expertise to establish a Center for Cyber Innovation in Texas, with a goal of rapidly fielding critical cyber capabilities.

General Alexander lists this capability as a top priority in his May 2012, Operations Directive, and it was something you requested in section 933 of last year's National Defense Authorization Act. As a result, Air Forces Cyber executes U.S. Cyber Command mission guidance by effectively supporting every combatant command, providing full spectrum cyber operations.

I am extremely proud to play a part, as our airmen play, in defending the Nation in cyberspace at the speed of cyber. For me as an airman, that is Mach 880,000. Offensive, defensive, and enterprise services are inextricably connected in this domain. We all rely on cyber to be there. We have a personal interest, a corporate interest, and a national security interest in making sure it remains available for all our use, while denying our adversaries' ability to use it against us. We have made great advances and will continue do so. That is our innovative culture as airmen, our obligation to General Alexander.

Thank you for your continued support for this vital mission, and I look forward to answering your questions.

[The prepared statement of General Vautrinot can be found in the Appendix on page 69.]

Mr. THORNBERRY. Thank you, and I appreciate all of your statements.

And I particularly appreciate, General, you and the Admiral mentioning the loss in Colorado. It is a specific reminder to us all about the tremendous potential of those lives that were tragically cut short by that event.

Let me just ask one question and then yield to my colleagues for their questions.

The ranking member mentioned sequestration. Obviously, it is near the top of our minds in all we do in this committee and around Congress. If there were to be sequestration, you know, just say on the order of 10 percent, what would that mean for the programs that you are responsible for?

If we could just go down the line briefly.

General Hernandez.

General HERNANDEZ. Congressman, thank you.

Clearly, with sequestration no part of the Army would go untouched. So we are not planning for it. And I would say, to Congressman Langevin's point, if we were to invest in areas that had to stay for us, it would have to be the people. We have all talked

about the significance of the workforce and training, recruiting, developing, retaining that workforce.

And the second piece would be that we ensure that we invest in the right S&T [Science and Technology] that allows us to really capture the requirements for the future in this domain.

Mr. THORNBERRY. I am sorry—10 to 15 percent in the first year alone. Obviously, if sequestration—we are talking about that year after year after year. And, you know, again, I am just kind of thinking about the first year.

Go ahead.

Admiral ROGERS. Well, I believe we are all in the same boat in the sense that the Department has done no planning or provided no guidance; and under the terms of the sequestration, it would be implemented across the Federal Government.

I think my concern as a commander, not having delved into the specifics, is if we lose the ability to prioritize, if we are going to take cuts that are just done indiscriminately—and I don't mean that to be pejorative—but if we are going to take cuts indiscriminately across the board, as an operational commander, if we lose the ability to prioritize, if we lose the ability to attempt to identify what are the core capabilities that we want to make sure that we continue to fund at consistent levels, that concerns me.

Mr. THORNBERRY. Well, that is the way it is. It is every program, project, activity cut in an equal amount. So what we are trying to get is, okay, what does that mean for cyber, an area that is so dynamic, that, as Mr. Langevin said, has actually been growing in recent years?

General.

General MILLS. Sir, again, the impact across the Marine Corps would be significant in readiness, in manning levels, and in our ability to train and to exercise our forces. I think probably the impact on Marine Forces Cyber and probably all cyber programs would be disproportionate because of the speed with which we have to acquire new equipment and new software. So I see it as having a significant impact across the board and I think a disproportionate impact within the world of cyber.

General VAUTRINOT. Chairman Thornberry, it would be devastating. The strategy that has been provided by the Department to move us forward in cyberspace and the vision provided by General Alexander rests on future acquisitions, on future changes; and I believe that under sequestration those would not be realized.

In addition, those advancements that we have made over the last years, as each of our commands stood up, requires sustainment; and those sustainment levels have not been created and stabilized. And so, as we back away from those, I believe that we would actually lose ground in this important area and in meeting the strategic goals that the Department has outlined and in particular my Service has put into its master plan.

Mr. THORNBERRY. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Thank you again to our witnesses for your testimony today and thank you for mentioning the losses in Colorado. Like the chairman said, it is important for us to be mindful of their service and the

loss that we have experienced in Colorado, and our thoughts and prayers are with them and their families.

I appreciate you addressing the issue of sequestrations.

I can move onto another area. Talking about cyber operators, can you tell me for each of you how many cyber operators do each of you have? How many more do you need? And where will you get them from? And how will you recruit and retain them?

The issue of retention is going to be a big challenge going forward, as identified. I know the private sector is always looking to recruit from the military and to retain them. So we have got a challenge on our hands to retain them.

How many do you have? And if you need to get back to us for the record, that is fine. But if you do happen to have those numbers, that would be helpful.

General, should we just start with you and go right down the line?

General HERNANDEZ. Congressman, let me start with a larger number that we believe are engaged in conducting the full range of cyberspace operations every day, which runs the three lines of operation consistent with Cyber Command for operate, defend, and offense. Of those organizations that are either assigned or under the operational control of Army Cyber at this point, we have about 11,000. Of that number, the predominant number is focused every day on operating and defending our network.

The standing up of the cyber brigade really is the brigade that brings the capability to conduct SIGINT [Signals Intelligence] operations, defensive operations, and, when ready, capable of conducting offensive operations. That brigade will be about 1,200 when we are done training that brigade. Because it is a long investment in training for that skill set, and I don't know what the total requirement is yet. I think that is really a part of the larger requirement with respect to how we are going to operate in cyberspace, what the roles and responsibilities will be. But we I think have a pretty good head start in that. Now it is a matter of how we leverage the skills that we have and retain those skills to do the missions that we have been assigned.

Mr. LANGEVIN. Have you thought about, too, about the retention aspect of it? Clearly, if people know that these are promotable skills and we can move them up the chain, they can have a place within your—they are in for the long haul, they are more likely to stay.

General HERNANDEZ. I think we have learned some really significant lessons as we recruited this cyber brigade. And we did a lot of things that were important in recruiting that are tied to how you assess, how you provide the right incentives to bring them in, through questionnaires, through interviews, through specific targeting of universities and different programs that we try to bring the skill set that not only had a desire to do this but they had a propensity for this hard work. And through a combination of bonuses and incentives, we are doing pretty good in bringing them in.

I think our most significant piece that we are learning is that the pool is not very deep, as you talked about earlier, and our development will have to be continuous. So we have adjusted development programs for them. And the incentives to retain them will have to

be targeted. As we have done in the past, we will have to continue to do.

Mr. LANGEVIN. Thank you.

Admiral.

Admiral ROGERS. Sir, within the Fleet Cyber Command arena, there is approximately 14,000 within our workforce focused on cyber operations, whether it is operating the networks, defending them, or looking at the offensive applications of the networks. The greater majority of those, probably something on the order of 75 percent, are associated with the operations of the networks; and the remainder are pretty evenly split between the offensive and the defensive side.

In terms of where do I think the number is going to grow in the future, clearly, I don't think we know yet what the ultimate end state in all this is going to be, other than I think we see some form of continued, measured growth.

When I say "measured"—because I think part of the challenge is, with 75 percent of our workforce oriented on actually operating the networks day to day, that is a percentage that, from my perspective, is totally out of whack. It is a reflection of an architecture and approach to networks that I think is very dated. As we shift into the cloud and we go forward across the Department in a Joint Information Environment, I view that as an opportunity to harvest the savings of those operators, if you will, and invest them as the seed corn for the cyber workforce in the future, to invest them in the defensive and the offensive side.

In terms of our ability to retain those men and women, to be honest, we have exceeded my expectations. As a person who has been doing this for about 10 years in one form or another now, I can well remember one of my concerns early on as I became involved in this mission set was how are we going to retain these men and women? I think the thing that has surprised me the most and heartens me the most and what I ascribe to that retention is the fact that increasingly these men and women view themselves as warriors, and that is the paradigm and the prism they use as they assess themselves and they think about their future.

And that is one distinct advantage I think for us in uniform. While our civilian counterparts offer many opportunities and, arguably, advantage, the one area that they don't offer is the ability to be a warrior. And the workforce really seems to crystalize around that idea. As well as the broader Navy as a whole is very energized by the mission set, has great respect for its cyber partners, and goes out of its way to highlight to its cyber partners how well positioned they think they are for the future. And the workforce really responds well to that.

Mr. LANGEVIN. Excellent. Thank you.

General Mills.

General MILLS. Sir, we draw our cyber warriors throughout the Marine Corps. We consider every marine a cyber warrior, and we have instituted training packages within our Professional Military Education to enable them to understand what cyber warfare is and how to utilize it.

Specifically, those that are directed to support Cyber Command we are going to grow to about 700 over the next few years, as I

said in my opening statement. We draw mainly from three fields—communications, intelligence, and signals intelligence—to source those warriors.

Of note is that as the Marine Corps lowers its end strength over the next few years as the war in Afghanistan winds down, cyber is one of the communities that will in fact grow despite the fiscal challenges that we face in the coming years.

Currently, we are increasing our marines that are involved in the direct support to Cyber Command, conducting offensive cyber operations. We are also growing a company that will be directed to support our deploying MAGTFs [Marine Air Ground Task Forces] as they go forward deployed aboard Navy shipping and look to crisis spots throughout the world. Those warriors are really a mixture of Active Duty marines, also reservists on Active Duty who support us, mainly within my headquarters outside Fort Meade, and, of course, civilian contractors that we have been able to identify to fill a need.

We intend to recruit, as we always have, the best-qualified young marines that we can find and then to ID those that may have talent and interest within the cyber area and then to train them adequately so they can move forward to do their job.

Like the other members up here on the board, we have not had any trouble at this point in retention. I think that will depend somewhat, obviously, on what the conditions are outside the Services in the years to come. But at this point we have not had a problem retaining our fine young cyber warriors.

Mr. LANGEVIN. Thank you, General Mills.

General Vautrinot.

General VAUTRINOT. Mr. Chairman, as General Mills pointed out, we have cyber expertise that is applied in our acquisition, our engineering, our testing environments. In our operational environment that is Air Forces Cyber and in the component that supports U.S. Cyber Command there are 17,000 great professionals. About 11,000 of those are Guard and Reserve for our total force, and some of those are being repurposed in order to expand on the capabilities that they have to better serve this great domain.

From the standpoint of that operation, it also leverages within the Air Force our Air Force ISR agency: Intelligence, Surveillance, and Reconnaissance; and I have the great privilege of borrowing from Major General Bob Otto's folks, 945 of them, that are in direct support of Air Forces Cyber operations in support of the missions every day.

The creation of the career fields, as mentioned by Admiral Rogers, was similar in the Air Force. Several years ago, we created a cyber operations career in the officer as well as the enlisted ranks. And the one, Bravo 4, is continuing to expand in our enlisted ranks, and we welcome them aboard with special expertise.

That special expertise goes across the training they receive at baseline, which is far, far more unique and applicable to this domain. And then the follow-on courses, as I mentioned in the statement, 10 courses within the Air Force that are resident, seven that are nonresident, many of those supported by our Guard and Reserve counterparts. And then, in addition, those courses, many of them now open to our Service counterparts. Also, the joint courses

that are provided by the Department, five different planning and specialty application courses that these folks are able to attend.

We are also working towards tactics, techniques, and procedures that apply that knowledge not just as cyber expertise but cyber expertise applied to operational applications in every domain. And the expansion of those TTPs [tactics, techniques, and procedures] is what allows us to operationalize this career field and this domain.

The last question was recruiting and retention. I am fortunate to be part of a Service that recruits to retain; and we have been privileged to have any number of folks that come in not just to gain that expertise, which is oftentimes the initiation, but they want to serve the Nation. Now they have the advantage of serving the Nation with extraordinary capabilities that are often not available in industry. And we find that the ability to serve, coupled with those extraordinary capabilities, is a retention factor, and it is a factor in our advantage.

Mr. LANGEVIN. Very good.

Thank you. I yield back.

Mr. THORNBERRY. Mr. Conaway.

Mr. CONAWAY. Well, thank you, Chairman.

And, folks, thanks to you all for being here.

Staying with the personnel theme, the typical cyber warrior, you don't think of them in the traditional warrior category. They need to be a lightning-fast typer and really be able to think and those kinds of things.

In terms of recruiting and targeting the folks you need, I am assuming that everybody you are talking about goes through the exact same basic training, the officer candidate school, all the regular entry-level schools that everybody else does. Is that a barrier to getting folks that you really want? In other words, do you ever foresee a point where they will need those kinds of skills to continue to conduct cyber warfare versus a group that might not be the prototypical marine or airman or sailor or soldier that would need to shoot real straight and be able to be physically very sound and aggressive?

General MILLS. Sir, I will take the first whack at that and say that our cyber warriors are marines first, will always be marines first. They will undergo the same training that every marine undergoes, whether officer or enlisted, and will be promoted and trained within the Marine Corps system. I don't see a problem there, sir.

Admiral ROGERS. For us on the Navy side, we are clearly concerned about that phenomenon. We created a few niche programs, if you will, to allow people with kind of unconventional backgrounds to come into the field. Those numbers are fairly small.

One of the thoughts in my mind is, over time, as our capacity grows, does it overgrow our ability to assess people in the kind of traditional models, if you will, that we tend to do now? It is something that we pay great attention to, and I am always looking in my mind when do we get to that critical typical tipping point where the conventional mechanisms just aren't going to be there for us? We are not there yet. I don't see us getting there in the immediate

near term, but it is something I watch for, because I am concerned about it in the future.

Mr. CONAWAY. General Hernandez.

General HERNANDEZ. Thank you, Congressman.

I would add, as the Marines have said, that we have not seen that as a barrier to entry. In fact, I think this idea of cyber warrior is critical, because they see themselves as warriors.

I have consistently said that in a way there are some characteristics or values that we all have to have, and in this domain there might be a few that we would add a little more emphasis to. So we have talked about a professional team of elite that we will have to really work our way through how we select them, train them, develop, and retain them. Trusted. Because I believe in this domain if you want to be able to gain the authorities to do the missions that you want to do you have to have trust. Discipline to do what it is that you can count on the person in cyberspace, as you would a battle buddy on the battlefield. And precise. Because collateral damage in this domain can be as devastating as any other.

So those are four values, if you will, that we would add to that. I do believe that we are clearly going to have to think about how we develop them differently. And the schoolhouse domain may not be in fact the same model. And they are learning every day because things are changing so frequently that they have to keep up, and the challenges need to stay in this domain. So they have to get the mission that comes with being a cyber warrior. And I believe that the entry will be similar to what we are doing now. But we are looking for that special, elite group.

General VAUTRINOT. Sir, I will echo my comrades. In wearing the uniform, there is great pride. There is also great responsibility; and the accession programs recognize that necessity and leverage that.

But, in addition, the numbers that I spoke to were our officers, our enlisted, our civilians, our contractors, and our citizen airmen that come from the Reserve and Guard. And all of them have the opportunity for this unique training. And as they apply that training, they apply it in defense of the Nation. So I think our cyber warriors extend to every one of those categories. And certainly the specialized training for those that wear the uniform and wear it in harm's way is appropriate to someone that you need to depend upon in that regard.

Mr. CONAWAY. Thank you, Mr. Chairman.

Mr. THORNBERRY. Well, I know you all will continue to watch that. Obviously, a little bit of intuitive common sense says that we may have to treat some of these folks differently; and if it gets to the point where that involves us with some sort of different compensation system, some sort of special carve-out or something, I would want you to let us know. Because it just seems on the face of it that as we go by and, as you said, as we expand and so forth, that we may have to not treat some of these folks the way we always treat everybody else. So I think we will all be interested in that comment.

Mr. Barber.

Mr. BARBER. No questions.

Mr. THORNBERRY. You have no questions?

Let me—I don't know. Maybe these questions are a little bit more suited for General Alexander, and maybe they are just dumb questions, but let me give it a shot.

I understand that each of you all are responsible for your Service's networks. Okay. But in thinking about supporting a joint operation of some kind, whether it is a physical operation that you are supporting or strictly as a cyber operation, how do you decide who does what? Because it seems to me that there is no particular benefit from one Service to the next, no natural sort of inclination. So is it going to work where Cyber Command says, okay, the Army is going to take care of this target set and the Navy is going to take care of this target set and kind of assign responsibilities? Or does Cyber Command say, okay, we will take four Air Force people, a marine, three sailors, and so forth. You all send them up to Cyber Command, and we will set them next to each other and we will tell them what to do. How does the Service component fit into that kind of national mission I guess is kind of what I am wondering.

Whoever wants to help me.

General HERNANDEZ. That is a great question, Congressman. In fact, we are all working through that right now with Cyber Command; and, really, there are several different layers that we have to work through.

The first piece is how do we provide value and resources and forces to a national mission, which is part of what General Alexander has, and what is our requirement for that? And then, second, what do we do with our Title 10 role to provide trained and ready forces to him for his Cyber Command mission? And the third piece is for us to support Geographic Combatant Commanders and in the Army's way also to be able to support tactical and operational commanders that are supporting Geographical Combatant Commanders. So we really have to nest that strategy from the top to the bottom of who is going to do what requirements.

I think we all believe that over time a couple things are essential. One is that is going to become more joint in most cases. Certainly the training and the standards that our cyber warriors will need will need to be joint so that you can count on them being able to interact with joint teams.

The second piece I think is the Joint Information Environment that we have all talked a little bit about and the need to get to that operational warfighting platform that allows us to really have an operational network that we can defend off of in a joint way. Because, after that, it will be coalition operations. As well as an infrastructure that we can conduct cyberspace operations off of. So I believe that work is ongoing, and it is going to have to be nested from the top to the bottom.

The last piece he has given us is a hard look at some functional requirements, what we might do for specific capabilities, command and control, IADS [Integrated Air Defense Systems], and those types of functional looks at how we might ensure that we are providing that capability as a force, as opposed to duplication of effort or worrying about deconflicting it too late because you have invested resources that might not have been done that way. So we are working on all of that together.

Admiral ROGERS. Sir, from my perspective, this is an issue we have spent a good deal of time working collaboratively with each other and with U.S. Cyber Command on to address so how are we going to apply the capacity and the capability that we are each generating.

I will speak for the Navy, but I think it is fairly common for all of us. We provide capabilities both within our Service but, at the same time, as U.S. Cyber Command's Naval component, or Navy component, my comment to him was, sir, we need to generate capacity and capability for you in a way that does this in an integrated fashion; and if we are each going to act on our own, this isn't going to get us where we need to go.

I think, to General Alexander's credit, within the last few months he has generated what we call the Operational Directive, the OPDIR, where he has laid out for each of us here is how my operational vision is in terms of how I will parse out who will have leadership within different geographic areas around the world. And then, once you are designated as the lead, then we collaborate with each other for how we are going to generate the full spectrum of capability and the capacity that we will need to support those joint commanders.

Tie in then, as General Hernandez mentioned, the Joint Information Environment that hopefully gives us over time an underpinning that we can all plug into somewhat seamlessly, as opposed to the environment where we operate in today, where that is definitely not the case.

I think between those two things we are able to apply our respective capabilities to maximum effect. But it is an issue of great concern.

The last comment I would make is one other comment I make regularly to U.S. Cyber Command, is please don't view your components as manpower pools. We are integrated warfighting organizations just like every other mission set within the Department of Defense. Task us, just as we do in every other mission area across the Department. Have us bring you capacity and capability in an integrated, cohesive unit whole, which is the way we are used to working as a Department and the way we have all structured our selves.

General MILLS. Sir, I would agree.

I would just add that we have talked about ensuring that we have standardization, if you will, of training those cyber warriors so they meet the requirements that General Alexander has published. I think this is not particularly a new problem. There are other areas in which you begin to cross over into Title 10 responsibilities of our Service chiefs to man, train, and equip their own forces. But we work in the joint environment in many, many other ways where there are some similarities of how we come together, how we provide forces that are trained to accomplish a specific mission and yet we retain our Service identities. So I think it is a thing we are working through as the growth of Cyber Command takes place, but it is not an insurmountable problem.

General VAUTRINOT. Sir, I will echo Admiral Rogers in the discussion of the Operations Directive, which does two things: It aligns us to provide direct interface with combatant commands that

have unique requirements, but it also leverages the core competencies that are specialties within each of our Services, not just for a given combatant command but in support of each other as we provide those rare capabilities.

In addition, the orders process across the board as U.S. Cyber Command was established has been very freeing in this regard. Because those orders come through to all of us in order to provide capability across the board. Cyber is foundational to every one of the air, ground, sea, space missions. And because it is foundational, we all need to operate in a synchronized and consistent manner. The orders come to each of us in the operation of our portion of the network to provide that synchronization. And so, in following those orders, we are all doing very like things but appropriate to the network that they must be applied to.

So that is foundational, providing the unique core competencies to enhance missions as they move forward, and then certainly expanding cyber in order to provide alternatives that are nonkinetic, that don't require heat-blasting fragmentation, to the Nation through the cyber domain.

Mr. THORNBERRY. Well, that is helpful.

It just occurs to me, as you all sort through these issues that seem to me rather complex, exercises are going to be really essential to test this out. Because, you know, I am not too concerned about the young folks that work for you all, but I am more concerned about the bureaucratic gobbledygook that can foul up even the best intentions. And until we exercise some of this capability, you know, it will be hard to know whether it will really work.

You all touched on this, but it was also a question I had about the relationship of your components to Geographic Combatant Commanders, how that is going to work. Is it Cyber Command directing operations in Central Command and the other commands? Or are you going to send a unit to the commander of Central Command and he is giving all direction for it so that they are completely a supportive body for the combatant commander?

I don't know. Maybe it is not an either/or situation. But you just think about an operation in country X. There is going to be elements that are obviously supporting the tactical fight there, but there are also elements maybe at a cyber domain that will exceed even that geographic area.

Mr. THORNBERRY. And how does that fit with our current geographic divided command structure of the combatant commanders. Make sense?

General HERNANDEZ. Makes absolute sense, Congressman. And that is really part of this directive in reality what we have been working for almost the last 2 years. So from an Army perspective, General Alexander has asked Army Cyber Command to take the lead for him for CENTCOM [U.S. Central Command] and NORTHCOM [U.S. Northern Command]. Now what that translates into is that we have a habitual relationship with a cyber support element that is operating everyday as part of Cyber Command. And we have participated in exercises that demonstrates our ability to bring capability to integrate with his plans as well as provide reachback support from Cyber Command. And as you have described, really there is a Cyber Command global mission that is

supporting an operation that would have a national piece to it and support to CENTCOM. And there is a CENTCOM piece that would be directed in support of CENTCOM principally led by Army Cyber Command but with Joint Forces and joint teams from all of Services.

Mr. THORNBERRY. So who calls the shots when there is a global component and a geographic component?

General HERNANDEZ. Clearly, in a global domain, it needs to be coordinated and integrated and deconflicted very quickly and at the Cyber Command level.

Mr. THORNBERRY. It just seems to me it may be a challenge to work our way through. I don't need to tell you that.

Last question for now, and then I will yield to my colleagues. There are rumors that there are rules of engagement bouncing around the Pentagon. I haven't seen anything yet, but I guess my question to you all is how comfortable are you that we are close to having rules of engagement that we—that the country can move forward and operate with?

Admiral ROGERS. That is really within General Alexander's lane, if you will, as the Joint Commander. It is an issue he continues to work with the Department and the Joint Staff leadership and the rest of the combatant commanders. It has been an issue of discussion for some period of time now. I think there is recognition that that is a requirement, something we need to do. The devil is always in the details, if you will.

But my sense is that at some point in the near term, we will start with something that will continue to evolve over time, which is what you see in our standing rules of engagement for the Department, for example. That is the way they worked those. I think you will find the same thing in the cyber arena as well.

Mr. THORNBERRY. Essentially, the Joint Staff and the Cyber Command will hand you all rules of engagement that you will then have to look at, plan with, operate from and will evolve understandably over time.

Admiral ROGERS. As will all commanders within the Department, be standing rules of engagement for all.

General VAUTRINOT. Chairman, there are existing standing rules of engagement for every one of the execute orders and the orders that the military is working under with regard to cyber operations today. And I believe the expansion of those orders is in the area of defense of the Nation as opposed to the defense of our Department's networks, but in defense of the Nation. And certainly work in that regard is what General Alexander is moving toward, but I did want to point out that the standing rules do absolutely exist. And we test those as well as test the potential rules of engagement in the exercises that you mention. For example, if I am working with the combatant commands on behalf of General Alexander to bring that face and that cyber expertise toward them, Turbo Challenge, Austeer Challenge, Global Lightning, Judicious Response and those kind of tier 1 exercises in each one of the combatant commands informs both the command and control relationships as well as the necessary rules of engagement and any shortfalls.

And then Cyber Flag by U.S. Cyber Command brings us together to do the force-on-force and engage and then take that information

back into both the Department's tabletop exercises as they do strategy as well as war games, like Unified Engagement, that bring leadership together to think about those rules of engagement and how the civil leadership wants the military to perform in that regard. So those exercises are very, very successful in bringing that information forward.

Mr. THORNBERRY. The only point I would add—not that it is you all's responsibility, but I made this point to other folks in the Department—it seems to me that in this area of cyber rules of engagement, it is more important than ever for the Department to engage with Congress because a cyber engagement is unlikely to take place in a timeframe where we can formerly pass a declaration of war and authorization to use military force.

The force that we are talking about here occurs at the speed of light, and so having that consultation ahead of time will smooth things for the time when there could be a use of military force in cyberspace that will start getting into constitutional issues and a variety of challenges for us on this side of the river as well as the funny-shaped building across the way.

So, Mr. Langevin.

Mr. LANGEVIN. I do, Chairman. And in tangential to what the chairman was just asking that is on my mind, because obviously, these are very powerful tools, both the offensive and the defensive side, and we have a lot of things to work through. Do you believe that you need additional authority to undertake your current mission sets?

And General, you touched on some of these things already, but can you describe the legal authorities that govern offensive and defensive operations, just to delve into it a little deeper?

General VAUTRINOT. Sir, probably not my lane, in terms of the legal authorities, and I certainly look to the Congress to ensure that we have those authorities to move forward.

However, I can say that in doing operations on a daily basis and in support of Cyber Command's mission tasking, we leverage the authority of the intelligence community under Title 50 of the U.S. code; certainly leverage the authorities in law enforcement under Title 18 in order to support those activities; and then of course your Title 32 authorities that you are very familiar with—I know that you support the 102nd—it is a Guard unit that works directly with us in mitigating and responding to emergencies in cyber on a daily basis, perform those operations under Title 32 for the Guard; and then, of course, Title 10 operations, which we are most familiar with in the military.

And the important area is to make sure that we can work with unity of effort as we are all working toward in the military and synchronize these things in a way that supports the nation, both protecting the national security while also preserving privacy and preserving intellectual property. And that is the difficulty, is making sure that we ensure all of those things, rather than trading off, and I applaud the work that has been done both to dialogue in the Congress and now going to the debates that will bring us forward in moving those authorities.

Mr. LANGEVIN. Thank you.

General HERNANDEZ. Congressman, I would add that I, too, am comfortable that we have the authorities needed to do our mission. But I would say that most significant is the legislation that is being worked. And I applaud that for a few reasons. First, it helps codify and clarify "dupe" [duplicate] roles and responsibilities. The second and important one to all of us is really if we are able to get into information sharing in ways of looking at protecting our critical infrastructure, that will now allow us to see things and do things in real time, where others know things that would help each other, they are left and right on a daily basis. So I think that is critical to our work.

Admiral ROGERS. And I would echo General Hernandez.

I am comfortable with our ability to execute our mission set. Now one think I like about the Navy's construct, like the joint world with General Alexander, the Navy cyber capabilities both in the Title 10 and Title 50 arena are all OPCON [Operational Control] to the Fleet Cyber Command and 10th Fleet, much like General Alexander does in both his Director of NSA [National Security Agency] as well as Commander, U.S. Cyber Command, hat. That gives us flexibility.

And as General Hernandez indicated, the biggest issue I see increasingly over time is the ability to share information outside the Department and with partner sets that traditionally we are just not used to dealing with. When I look at the problem set, it is the nature of the future in this domain.

Mr. LANGEVIN. Thank you.

General MILLS. I would echo what my partners here have said, I would point out that gap that exists between the authorities we have to protect our critical infrastructure onboard our bases and the critical infrastructure that exists out in our local communities that yet support our bases, electricity and things like that. So that gap in authorities I think needs to be closed, and I believe that is what the legislation is going to do. And that is why it is so critical, I think, to the overall attempts of what we are trying to do.

Mr. LANGEVIN. Very good. Thank you.

Mr. CONAWAY. Kind of a two-prong question.

One, does the Department of Defense have an adequate definition of what is and isn't cyber with respect to budgeting issues and how that all gets captured?

And then, two, acquisition, when you are buying big stuff, it is obviously a problem to stay on the cutting edge. Your domain, it would seem to me, would need to be the best tools available at any one point in time, whether that is software, hardware, those kind of things. Do you see acquisition challenges that will prevent your team from having the best F–35 in the Air Force's case? You know, that is leading to, are the incremental costs not so much that it is really an issue?

General VAUTRINOT. Let me talk a little bit about acquisition because we have had some real movement in this regard, and I mentioned it in the written testimony as well as the spoken. When you asked us in the authorization act to look at the methodology by which we acquire and make it appropriate for cyber, there is a recognition that the 5,000 series, the acquisition of very long-term, long-term sustainable bent-metal type programs is not appropriate

to both the rapid change in cyber as well as the ability to leverage capabilities against an existing and very dynamic architecture.

And so we have moved forward in both providing real-time development of tools that can be resident on those architectures and can leverage the existing architectures, which certainly we have already been working and provided capabilities both to U.S. Cyber Command and to the combatant commands.

The next step in that response is rapid acquisition, which scales the folks that are doing material acquisition, the engineers and the acquisition professionals that I would see in ESC [Electronic Systems Center] as part of Materiel Command, brought together with the testing environment, brought together with the professionals in the Air Force, research, laboratory, all of those folks are coming together, in my case, in Texas, not to work for each other but to work those elements of science and technology, prototyping, development, test, fielding, and training of the forces to use those resources and those capabilities in real-time.

And so that rapid acquisition is part of the response I believe you will see from the Department in terms of how we need to acquire for cyber and move forward more rapidly.

Mr. CONAWAY. Is that a joint acquisition, or is that each Service would have their own stovepipe like you are talking about?

General VAUTRINOT. Sir, I will defer to OSD AT&L [Office of the Secretary of Defense for Acquisition, Technology, and Logistics] as they respond to that, but the methodology is the methodology that they are exploring. We are the pilot case. We are actually applying that methodology within the Air Force down in Texas.

General HERNANDEZ. Congressman, a couple points——

Mr. CONAWAY. If you don't have anything to say, you don't have to say. I mean, it is not a required response, but if you have something, I would appreciate hearing it.

General HERNANDEZ. I would start by saying we are working very hard to capture all costs associated with this. As you know, it is not—as you start defining cyber in the three lines of efforts between operate, defend, and offense, there is a lot of information technology. And how you sort those costs out is work going on significantly in all the Services.

Within the Army, the Secretary of the Army has started an IT [information technology] management reform initiative. There are several pillars to that, but one of them is to establish a governance that allows us to get after the cost, and another one is a process that allows us to acquire IT through an agile process. In the meantime, as we work through that, we have worked hard our requirements from both defense and offense.

From a defensive standpoint the network integration evaluations that we do every 6 months at Fort Bliss, where everything that we intend to put on the network is tested there, allows us an opportunity to rapidly test, deliver, and field capabilities. And at the same time, we look at all of them to make sure they are bringing no vulnerabilities to our network. So I believe that will cause the process to go faster with respect to acquisition from that end.

We do have—are working with an organization in the command that has given us authorities to rapidly field and test capabilities that we would need to have quickly if we wanted to put inside of

an operation. But I think the future really is how we do more of that better and get at capabilities across all the Services in a joint way.

Admiral ROGERS. Sir, the only thing I would add, in the Navy, this is something we spent some time thinking about, how do you meet the acquisition challenges in the cyber arena? While work with our broader joint partners and the broader standard acquisition mechanisms within our Service, we also, within Fleet Cyber Command, created a small core R&D [research and development] capability under my control as operational cyber commander for the Navy with some seed corn in it, if you will, that allows me and others to rapidly acquire and develop kind of top priority cyber capabilities for us that are done outside, if you will, the traditional acquisition pipeline for us, with some specific restrictions, if you will, about how we do it so we are not duplicating the effort of others, but it has proven to be a great capability for us.

Mr. CONAWAY. One quick follow-up, and it occurs to me while we are sitting here thinking, is if we have got an array of weapons that are appropriate for a Marine company or a platoon, they are given certain tools and certain weapons that we all agree to.

In this arena, there seems to be that each of those operators have the opportunity to either build their own tools or their own weapons, their own equivalents. Is that—have you thought about that as a concern yet at this point in time, in terms of what these folks are able—because these are going to be bright people, and they are going to be in an arena where innovation and being the first to be able to do X, Y or Z is a real issue. And they are going to be—competition and competitive to try to do that. How do you let that happen but don't lose control of it?

Admiral ROGERS. I will give you my perspective. I think the positive side is so far we have managed to strike a good balance that provides for the initiative, which is I think is at the heart of really one of our positives, both as a nation and within the Department. At the same time, as we each generate unique capabilities, if you will, within our Service, we will push them up in the joint arena to U.S. Cyber Command and the National Security Agency to kind of act as a central repository, if you will. And then we will harness that capability as we are looking at different mission sets and what tool sets are available out there that other partners have developed, and we are finding ourselves more and more using tools and techniques developed by other Services and by our joint counterparts.

Mr. CONAWAY. Okay.

Mr. THORNBERRY. I think we have had provisions in the fiscal year 2010 and fiscal year 2011 defense authorization bill on rapid acquisition for cyber.

So I was listening to your answers, but I will make the same offer, as you work through these issues, if you find that you need some additional authorities, you know, please let us know. We have provided some unique authorities in some other areas, Special Operations and whatnot, and it may well be that cyber just doesn't fit or somehow the tools available to DOD do not fit this domain, and so I wanted to make that offer as well.

Ms. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman, and I am sorry that I wasn't able to be here until the last few minutes, but I certainly appreciate all of your work, your dedication to our country, thank you very much.

I wanted to just ask a people question, and you may have already addressed this, but in this unconventional domain in which we are asking you all to work right now, could you just talk for a minute about the stress levels and what you're feeling or finding in terms of morale of the force that is the feeling in this new area? What are we learning about that? And are there things that we should be doing to really help and support people along the way?

General HERNANDEZ. Congresswoman, thank you.

We did have a little bit of this conversation, and I think the key point I would say is, one, they appreciate being cyber warriors. They are excited about the opportunity. They are excited about what they are a part of. And our charge is to continue to develop them and continue to keep that excitement because we can't do it without them.

Admiral ROGERS. I guess for me it is kind of interesting I guess the more junior you are in our workforce at least, the less you think about the challenges and the much more you are focused on the opportunities and the energy that you bring to the fight. Generally, as you are more senior, perhaps a little older, I generally see at that level, you are much more concerned or really focused on the challenge set. And you see that stress where you are looking at the range of things that you know we need to do. You are looking at the range of resources that you have right now to do it, and you know you have to prioritize. You have got to focus on what needs to be fixed first. And so there is always those trade offs. But the positive side I think is for our workforce, they are energized by the situation, which is a great thing for us and the Nation.

General MILLS. I would offer up the same observation. I think morale is extraordinarily high because I think that the people involved in the cyber understand that they are cutting-edge, and they are developing a new weapon system that is going to have a huge impact on the battlefield, and they are excited about that. I think they are also excited about being a part of ongoing real-world operations, and they understand that what they are in is not just not simply a training mission or an exercise, but they are out there doing real things and having a real impact. I think that enables the morale to stay high, despite the long hours and perhaps the shortage of personnel we have from time to time to—morale is not an issue.

General VAUTRINOT. I will echo my Service counterparts. There is an excitement. It is a target-rich environment of things to fix, of things to change and an environment where you can have so much impact on how the Nation is going to leverage this capability and how we are going to help to protect the Nation and meet the requirements. They are rising to that challenge. I think that is what we see every day is that level of excitement and that level of commitment.

Mrs. DAVIS. And do you have any concerns that you won't be resourced properly? You said sometimes the numbers, as you are

growing more of this force, is that an issue? Are you worried about that? You probably already talked about that as well.

General MILLS. I don't. I think the training pipeline is long, and so once you identify the personnel and you train them within your own Service and then get them the joint training they need to be able to be employed, that takes a while. And so that is a challenge, but it is a challenge that we can overcome.

Mrs. DAVIS. Great.

Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank you.

Is there any disadvantage to choosing one of the career fields in cyber right now as far as a long-term military career? Have we standardized everything so there is no problem at all, or can you pick one of these new cyber career fields, stay in it for 20, 30 years, if you want to, and retire and so forth and move on? Or is there any disadvantage is really my question?

General HERNANDEZ. I see no disadvantages today. In fact, I think we talked that word before; they see more opportunity. And as we develop the domain more and we move to an operational network, I think we will see more convergence. And with convergence comes the ability for defenders to also do not just defense but operate potentially offense, and that is exciting. And those that are offense will learn skills on how to defend, and that moves us to a domain that you can really operate in, and I think that will provide more opportunity and more excitement for them than being stovepiped or think that they are too narrowly focused. So getting that balance between generalization and specialization with great development opportunities I think is the future here.

Mr. THORNBERRY. I think that is a fair point. I guess I was really thinking just more the way the military sees careers and what it rewards, what it doesn't, who it promotes, all of those sorts of issues. Do you think we are at a point where these cyber career fields are treated equitably at least of other career fields?

General MILLS. I think it may about a little too early to tell the answer to that question.

Mr. THORNBERRY. Haven't had enough experience yet.

General MILLS. Yeah. I don't think there is enough depth yet, enough officers are enlisted who have gone up for promotion, et cetera, et cetera. I think that will play out. I think part of that is incumbent on us to make sure that our Services are educated as to what the individuals are doing, to ensure that the Services understand the contribution they are making, and understand, although their service record may be unconventional, that in fact, much like special operators, what they are doing is extraordinary valuable. So there is a—time will tell.

Mr. THORNBERRY. Okay. Let me just ask this, thinking midterm maybe, 3 to 5 years ahead, what technical capabilities would be your priorities for development? And kind of an ancillary question, do you have input into your Services' R&D priorities for the future? That is another area the subcommittee covers, our S&T programs. So what are your technical priorities for the next 3 to 5 years? And do you have input into your Services' research and development program over that period?

General HERNANDEZ. Congressman, I would answer absolutely we do. And our R&D priorities are nested with the Department of Defense's priorities in this arena. We have helped shape several of the requirements that we know we will need from an S&T standpoint for the future. And we are also working with a lot of partners on near-term things that they can assist us with.

My number one requirement for the near term really would be capability that increases our situational awareness, that allows us to see ourselves better, allows us to see the threats better and allows us to see the cyber terrain we are operating in. That is not an easy problem, and it is one that we are only going to be as what we see and as we move through a global domain, we will have to have better visibility to cross all of it. So that's my number one short-term requirement.

Admiral ROGERS. I would echo General Hernandez, probably situational awareness, number one. Because if you want to defend an operation—if you want to defend and operate in an environment, the human condition, generally you have to be able to visualize it and you have to be able to understand it in a way that enables better and quicker decisionmaking, particularly in this environment. The only other things that come to my mind are automating—automated decision aids, again, that increase speed and agility because we are going to continue to use traditional timelines and methodologies we are going to be behind the power curve in this domain. And then, lastly, automating a lot of our defensive capabilities, things that still require more of a man-in-the-loop than I would like, for me at least.

Mr. THORNBERRY. I am sorry, General, if I could interrupt. So do you have input into the research and development the Navy puts into those issues, or do you look primarily to the private sector for some of that?

Admiral ROGERS. I do both, to be honest.

Mr. THORNBERRY. You develop it——

Admiral ROGERS. Well, I—and I also look to the private sector as to what kind of things are you working on that might have applicability for us.

General MILLS. Sir, I would echo what the Admiral said, as well, and I would add that the Marine Corps looks to develop ways to make these capabilities expeditionary; how we can forward-deploy them, how we can support our crisis response forces that are out forward-deployed at the point of the spear, how we can bring those with us in an expeditionary manner. I would also look to help us solve some of the area denial, anti-access threats that are appearing, and we have to deal with as we look at, again, maritime operations in areas in which we may not be welcome. Those are the areas in which we are looking at, as well as what the Admiral said.

General VAUTRINOT. Sir, I will address the second first, and that is, do I have input? And the answer is absolutely. In the Air Force, we have a core function lead integrator for the entire Service that looks at each one of the core areas. And for cyber, that is General Shelton who is Air Force Space Command. And so, in a prioritization, we directly input, and that is exactly what came out of the master plan in terms of the prioritization.

We also do the "one to n" priorities associated with science and technology and the research and development activities that are being done by our Materiel Command in this regard. So it is a very direct input, and we are seeing the benefits of that collaboration and seeing it all come all the way back into that what kind of capabilities we are now able to field. So let me answer that portion next.

In the capabilities that we are seeing fielded, on the defensive side, we talked about the AFNet migration, the Air Force Network migration, which is an effort to create from the heterogenous, the very individual networks that were then brought together to become the network from the way that they were originally designed, how do you make that more homogenous and then you are able to apply situational awareness, an automation to that homogenous network, and so we are very far I long the path in doing that on our unclassified networks at every one of the bases worldwide. So we have created an architecture that says we go under the gateways, everyone comes through those areas, that allows us to treat everything as an operational environment and defense in-depth and then apply the tools to best leverage and give additional capability, so it is a platform, not discrete individual items thrown at the problem. So you are doing it in an organized, operational, normal fashion but at a very rapid pace.

Those same tools can then be applied to protect infrastructure to look at what the vulnerabilities, the key terrain in cyber for all of that infrastructure capability. And I was talking to Congressman Langevin earlier about remote forensics and the ability to do that in real-time and then apply the lessons, both from the intelligence community that are very dear, as well as your understanding of your own network. So we are seeing both the prioritization and, more importantly, the application to those priorities to the capabilities that are right now coming out on both the defensive and the full spectrum capabilities we are applying to Cyber Command.

Mr. THORNBERRY. When you get all those networks working together, I want to send you over to the finance people at the Pentagon so maybe they can pass an audit before too long.

Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

General Vautrinot, I wanted to touch on the role of the Guard since you talked about that in your testimony, and I am pleased to see that in your testimony, you did highlight the role of Rhode Island Air National Guard's 102nd Information Warfare Squadron. Can you talk about how you see the role of the Air Guard, and Reserve cyber units evolving in future years? And are these units properly resourced and manned? And then, in addition to that, I talked about the combat communications unit in Rhode Island that is going away and how General McBride is looking to increase, kind of have that role evolve and have the cyber warfare unit play an expanded role as that is being replaced. But if you can talk on the role of the Guard and Reserve and the cyber units and how they are going to evolve in future years, that would be important.

General VAUTRINOT. Certainly, sir.

Admiral Rogers would say, a rising tide serves all boats. In the airmen language, that would be, you need to gain a little altitude

in order to be able to maneuver. The use of the total force gains us that altitude because these are citizen-soldiers, and they go back to their communities. So, in the case, for example, of the 102nd, they are part of the Air Force Cyber Emergency Response Team.

They are using the same very high-end capabilities that we just described in their day-to-day mission. It is an operational mission, and it is serving the Air Force and Cyber Command, but it also serves in bringing their level of training, the exact same training and the same equipage, the same capabilities, they can take that back to their community, back to their corporate entities that they serve on a day-to-day basis, and they can apply that same knowledge in the same way that citizen airmen do when there is a crisis of any kind. In this kind, it is a very technical application.

So, as we expand that, then we have I guess in cyber, it is about team, and there really is an "i" in team. It is about industry. It is about the intellectual capital of our universities, like your University of Rhode Island, who just got the Center of Excellence Award from NSA, very rare, sir. It is about interagency, and it is about international cooperation. And so you bring all of those "i"s into team, and literally, what you are doing by bringing the total force together is expanding that across the Nation so that we can all apply that.

Do we have sufficient resources? As the Guard does those transitions from some missions that are no longer most appropriate in the cyber environment, and so for combat communications, they are a national treasure, but that treasure is about hooking up communications in a deployed environment. And what General Alexander and the Nation needs is the ability to extend a defensible, robust, trusted network. And so that extension is the way that we are moving forward in the future, and so as the Guard would service that intent and that vision, we would want to repurpose those forces into those kinds of missions and make sure that we move forward.

In terms of total numbers, for example, the 119th in Tennessee, a great effort to provide some resilient facilities in Tennessee. And we are working with the Guard to try to actually put resources, manpower resources, against that facility to allow it to be a resilient capability for the Nation, for the Air Force, on behalf of General Alexander.

So we need the Guard and the Reserve to move in that manner in order to move this mission forward.

Thank you, sir.

Mr. LANGEVIN. Any other——

General HERNANDEZ. If I could add a few points, we are working closely with Reserve component, both Guard General Ingram and Army Reserve General Talley. All those units that have cyber capability are under the operational control of Army Cyber Command today. We leverage them routinely. They bring unbelievable skills to all the mission sets.

There are a couple other areas that there is tremendous opportunity that we are working with them on. And first is, what else can they do to help with homeland defense, with the defense network the National Guard has, not only in a recovery but in a preventative way with their defenders, as well as critical infrastructure protection?

The second thing is they have tremendous skills that we haven't harnessed those skills. We know about where they are, but they sign into units that are different than the skill set. We haven't determined how we can best utilize those individual skill sets. I think there is opportunity there that we are working on.

The other area, as you know very well, is there are state partnerships are strong and vibrant in other countries, and our part of that would be, how do we establish those partnerships in this domain with other countries where building partnership capacity is important and there is a cyber element from a state unit that could support us with that?

And the last one I would highlight is we have a pretty robust STEM [Science, Technology, Engineering, and Mathematics] program in e-cyber mission, and I think that there is tremendous opportunity that we are starting to work with States from the National Guard perspective to expand that STEM to the communities.

Mr. LANGEVIN. Yes, sir.

Admiral ROGERS. And I would just add on the Navy side, I find our Reserve teammates among the most flexible and willing to try new innovative things when it comes to the application of their capabilities. Every major combatant commander has tier 1 exercises during the course of the year, and the Pacific TERMINAL FURY is Pacific Command's largest tier 1 exercise during the course of the year. Like we do with every major exercise in every major operation, we do we integrate our Reserve teammates into what with do. For TERMINAL FURY 12, we decided to try something a little different. Traditionally we apply skill sets based on a pay grade or a designator if you will that kind of codifies an individual's background. We approach the Reserves this time and said, let's try something a little different. I don't want to specify pay grade; I want to specify a particular background or skill set in the civilian sector and see how we would match those like matching by pay grade, which was just amazing, the amount of capability and expertise that is resident in that structure when you look at it slightly differently and their willingness to do that. I didn't get any pushback at all; was just amazing, and it really energized them. So it is something we hope in the Navy hope to build on in the future as a great experience and hope to do more of them.

Mr. LANGEVIN. General Mills.

General MILLS. Our mobilized individual reservists bring great skill sets with them when they come on Active Duty. They play a very important role both at my headquarters MARFORCYBER [Marine Forces Cyber], as well as over at CYBERCOM [U.S. Cyber Command], where they fill some very critical billets. So very, very important role for us as well.

Mr. LANGEVIN. The last question I had since obviously the younger generation seems to obviously take to technology like fish to water and probably some of the youngest recruits are going to have some of the most robust skills, what kind of transparency or situational awareness do you have in terms of throughout your various Services of those individuals that aren't assigned or haven't chosen the cyber route as a career path but that you could potentially tap into and recruit from the rest of the various aspects of your Services that might at some point have to think about encouraging

them to go into a career in cyber or that, in the event that the Nation needs surge in the area of cyber, that you could quickly identify and tap into and then draw the folks into your various roles? Have you thought about that and if you could can you talk about that briefly?

General HERNANDEZ. I will start. We, our personnel systems have limited visibility on the depth of skills that we would want to identify for this particular domain. We have an initiative that we will work total Army that is intended to get at Active, Reserve component military and civilian called Green Pages. We have done some pilots in the Army with Green Pages that says, these are the list of skills that we are looking for; do you have these skills, sign up for that. And then there is a potential opportunity for you to serve in these assignments, and you might get better matches than the way we currently do it today. But it is a pretty large holistic view that says what are the skills we would want to have and start describing those that so that they can tell us what they have and allow us to get a better utilization of them, but that is work to do Congressman.

Admiral ROGERS. Sir, I think for us—I think it is true for all the Services—our view is that cyber is so fundamental to the future that the idea that the only people that we are going to train are some sort of core specialists, if you will, isn't where we need to go. So as a Service, we have tried to put a fundamental layer of cyber education, training, and awareness across the entire force. As we do that we do that, we quite frankly also use that as a vehicle to try to find, so who is out there who would be interested in this, who has some skill that might be interested in changing rating, if you will, or specialty? And we have structures in place designed to allow us to do that. We have been able to do that with a pretty high degree of success so far about reorienting, if you will, the workforce internally to align people that their skill sets against perhaps a different specialty than they started their journey.

General MILLS. We identify those individuals at the entry level who had that skill set or who are interested in a skill set or at least had the academic qualifications to be able to train in those areas. Being relatively a small Service and joined from basically three communities, which are achieving narrows that pool down, I think it becomes easier for us to identify candidates that would do well with the cyber specialty. We also give marines the opportunity to move from MOS [Military Occupation Specialty] to MOS at certain times during their career, during their reenlistments for instance. And as we draw down in certain areas, we expand within cyber; our young marines again will pick up on that and will have the opportunity if they are qualified, they are talented, if they are interested, to be able to move over into cyber.

We see the cyber warriors, if you will, moving into cyber and then moving back to their own specialty in communications or intelligence during their career, and that will grow a pool of qualified individuals that we could assign if there were in fact a requirement for a surge at some particular time.

Mr. LANGEVIN. Thanks. Very good.

General VAUTRINOT. Congressman, on the Active Duty side, our Air Force personnel center affords extraordinary insight into the

capabilities, the scores, the testing that are done in the sessions. Particularly for our enlisted force, most of the career fields in cyber are not accession career fields. We actually cross-load them based on both their excellence and those scores on the test and then bring them in and do the training at a higher level. And so we have no shortage of folks that want to move across in that crossflow, and it is usually the program shortfalls that don't allow us to bring them fast enough, and they are working on those across the board.

On the Guard and Reserve side, there is less visibility, but I know that our counterparts are trying to work that visibility, get the kinds of information that Admiral Rogers mentioned in terms of what kinds of skill sets did they use in their private employment? What kinds of skill sets did they have as they were coming through their educational opportunities that may differ from their current responsibilities and their current functional designation and allow us to leverage them and train them in this area, whether it is applied to their current functions or whether it is applied directly to the cyber environment?

Mr. LANGEVIN. Very good. I thank you all for your answers on those, and I am glad you are giving it thought. And obviously, we are challenged nationally in terms of the number of people that we have that can go into this field, and the STEM fields, we have to do a better job at encouraging kids to go into science, technology, engineering and mathematics.

General, you talked about Cyber Patriot, and we have created in Rhode Island—and it is a national program; there are a few different states that are doing it. It is called the Cyber Challenge program. You take kids that are in high school, and it is about a 6-week program, and you put them through the paces. And you take kids that think maybe the computer is something they do and it is a hobby, but you get them thinking about a career path in that field and that is what Cyber Patriot and Cyber Challenge are all about. I thank the chairman. I yield back.

Mr. THORNBERRY. So, in that discussion, I think I have this right, reminds me of Estonia, where after the denial of service attack that they have suffered, they have people lined up in banks, in retail all scattered all over the country to help defend the country in cyberspace if they need to. Maybe that is the sort of surge capability we need to think about eventually.

Ms. Davis, do you have other questions?

Mrs. DAVIS. No.

Mr. THORNBERRY. I think that is it.

Thank you all very much. We appreciate hearing about your successes, but we also, as we move forward, want to hear about the challenges you encounter. That, as I said a while ago, I think that open communication across the river is going to be especially important in this area. So, again, thanks for being here.

With that, the hearing stands adjourned.

[Whereupon, at 5:17 p.m., the subcommittee was adjourned.]

# A P P E N D I X

JULY 25, 2012

## PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JULY 25, 2012

**Statement of Hon. Mac Thornberry**

**Chairman, House Subcommittee on Emerging Threats and Capabilities**

**Hearing on**

**Digital Warriors: Improving Military Capabilities for Cyber Operations**

**July 25, 2012**

We welcome our witnesses, guests, and members to this hearing in the Emerging Threats and Capabilities Subcommittee on "Digital Warriors: Improving Military Capabilities in the Cyber Domain."

There is widespread agreement that cyberspace is now a domain of warfare, and many people regard it as the most difficult, perplexing national security challenge we face. Certainly the laws, policies, and organizations have not kept pace with the evolution of technology. But if cyberspace is important to our country's security and if it is a domain of warfare, our military services, on whom we rely to protect and defend us, must be prepared to operate in cyberspace as well. That preparation involves a number of issues, including organizational structure, recruitment and retention of qualified personnel, training, rapid acquisition, among others; and it is those issues which we want to examine in today's hearing.

**Statement of Hon. James R. Langevin**

**Ranking Member, House Subcommittee on Emerging Threats and Capabilities**

**Hearing on**

**Digital Warriors: Improving Military Capabilities for Cyber Operations**

**July 25, 2012**

Thank you, Mr. Chairman and thank you very much to our witnesses today. It's a pleasure to see you all again and to have you join us for what I believe is a critically important hearing.

There is no more critical task in today's environment than safeguarding the Department of Defense's networks. The cyber domain has become an integral part of every action DOD undertakes, whether offensive or defensive. And as operating environments grow ever more complex, we need joint forces that are manned, trained, and equipped to conduct the full spectrum of operations in support of, and in some cases, supported by, what we think of as traditional military forces.

The Congress, and the country has a whole, has been struggling with what cybersecurity means to us as a nation. We're grappling with how to protect our systems and our privacy at the same time. I'm proud to be part of that robust discussion. I've helped draft some legislation and co-sponsored others, and now it looks as if something may be moving over in the Senate. Let's hope so. I hope today we'll hear your thoughts on what sorts of additional authorities you may need and how the proposed legislation may or may not affect those needs, as well as your thoughts on the delegation of authorities within the executive branch.

But most importantly, I hope we hear about how you are finding and retaining the sort of people you need today and for the future. This is, I believe, the fundamental challenge that faces us. It is often said that the root strength of our military is the quality of our people and nowhere is that more true that in your organizations. As you think about growing your forces, what thought have you given to where the people are going to come from? How will you keep them, promote them, educate them and continue to challenge them, even when outside organizations are keen to lure people with these skill sets away to the private sector?

Lastly, I need to take a minute to talk about a topic that would be irresponsible to avoid. We all know that we are facing significant fiscal challenges in the coming years, even without the threat of sequestration looming. Cyber-related activities are faring reasonably well so far, but nothing is immune, and even non-cyber-specific cuts could have an impact on your commands as personnel resources are reduced or research and development funding decreased. Those are just two examples. As you look ahead, how do you factor in the possibility of even more austere fiscal environments? This is a tough question, but one we must face in order to responsibly address the complex challenges of the future.

Thank you, Mr. Chairman, for holding this hearing, and I look forward to a robust discussion.

RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL RHETT HERNANDEZ
COMMANDING GENERAL
U.S. ARMY CYBER COMMAND/2ND ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

CONCERNING DIGITAL WARRIOR: IMPROVING
MILITARY CAPABILITIES IN THE CYBER DOMAIN

SECOND SESSION, 112TH CONGRESS

July 25, 2012

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Chairman Thornberry, Ranking Member Langevin, and members of the Subcommittee, thank you for your ongoing support of our military and for the opportunity to tell you about Army Cyber Command. I am honored to represent the required staff of 561 Soldiers and civilians, whose great work enables our Army's ability to operate everyday and adds to our Nation's security. I am humbled and proud to serve with them, and amazed at what they have accomplished and continue to do daily to address cyberspace challenges and opportunities.

Much has happened since I last spoke to this Congress in September of 2010, before activating the command. The men and women of Army Cyber Command have been hard at work increasing the command's capacity and capability, securing and defending all Army networks, conducting cyberspace operations in support of USCYBERCOMMAND (USCC), and preparing the Army to prevent, shape, and win in and through cyberspace.

The Secretary of the Army created the United States Army Cyber Command/2nd U.S. Army pursuant to General Order 2010-26, establishing it as an operational-level Army force reporting directly to Headquarters, Department of the Army. The Command attained full operational capability on October 1, 2010. Army Cyber Command is the lead for Army missions, actions and functions related to cyberspace, and responsible for planning, coordinating, integrating, synchronizing, directing and conducting Army network operations and the defense of all Army networks. When directed, Army Cyber Command conducts a full range of cyberspace operations to ensure freedom of action in cyberspace, and to deny the same to our adversaries. Army Cyber Command serves as the single Army point of contact for reporting and assessing Army cyberspace incidents, events, and operations and for synchronizing and integrating responses thereto.

The Secretary of the Army has also assigned responsibility for conducting the Army Information Operations (IO) mission to Army Cyber Command. As cyberspace is a global domain within the information environment, having a single three-star Command responsible for both cyberspace and information operations allows for the necessary integration in support of these two mission areas.

Army Cyber Command also serves as the Army's force modernization proponent for cyberspace operations and is responsible for the development of required Doctrine, Training, Leader Development, Organization, Materiel, Personnel, and Facilities.

The Command is a split-based command, with the Headquarters at Fort Belvoir, Virginia, with select staff elements at Fort Meade, Maryland. The Headquarters is has a required strength of 561 personnel and a current strength of 509 personnel. Other Army Commands supporting our efforts include the U.S. Army Intelligence and Security Command (INSCOM), Fort Belvoir, Virginia; the 1st Information Operations Command (Land) (1st IO), Fort Belvoir, Virginia; and,

the U.S. Army Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM), headquartered at Fort Huachuca, Arizona. Together these units provide more than 21,000 Army Soldiers, civilians, and contractors in support of cyberspace and information operations worldwide.

Army Cyber Command and its supporting units are in action every day securing and defending Army networks and conducting cyberspace operations critical to DOD and Army missions. To defend and advance our national interests, Army Cyber Command must, like the entire Army, balance resources and risk to perform the Army's three roles: prevent conflict by maintaining credibility based on capacity, readiness, and modernization; shape the environment by sustaining strong relationships with our military allies in other nations, building their capacity and facilitating U.S. strategic access; and, win decisively by applying combined arms capabilities to dominate the operational environment.

As the Army looks toward its future, we must continue our fundamental transformation to meet the challenges of the 2020 strategic environment. This transformation must include the development of Cyberspace Warriors and organizations able to use cyberspace to gain advantage over threats to seize, retain, and exploit the initiative. Cyber Warriors and formations will help joint force commanders prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution by being trained, organized, and equipped to conduct, as directed, the full range of cyberspace operations.

**Cyber Threat**

We all recognize that cyber threats are becoming more dangerous and are on the Intelligence Community's list of biggest challenges to our Nation. These threats are real, growing, sophisticated, and evolving. There is a wide range of actors ranging from lone individuals to organized hacker groups, criminal syndicates, violent extremist organizations, and sophisticated nation-states. All pose a danger of increasing their ability to disrupt the networks or critical infrastructure we count on to operate and conduct missions, and advancing their techniques to exploit our people and information. Others are seeking more disruptive or potentially destructive capabilities to impact our freedom to operate and our national security. Collectively, these threats create a dynamic and dangerous cyberspace environment.

Daily there are thousands of attempts to penetrate Army networks. Each Army computer faces multiple unauthorized attempts a day to penetrate Army networks. End users remain our most vulnerable link. Every time Army Soldiers and Civilians enter the network, regardless of where they are, they must recognize they're in a contested environment. Everyone must be aware of the cyberspace threats and remain vigilant against them.

**Defense of All Army Networks**

Army Cyber Command's primary focus is to secure and defend all Army networks. Serving as the Army's service component to USCC has provided unprecedented unity of effort in defending DOD and Army networks. Their ability to stop threats before entering our networks has added to an integrated, defense in depth.

Over the past 22 months, Army Cyber Command has blocked more than 400,000 attempts by individual internet protocol addresses to gain unauthorized access to Army networks; 4,000 known bad/malicious websites; 400 email phishing campaigns from accessing Army computers. On average, we block 64 million internet protocol addresses and 4,500 web sites daily and add more to the list weekly.

Enterprise Email transition continues, with more than 330,000 Army e-mail accounts completed. Common Access Card users will authenticate and access email services from centralized DOD data centers, and connect from anywhere in the world. This service provides a single identity, with a single internet protocol address, increasing effectiveness and strengthening the security of our networks.

Our work on compliance has improved Information Assurance, reduced vulnerabilities, and mitigated risk to operations. Our Web Risk Assessment Team scanned over 10,000 documents for cyberspace threats on Army web pages, while our education and leader outreach reduced the number of cross domain violations by 50 percent. Additionally, through a comprehensive approach, and implementation of a wide range of initiatives we increased the security of the Army Knowledge Online (AKO) website.

We continue to implement and leverage the capabilities of Host Based Security System (HBSS) on Army computers to better protect the individual at the end point system, and supports consistent implementation of DOD security policy on all computers. HBSS is critical to maintaining network security, and addresses current network vulnerabilities to prevent intrusions.

Knowing what's happening across all Army networks is vital to the Army's cyber ability to operate and defend our networks. While our asset visibility is increasing, our need for increased situation awareness and a common operating picture (COP) is essential. Fed by real-time network systems data and indications and warnings, an effective COP would allow us to act, react, and counteract at network speed, while conducting informed active defense operations. We continue collaboration with USCC, NSA, and key partners to unify research efforts and combine operational data with intelligence on Army systems to increase our cyberspace situational awareness.

The Army Cyber Defense in Depth strategy (Active Defense) facilitates a clear identification and prioritization of key cyber terrain, including physical and logical infrastructure and mission data. The strategy employs three overarching strategic objectives to protect key cyber terrain: Protect, including Defense of the Global Information Grid Operations (DGO) and Information Assurance (IA) measures; Defend, including passive Defensive Cyber Operations (DCO) organized around the deployment of perimeter and key terrain focused sensors, firewalls, and various host-based security systems and programs; Hunt, consisting primarily of active DCO utilizing advanced "active" sensors and rapid response actions. We continue to increase our capacity and capability to conduct each objective and our efforts will remain synchronized with the transition to the DOD Joint Information Environment (JIE).

**Title 10 Responsibilities to Organize, Train, and Equip for Cyberspace Ops**

As the Army's service component to USCC, Army Cyber Command exercises the designated command and control authority and responsibility over trained and ready Army forces, as delegated by the Secretary of the Army and the Commander, USCC in support of his global mission. Additionally, Army Cyber Command, when directed, will serve as Joint Force Cyber Component Commander/Joint Task Force-Cyber.

**Organized for today and moving to the future**

Army Cyber Command is organized as the Army's single operational level force with the major functions required to conduct our stated mission. Daily, we provide trained and ready forces to USCC support the execution of their mission. We have completed a wide range of work and continue to pursue other initiatives to better train, organize and equip the Army to conduct operations in cyberspace today and in the future. We are nested with the USCC mission and their three lines of operation--operate and sustain DOD information networks, defensive and offensive cyber operations. The command remains focused on providing an Army cyber force capable of meeting USCC and combatant commanders' requirements in support of national and operational objectives, and in support of Unified Land Operations, to ensure U.S./Allied freedom of action in cyberspace.

Unity of effort and unity of command is essential in the cyberspace domain. Since activating the command, other organizations have been placed under the operational control of Army Cyber Command. The Army's Network Operations Security Centers and our Regional Computer Emergency Response Teams are now part of the command, increasing the unity of command for the operation and defense of our networks. Additionally, Reserve Component cyber and information operations organizations are now under our operational control.

The most significant organizational milestone occurred on December 1, 2011 when the Army activated its first dedicated cyber brigade at Fort Meade, Maryland. The 780th Military Intelligence Brigade (780th MI BDE) (Cyber) is organized to support USCC and combatant command cyberspace operations. Army Cyber Command has operational control of the brigade. This brigade conducts signals intelligence and computer network operations, and enables Dynamic Computer Network Defense of Army and Department of Defense networks. When fully staffed, the 780th MI BDE will have more than 1,200 assigned Soldiers and civilian employees.

Additionally, Army Cyber Command is organized to provide dedicated information operations (IO) and cyberspace integration support to the Army and other Military Forces through the 1st IO Command and mobilized forces resident in the four Reserve Component Theater Information Operations Groups. These organizations deploy IO and cyberspace support teams; provides IO and cyberspace planning, analysis and technical reach back; and offers specialized IO and cyberspace training to assist the warfighter in garrison, during exercises, or in conflict. This support includes conducting IO and cyberspace operations planning, preparation, execution and assessment of the information environment; identifying IO and cyberspace vulnerabilities; leveraging IO and cyberspace intelligence analysis; and conducting training in IO and cyberspace operations to improve a unit's ability to successfully operate throughout the information environment. We have organized and deployed support teams to provide IO support to numerous Overseas Contingency Operations, exercises, and operations worldwide. We have also trained over 1,600 students in multiple information operations and cyberspace courses.

Army Cyber Command's robust and active involvement in assessments, wargames, and exercises with USCC, other combatant commands, and the Army, coupled with the results of the Training and Doctrine Command (TRADOC) *Cyber/Electromagnetic Capability Based Assessment* identified gaps in our ability to conduct cyberspace operations. In FY14, we will increase our capacity and address the following gaps: increase our World Class Cyber Opposition Force (WCCO) capacity to provide realistic, challenging cyberspace training in the conduct of Unified Land Operations to exercises, Home Station Training, and Combat Training Centers; increase our capability to conduct active defense of Army Networks through "Hunt Teams" that can find, fix, and mitigate currently un-detected malicious actors already inside the DoD infrastructure; provide capability to integrate cyberspace operations into Regional Army Land operations to support commanders' tactical and operational cyber planning and integration; increase intelligence personnel to support Army Cyber Command's operations Center, and improve our capability for rapid development of network defense tools; increase capacity to conduct our ability to conduct force modernization for cyberspace operations by developing requirements and solutions.

Army Cyber Command is working with the Reserve Component to identify capability gaps in support of Army Cyberspace Operations. Reserve forces will play a critical role in cyberspace operations for Homeland Security and defense of critical infrastructure.

**Training for today and tomorrow**

Strong training, leader development, and education programs are critical to operating in the cyberspace domain. This requires robust individual and collective programs to protect the force, conduct cyberspace operations and ensure mission accomplishment.

Everyone must increase their basic cyber awareness and the Army continues to conduct training to better protect our people from cyberspace threats. Army Soldiers, leaders and commanders must increase their understanding of cyberspace threats, vulnerabilities, and capabilities. Leaders must understand the operational impact, the risk and what they must do to mitigate their risk to ensure they maintain the freedom to operate in cyberspace and are able to leverage cyberspace to help achieve their objectives. We continue to increase cyberspace operations training in key Army leader education programs. As the cyberspace operations doctrine continues to develop, we will adjust our leader development programs.

In support of collective training and to prepare commanders and units for the cyberspace challenges they will operate in, we established and are employing a World Class Cyber Opposing Force (WCCO) at the National Training Center and in support of COCOM exercises. This realistic training allows commanders to see if they can defend against threats attempting to penetrate their network and increase their ability to operate in a contested and degraded cyberspace environment.

Our integration with USCC and sister service cyberspace components in support of exercises is robust. Army Cyber Command has doubled their participation in USCC, combatant command, and service exercises each year. We will integrate cyberspace operations into 13 Joint and Army exercises this FY, and will double that number next year. In addition to the WCCO we are providing Expeditionary Cyber Support Elements to combatant command and Army exercises, in order for commanders to plan, integrate and conduct cyberspace operations, with their operations.

As the Army finalizes Army Training Strategy 2013, training to conduct cyberspace operations will be a key component, to ensure we train as we fight. The training support system requires an integrated training environment with the right mix of live, virtual, and constructive capabilities to enable realistic cyberspace training to meet commander's training objectives.

**Equipping to Conduct Cyberspace Operations**

The Army has a wide range of capabilities being leveraged everyday to operate, defend and support offensive operations. We continue to respond to USCC and combatant commanders' requirements and have rapidly produced capabilities to support missions.

In order to attain and maintain cyberspace superiority, it is essential that we maintain an agile and responsive cyberspace acquisition process to provide required materiel solutions to operational requirements that keep up with the speed of change and stay ahead of potential threats.

Our research and development efforts are nested with DOD science and technology priorities, and we're working with key elements of Army Materiel Command, Defense Advanced Research Project Agency (DARPA), Federally Funded Research and Development Centers (FFRDC), and industry partners to provide a wide range of capabilities that assure effective missions, provide resilient infrastructure, support agile cyberspace operations, and are built on foundations of trust. Increasing our situation awareness and developing a defensible architecture that serves as an operational platform to the tactical edge for cyberspace operations are key efforts.

Through Network Integration Events (NIE) coupled with the Brigade Modernization Command (BMC) at Ft Bliss, the Army is fundamentally changing how it develops, tests and delivers networked capability to its operating force. This provides an opportunity to address capability gaps and insert new technologies into a robust operational environment to ensure they perform as required and create no cyberspace vulnerabilities.

The critical effort is to achieve a Joint Information Environment which provides a defensible architecture and an operational platform that enhances our ability to conduct cyberspace operations.

**Recruit, Develop, and Retain a Cadre of Cyber Professionals**

While technology plays an important role in the cyberspace domain, it is not technology that will win on the 21st Century's cyberspace battlefields. A team of elite, precise, trusted, and disciplined cyberspace professionals able to quickly act across the full range of mission sets is who will make the difference.

To meet today's and tomorrow's threats, we must recruit, develop and retain skilled, professional Soldiers (active duty and reserve component), Civilians and contractors who can meet future challenges and dominate the cyberspace terrain. However, our success requires a

highly skilled technical workforce that both government and private industry are competing for. We need to create a deeper national pool, while we develop the cyber skills we need now.

The Army's Military Intelligence (MI) and Signal Center (SC) Centers of Excellence (COE) are in the process of creating and revising skills that will better develop our cyber force to conduct cyberspace operations. In concert with this, they are reviewing and providing incentives, updating career development opportunity, and pursuing ways to retain these key skills.

The Army has created the 255S (Information Protection) Warrant Officer MOS. This specialty has been approved and trained warrant officers are now entering the Army inventory. We have also created the 35Q, Cryptological Network Warfare Specialist, and recruitment of Soldiers with a variety of incentives will begin this October. Additionally we have created new Additional Skill Identifiers for key cyber areas and are working to implement concepts for the development of new Areas of Concentration (AOC) focusing on Cyberspace Networks Integration as well as efforts to consolidate network engineering and information systems functional areas. A new enlisted MOS 25D, Cyber Network Defender, will be created and will start at the rank of Staff Sergeant.

**Army Cyber Command Initiatives**

Operational Planning and Critical Infrastructure Protection

Integrating cyberspace operations into planning is vital. Army Cyber Command planners and analysts are providing cyberspace operations planning and targeting support to USCC and Combatant Commanders to accomplish operational cyberspace effects. We're working to incorporate cyberspace and information capabilities into all contingency and crisis action plans. A key initiative includes leveraging existing plans developed by Headquarters, Department of the Army under their Force Protection and Antiterrorism Programs. We've built cyberspace operations into the Army's Critical Infrastructure Risk Management Program with the objective of identifying, assessing and reducing risk to the Army's critical assets beyond the conventional 'guns, gates and guards' approach. We're working with the Corps of Engineers to provide them the requisite cyberspace expertise to improve protection of their critical civil works infrastructure. Additionally, we're engaged in collaboration with Army Materiel Command and Installation Management Command to increase the security posture of Army owned Industrial Control Systems and Supervisory Control and Data Acquisition systems on Army installations.

Building Partner Capacity

We're building relationships with key allies and partner nations through operational planning and Theater Security Cooperation efforts, and supporting the development of combatant command and Army Service Component Command plans worldwide. We've completed our Theater Security Cooperation Strategy, which focuses on building partner capacity, enabling stability and security in the future cyberspace environment. By forging strong relationships with a variety of partners we are strengthening our collective cyberspace security and improving interoperability. Working closely with our allies and partners will promote better collective self-defense and present a collective deterrence while enabling the U.S. military to extend its ability to defend the Nation at home and abroad.

Building a Constellation of Cyberspace Partners

Army Cyber Command is leveraging existing Army processes to enhance a network of government, academia and industry partners with expertise in cyberspace. We are working closely with the United States Military Academy, Army Research Lab, and other partners to leverage intellectual capital and address our most significant challenges. We have also increased our investment in internships and fellowships, in scholarships with opportunities for advanced degrees, and in training with industry. Also, we are developing outreach programs through Science Technology Engineering Math (STEM) vehicles with academia.

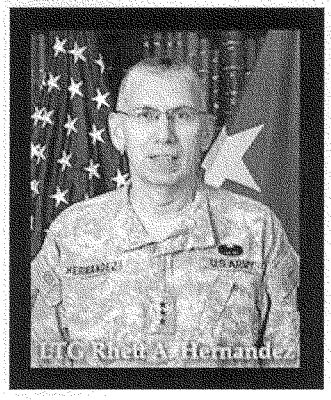
**Conclusion**

For a command built around technology, it's important to understand people are Army Cyber Command's most valuable asset. Cyberspace operations require a world-class cyberspace force able to operate effectively today and in the future. Developing a robust cadre of cyber warriors is a top priority to ensure we maintain the advantage in the highly contested cyberspace domain.

Army Cyber Command has made great progress and will continue to remain trained and ready to ensure our forces maintain our freedom to operate. We're focused on providing a professional team of elite, trusted, precise, disciplined cyber warriors who defend our networks, provide dominant effects in and through cyberspace, enable mission command, and ensure a decisive global advantage. We provide depth and versatility in cyberspace to the joint force, and with our cyberspace capability we're providing options and flexibility for commanders and national decision makers to ensure the Army remains America's Force of Decisive Action, and Army Cyber Command remains, "SECOND TO NONE".

U.S. ARMY CYBER COMMAND / U.S. 2ND ARMY

ARMY CYBER




# LTG Rhett A. Hernandez

Lt. Gen. Rhett A. Hernandez was commissioned as a second lieutenant of Artillery from the United States Military Academy, West Point, New York on 2 June 1976.

His commands have ranged from the Battery level with 2nd Battalion, 33rd Field Artillery and 1st Battalion, 5th Field Artillery to Battalion level with 1st Battalion, 14th Field Artillery, later redesignated 3rd Battalion, 16th Field Artillery to Brigade level command as the Commander of Division Artillery, 4th Infantry Division (Mechanized), Fort Hood, Texas. He also served as the Assistant Division Commander (Support), 1st Armored Division, United States Army Europe and Seventh Army, Germany and OPERATION IRAQI FREEDOM, and the Commanding General, United States Army Human Resources Command, Alexandria, Virginia. His current assignment is as the Commanding General, U.S. Army Cyber Command / Second Army at Fort Belvoir, Virginia.

In addition to his command time, Hernandez has also served in numerous key staff assignments to include Strategic Planner, Officer Personnel Management System (OPMS XXI) Task Force, Alexandria, Virginia; Chief, Operations Division, J-39, The Joint Staff, Washington, DC; Director, Officer Personnel Management Directorate, United States Army Human Resources Command, Alexandria, Virginia; Chief, United States Military Training Mission Saudi Arabia, United States Central Command, Riyadh, Saudi Arabia and Assistant G-3/5/7, United States Army, Washington, DC.

Hernandez holds a Bachelor of Science degree from the United States Military Academy, a Masters of Education degree in Systems Engineering from the University of Virginia, and a Master of Science degree in National Security and Strategic Studies from the National War College, Fort Leslie J. McNair, Washington, D.C.

Hernandez' awards and decorations include the Distinguished Service Medal (2nd Award), Defense Superior Service Medal (2nd Award), Legion of Merit (2nd Award), Bronze Star, Meritorious Service Medal (5th Award), Army Commendation Medal (5th Award), Army Achievement Medal (2nd Award), Combat Action Badge, Joint Chiefs of Staff Identification Badge, and the Army Staff Identification Badge.

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE
ARMED SERVICES COMMITTEE

STATEMENT OF

VADM MICHAEL S. ROGERS

COMMANDER, UNITED STATES FLEET CYBER COMMAND

BEFORE THE

EMERGING THREATS AND CAPABILITIES

OF THE

HOUSE ARMED SERVICES COMMITTEE

ON

25 JULY 2012

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE
ARMED SERVICES COMMITTEE

Chairman Thornberry, Ranking Member Langevin and distinguished members of the Subcommittee, thank you for the support of our military. I appreciate the opportunity to appear before you today with my counterparts from the other military services and to discuss the United States Fleet Cyber Command and U.S. TENTH Fleet.

Mr. Chairman, I have been in command of U.S. Fleet Cyber Command and U.S. Navy TENTH Fleet for just under a year. As the Navy's Component Command to United States Cyber Command, and an Echelon Two Command, subordinate to the Chief of Naval Operations, Fleet Cyber Command directs cyberspace operations in defense and support of Navy and Joint forces to deter and defeat aggression while ensuring freedom of action. Since my predecessor, VADM Barry McCullough, testified before this Subcommittee last September, the Department of Defense and the Navy continue to mature cyberspace operations by growing the workforce, exercising our process, and developing the capabilities that support those operations. This progress is, and continues to be, guided by the *DOD Strategy for Operating in Cyberspace*. I would like to take this opportunity to highlight a few areas of progress over the past year and some of the challenges that we continue to address.

*Operations*

The Department of Defense and the Navy have made significant strides in our ability to conduct cyberspace operations. It has been an iterative process and we will continue to refine our concepts and doctrine as necessary, but there are two major achievements that I would like to bring to your attention. First is the Transitional Command and Control Concept of Operations which was approved by the Secretary of Defense this past May. This CONOPS provides geographic Combatant Commanders and the Services a standard baseline for executing cyberspace operations by documenting Joint Cyber Center and Cyber Support Element command

relationships, missions, functions, and tasks. It also serves as a common starting point for assessing and refining cyber command and control in the future. For its part, the Navy is working closely with U.S. Cyber Command and the other Services to implement and assess this transitional command and control framework. The second item that I would like to highlight is the initial U.S. Cyber Command Operational Directive 12-001 that was issued to each of the Service Component Commands this past April. This Operational Directive specifies standard tasks and mission responsibilities for each of the Service Components, providing initial insight into how U.S. Cyber Command intends to use the Service Components in the planning and execution of cyberspace operations. This in turn, provides a foundation for generating Navy planning and resource requirements. Both of these efforts provided much-needed initial guidance and the Navy will continue to support U.S. Cyber Command and collaborate with the other Service Component Commands to continually assess and refine lines of effort as cyberspace operations evolve.

The Navy's support to Joint and Navy exercises is a critical element to our continual improvement of cyberspace operations. These exercises provide an invaluable opportunity to test our capabilities and identify areas of improvement across the six military functions of Command and Control, Intelligence, Fires, Movement and Maneuver, Sustainment, and Protection. U.S. Pacific Command's Terminal Fury 2012 is one such example that allowed us to exercise cyberspace operations as part of a larger joint operation. The lessons learned from this exercise, and those like it, directly inform the development and refinement of doctrine and tactics, techniques, and procedures. In addition to Joint exercises, U.S. Fleet Cyber Command conducted war games and tabletop exercises to continue to refine Service-level tactics, techniques, and procedures. However, as my predecessor has stated, cyberspace is a man-made

domain and is continually changing. We cannot rest on our past success or recent progress; we must continually exercise and refine our cyberspace operations to keep pace with the evolving threat. Moreover, building and sustaining a highly capable cyber workforce is critical to our operations. Navy initiatives, such as the ongoing Cyber Wholeness Review, will define areas of concern so the Department of the Navy can align resources efficiently to the challenges identified in the cyber domain.

Additionally, the Navy continues to take steps to strengthen our cyber capability afloat through aggressive cyber inspection programs, assist visits, and the use of Navy evaluation teams. Prior to deployment, Navy afloat commands and cyber systems are groomed and assessed for compliance with Department of Defense information assurance requirements. These systems and their operators are evaluated at-sea by Navy teams who further probe cyber systems using tactics, techniques and procedures that potential threats may employ against our forces. This ultimately results in increased cyber readiness across the maritime domain to address the ever changing cyber environment.

*Workforce*

The Navy's workforce is perhaps our greatest strength in this emerging discipline. Our Sailors and civilians are at the forefront of advances in cyberspace operations for the past several years in the Navy and Joint community. However, the recruitment, development, and retention of a highly capable cyber workforce remain a significant challenge, given the rapidly evolving nature of cyberspace and the intense competition from industry for top talent. Over the past year, the Navy has made significant strides establishing the necessary policy, incentives, and training to recruit, develop, and retain a highly capable cyber workforce.

We have several efforts underway to enhance recruitment of individuals with critical cyber warfare skill sets by building awareness of Navy cyberspace operations and associated career options. The U.S. Naval Academy established a summer intern program with the Navy Cyber Warfare Development Group, enabling midshipmen to gain exposure to a wide range of cyber activities over a six week period as part of their summer training. A similar program was established for Naval Reserve Officer Training Corps midshipmen with computer-related curriculums that allow them to attend the Navy Cyberspace Defense Operations Command for their First Class summer cruise. Additionally, the Navy established the Cyber Warfare Engineer career field enabling direct accessions for a few recent college graduates each year with deep cyber-expertise. These Cyber Warfare Engineers will apply the principles and techniques of computer science and computer engineering to research, design, develop, test, and evaluate software and firmware for computer network attack, exploitation, and defense in cyberspace operations. Our biggest roadblock to maintaining a highly skilled workforce is competition with industry as well as other government agencies demand signal for technical experts. While the Navy cannot compete with the compensation offered by industry, we provide individuals with unique opportunities that they cannot receive out in industry and the highly motivated Navy cyber workforce is opting to stay Navy at record levels. Building awareness of those opportunities early on is central to our recruiting efforts.

Developing and maintaining cyber expertise is another critical focus area for the Navy and the broader Department of Defense. To meet the Operational Commanders' requirements we need a training model that has the ability to rapidly adapt to external innovations and evolving threats. We have supported Department of Defense, U.S. Cyber Command, and Department of the Navy efforts to establish the necessary standards for professional development

and continuous learning that provide the foundation for an effective training model. We incorporated these standards into the implementation of a tiered cyber training strategy for the Navy workforce that tailors cyber training based on an individual's roles and responsibilities. The first tier focuses on building cyber awareness across all users on cyber threats and the role of cyberspace in naval operations. The second tier is tailored towards leadership and focuses on their responsibilities for Navy networks and building accountability for the application of offensive and defensive cyber capabilities. The third tier is designed to build a professional cyber workforce, ensuring they develop and maintain the expertise necessary to conduct effective cyberspace operations across the full range of military operations. As part of this strategy the Navy is implementing an adaptive end-to-end approach that includes both formal and informal training throughout one's career. We will employ a flexible training delivery model that includes traditional schoolhouse training that will be augmented with training through a virtual environment. This will enable our Sailors and civilians to stay up to date on the latest threats and technology advances while mitigating cost and the loss of key personnel from units for an extended period of time. In addition, The Navy Cyber Manpower 2020 Task Force has been established to plan and execute the steps necessary to develop a comprehensive near to mid-term cyber manpower strategy based on the results of the recently completed Navy Cyber Manpower Zero Based Review (ZBR), validated operational requirements and a properly aligned and focused Navy force posture that is supported by a prioritized POM resourcing submission across the Future Year Defense Plan (FYDP). This workforce effort will be in phases and include defensive and offensive cyber operations for all officers, enlisted and civilians. It will include partners in industry and other agencies and will reflect a new force balance of organic

and situational alliances. The final phase will address the workforce focused on cyber capabilities embedded in warfighting systems.

*Strengthening our Networks*

To reduce the attack surface exposed to criminals and our adversaries, the Navy engaged in a comprehensive campaign to achieve shore network consolidation and modernization by terminating all Navy legacy networks by 2014. This is being accomplished either by consolidating those networks and applications into a standard Navy Enterprise Solution or by terminating the capability as being no longer needed. Since early 2007, over 1000 Navy shore-based networks have been terminated, and those allowed to remain are being brought under strict standards for security and operations under the central command and control of US Fleet Cyber Command. This improves our aggregate security posture, streamlining our network command and control, and delivers cost efficiencies.

The Navy has emphasized cross-communication between our large network programs, Next Generation Enterprise Network (ashore) and the Consolidated Afloat Networks and Enterprise Services (afloat). Common standards and architecture will deliver a consistent operational environment that works to reduce inefficiencies in operations, training, maintenance, and life cycle support costs that come from specialized, one of a kind, technical solutions. Because networks are closely linked with our combat systems, synchronization of new capabilities must be worked in great detail across all the Navy's Systems Commands.

The Navy is also actively engaged in the developing concepts of a Joint Information Environment which will be comprised of information technology infrastructure and enterprise services. This effort is expected to improve mission effectiveness, increase security, and realize IT efficiencies across the Department of Defense. Over the past year we have supported multiple

pilot efforts that will help shape and inform the development of the Joint Information Environment. Additionally, the progress we have made in developing the Next Generation Enterprise Network and the Consolidated Afloat Network Enterprise Services informed the development of the Joint Information Environment. This includes Navy's efforts in network consolidation, identity management and access control, data center consolidation and enterprise services. As we continue to move forward, we will ensure that the Navy's efforts remain aligned and supportive of the Joint Information Environment.

The investments we have made in network consolidation and deployment of enterprise services have already provided the Navy with greater situational awareness of our networks. This includes near-term insight into the health of our networks as well as long-term trend analysis of attack, sensing, and warning data to detect more discrete cyber threats and irregularities. For example, The Navy's Computer Network Defense Service Provider has just completed development of a capability to allow operators to visualize enterprise level data to identify trends specific to a region or area of operations. The Navy's improvements in cyber situational awareness have begun to improve the efficiency and effectiveness of our operations and enabled us to provide U.S. Cyber Command with a more complete picture of Navy Networks.

In addition to network consolidation and enhancing situational awareness, the Navy continues to make strides in enhancing our network defense capabilities, particularly in our tactical environment at sea. A critical component of this effort was the deployment, operation and maintenance of the Host Based Security System, or HBSS. The Navy has significant challenges in terms of the sheer number of HBSS servers that it must deploy in order to account for every shore and afloat unit. Despite this challenge the Navy achieved 100% deployment of

HBSS across the SIPRNET enclave and is in the process of deploying HBSS across the NIPRNET afloat enclave.

While we have made significant progress enhancing our networks and their defense, we must remain agile. Over the past year U.S. Fleet Cyber Command substantially broadened its efforts to identify Navy network vulnerabilities. We assumed ownership for the U.S. Cyber Command inspection program for Navy sites, added an emphasis on personnel network behavior, and doubled the number of Navy sites inspected compared to previous years.

In many cases it is difficult to determine if an open vulnerability could lead to an exploit with negative mission impact. We generally assume that a dedicated adversary would be capable of exploiting open vulnerabilities. We also assume that a clever adversary would wait to use this capability until it would provide a tactical or strategic advantage. The difficulty of trying to determine if an adversary knows about a vulnerability, is capable of exploiting it, and has the will to do so, has led us to focus on a zero-tolerance methodology.

Our biggest challenge is determining which vulnerabilities equate to a credible risk to mission. We find few sites fully compliant, and yet we find few sites that have been compromised or are at serious risk of compromise. The challenge lies in being able to link non-compliance with operational risk. As we move forward, we will continue to refine our inspection methodology to provide greater insight into which vulnerabilities have the potential to have a substantially negative impact on mission accomplishment, and which would have little to no effect if exploited, allowing the Navy to focus limited resources on the most critical areas.

*Summary*

Our success in the maritime domain and joint operational environment depends on our ability to maintain freedom of maneuver and deliver effects within cyberspace, and to

accomplish this, the Navy's workforce needs to be highly trained and possess the skills required to operate in this ever changing environment. To ensure we maintain our edge the Navy will continue to drive advancements in Navy cyberspace operations, and will be guided by the *Department of Defense Strategy for Operating in Cyberspace.* This strategy, combined with the CNO directed Cyber Wholeness Review, scheduled for the late summer; demonstrates the Navy's commitment to Cyber Operations. I believe, based on the ever increasing requirements and diversity of the threat, that it is safe to assume our cost will increase no matter how efficient we become in this domain. I thank you for this opportunity to present the efforts of U.S. Fleet Cyber Command and U.S. TENTH Fleet, and appreciate your support of our Navy and Department of Defense. I look forward to answering your questions.

United States Navy
# Biography

## Vice Admiral Michael S. Rogers
## Commander, U.S. Fleet Cyber Command
## Commander, U.S. 10th Fleet

Vice Adm. Rogers, a native of Chicago, attended Auburn University graduating in 1981, and receiving his commission via the Naval Reserve Officers Training Corps.

Originally a surface warfare officer, he first served as combat information center officer and anti-submarine warfare officer in USS *Caron* (DD 970) from 1982 to1985, participating in operations off Grenada, Beirut and El Salvador, including combat naval gunfire support. Duty on the staff of the Naval Military Personnel Command in Washington, D.C. followed until 1986.

Subsequently designated a cryptologist (now information warfare), he reported to Naval Communication Station, Rota, Spain, in 1987, serving as electronic warfare officer and direct support officer aboard ships and submarines in the Mediterranean and Persian Gulf, and participating in the initial *Earnest Will* reflagged tanker escorts during the Iran-Iraq war. He then served, from 1990 to 1993, on the staffs of Commander in Chief, U.S. Atlantic Command and Commander in Chief, U.S. Atlantic Fleet as head of the Cryptologic Plans, Policy, Programs and Requirements branch.

He next served as the staff cryptologist for Commander, Carrier Group Two/*John F. Kennedy* Carrier Strike Group, conducting operations in the Baltic and as Combined Joint Task Force 120 for Operation *Support Democracy* (Haiti). He became the cryptologic junior officer detailer at the Bureau of Personnel in Washington, D.C., in 1995 and subsequently served as aide and executive assistant (EA) to Commander, Naval Security Group Command from 1997 to 1998 at Fort Meade, Md. Duty as commanding officer, Naval Security Group Activity Winter Harbor, Maine, followed in 1998.

In 2000, he assumed the duties as fleet information operations (IO) officer and fleet cryptologist on the staff of Commander, U.S. Sixth Fleet, embarked in USS *LaSalle* (AGF 3) in Gaeta, Italy. The tour included contingency support to U.S. and North Atlantic Treaty Organization forces in the Balkans as well as Maritime Interdiction Operations in support of Operation *Enduring Freedom*. He reported to the Joint Staff in 2003, and served as head of the Computer Network Attack/Defense Branch, IO division chief, EA to the J3, EA to two directors of the Joint Staff and special assistant to chairman of Joint Chiefs of Staff/director, chairman's action group.

He next assumed duty as the director for Intelligence (J2), U.S. Pacific Command in 2007. Duty as the Joint Chiefs of Staff director for Intelligence followed in September 2009. He assumed his current duties as commander, U.S. Fleet Cyber Command/commander, U.S. 10th Fleet, in September 2011.

*Updated: 13 October 2011*

NOT FOR PUBLICATION UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS &
CAPABILITIES

STATEMENT OF

LIEUTENANT GENERAL RICHARD P. MILLS
DEPUTY COMMANDANT
COMBAT DEVELOPMENT AND INTEGRATION &
COMMANDING GENERAL, MARINE CORPS COMBAT DEVELOPMENT COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

CONCERNING

DIGITAL WARRIOR: IMPROVING MILITARY CAPABILITIES
IN THE CYBER DOMAIN

ON

July 25, 2012

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Introduction

Chairman Thornberry, Ranking Member Langevin, and distinguished members of this Subcommittee, it is an honor to appear before you today. On behalf of all Marines and their families, I thank you for your continued support. We value what this Committee is doing to highlight the importance of cyberspace operations; and the Marine Corps appreciates your support as we collaborate with the other Services to develop our cyber capabilities and workforce capacity to support Department of Defense policies, U.S. Cyber Command requirements, and integrate cyber across the Marine Air Ground Task Force (MAGTF). While we are making great progress, we recognize that the risks are increasing daily.

As the nation's expeditionary force in readiness, the Marine Corps is prepared for all manner of crises and contingencies – including those arising in the cyber domain. We recognize the complex, highly adaptive threats that we face. In the future, as in the past, multiple regional powers and a host of lethal groups will exploit numerous seeds of instability, proliferating increasingly lethal technology and extremist ideology, while leveraging the advantages of networks hidden amongst the population. Marines are prepared to meet these challenges with our Navy, Special Operations, Army, Air Force and interagency partners.

New strategic guidance issued by the President and the Secretary of Defense provides the framework by which the Marine Corps will balance the demands of the future security environment with the realities of our current budget. The guidance calls for a future force that is "agile, flexible, and ready for the full range of contingencies. In particular, we will continue to invest in the capabilities critical to future success, including intelligence, surveillance, and reconnaissance; counterterrorism; countering weapons of mass destruction; operating in anti-access environments; and prevailing in all domains, including cyber." [1] Operating effectively in cyberspace is now a primary mission of the U.S. Armed Forces. The guidance re-validates the Marine Corps' role as America's expeditionary force in readiness – forward deployed and forward engaged, ready to manage all manner of crises and contingencies.

In this evolving strategic security environment, the Marine Corps recognizes that it cannot conduct operations without reliable information, communications networks, and assured access to cyberspace. Ensuring a stable cyber domain means ensuring stability for our weapons systems, command and control, industrial assets, et al. The cyber domain touches every aspect of our operations and must be contemplated at the lowest levels in the Marine Corps planning process. Indeed, Marines have been conducting cyber operations for more than a decade, and we are in a multi-year effort to expand our capacity. Three years ago, the Marine Corps established U.S. Marine Corps Forces Cyber Command (MARFORCYBER). We have made great strides in expanding the capability and capacity of MARFORCYBER, as well as our cyber-related Military Occupational Specialties. We plan to increase our cyber workforce by approximately 700 Marines and Civilian Marines through FY16. Given the fiscally constrained environment and complexity of cyberspace, our approach is focused on increasing capacity for network operations, defensive cyberspace operations, and when directed, offensive cyberspace operations; and through the introduction of planners within our command element staffs to further integrate cyberspace operations into our plans and operations.

[1] *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, White House letter.

Overview

The rapidly evolving events of the past year alone indicate a new constant. Competition for resources; natural disasters; social unrest; *hostile cyber activity*; violent extremism; regional conflict; proliferation of weapons of mass destruction; and advanced weaponry in the hands of the irresponsible are becoming all too common. Marine Corps intelligence estimates rightfully point out that "more than half of the world's population live in fragile states, vulnerable to ruinous economic, ideological, and environmental stresses. In these unstable regions, ever-present local instability and crises will erupt, prompting U.S. responses in the form of humanitarian assistance and disaster relief operations, actions to curtail piracy, stability operations, and the rescue and evacuation of U.S. citizens and diplomats."[2]

In this unpredictable, unstable and uncertain future security environment, there is an emphatic trend in warfare--the dynamic combination of conventional and irregular warfare by state, non-state and criminal threats. The Marine Corps is manned, trained and equipped to continuously adapt to, deter and defeat these adversaries with increasingly discriminating and precise full spectrum operations. Through a comprehensive force structure review, we designed a post-Operation Enduring Freedom force in readiness that counters this hybrid threat, creates options and provides decision space for senior leadership while, when necessary, setting the conditions for a comprehensive joint, interagency and allied response.

As we look to the future, the post-Operation Enduring Freedom Marine Corps of 182,100 is fundamentally different from the current and pre-9/11 force. It draws on a rich history of innovations in irregular warfare but is recast as a scalable crisis response force ready to counter complex irregular, conventional and hybrid threats--and the gray areas in between. We have substantially invested in relevant organizations such as Marine Special Operations; intelligence, surveillance and reconnaissance; communications; partnering; civil affairs; electronic warfare; regionally oriented command and control; information operations; and of increasing importance - cyberspace operations. Task organized with our highly trained line units, these enablers provide versatile, scalable capability for a broad range of missions to include deterrence, counter-terrorism, counter-proliferation, partnering, reinforcement to our allies, humanitarian assistance, and assured access for the joint force under any condition our national interests require.

The Marine Corps will conduct full spectrum cyberspace operations - to include Department of Defense information network operations, defensive cyberspace operations, and when directed, offensive cyberspace operations - in support of Marine Corps Operating Forces, the supporting establishment, the joint force, and combined operational requirements, in order to enable freedom of action across all warfighting domains while denying the same to adversaries. Recent cyber accreditations and readiness inspections validate our network operations command and control processes and procedures. As we transition to a Government owned and operated network environment, the Marine Corps will pursue efficiencies through automation, consolidation and standardization to ensure availability, reliability and security of cyber assets. The Marine Corps has already standardized its security boundary architecture and its implementation on the Marine Corps Enterprise Network (MCEN) and is working with the Joint

[2] *Five Year Forecast: 2012-2017 Assessment of International Challenges and Opportunities That May Affect Marine Expeditionary Forces* January 2012, pg 1.

Information Environment framework to comply with the developing shared security architecture standards. As we assume full control over our network transport and enterprise services, we will collapse remaining legacy networks which reduce our management footprint and costs, while achieving greater compliancy and consistency throughout the MCEN. Underlying all these efforts has been a consistent process development, improvement and enforcement of our Enterprise IT Service Management plan whereby we maintain strict control over network changes while still providing communication and information system services to all users in all mission areas.

In the sections below we describe the strategic, operational and tactical importance of cyberspace operations for the Marine Corps; how we will meet future demands for supporting Marine Air Ground Task Force (MAGTF) operations; and our vision for ensuring a stabile network that is secure, robust and yet flexible enough to support the Marine Corps' role as America's expeditionary force in readiness.

Current Developments

*Cyber Work Force*

The Marine Corps Force Structure Review positions the Marine Corps to respond to the most likely missions while preserving the capability to project punishing combat power when required. The cornerstone of the future Marine Corps rests on the quality and flexibility of our Marines, which allow us to support the joint force commanders' diverse requirements. Our 182,100 Marine Corps represents fewer infantry battalions, artillery battalions, fixed-wing aviation squadrons, and general support combat logistics battalions than we had prior to 9/11. However, it adds cyber operations capability, Marine special operators, wartime enablers and higher unit manning levels—all lessons gleaned from 10 years of combat operations; it is a very capable force.

Cyberspace operations play an essential role in addressing future operations. The future force will include enhanced cyber capabilities enabled by:

- Reorganizing our intelligence collection and exploitation capabilities to enhance readiness by directly linking deployed forces, garrison support, and the intelligence community; and

- Increasing capacity for full-spectrum cyber operations by increasing structure across appropriate MAGTF and Supporting Establishment units/organizations, and by increasing the structure of Marine Corps Forces Cyber Command.

The development of Marine Corps cyber forces is progressing on schedule, with all forces scheduled to be fully manned by FY16.

*Organizations/Units*

MARFORCYBER provides cyber capabilities through its subordinate elements: the Marine Corps Network Operations and Security Center (MCNOSC) and Lima Company, Marine Cryptologic Support Battalion (Lima Company). Together, these units operate, maintain, and defend the Marine Corps Enterprise Network; conduct defensive cyber operations as part of its routine operations as well as offensive cyber operations when directed.

*Network Architecture*

The Marine Corps Systems Command is the Engineering Competency provider for the Marine Corps with the systems engineering expertise across all engineering disciplines - including computer, networking and cyber security to deliver secure tactical and enterprise systems. The Marine Corps Cyber Engineering strategy takes a holistic, enterprise-wide view and is focused on an end-to-end security architecture. The network architecture strategy focuses on designing systems securely from the beginning - during systems engineering development. By ensuring that network defenders understand the network's design, we increase the ability to protect the network.

The Marine Corps has made significant progress in reducing the number of applications across the functional areas.

The Marine Corps Enterprise Network consists of network infrastructure and equipment, and the people and processes that work on and within the network - from forward deployed tactical users, bases and air stations, to Headquarters Marine Corps staff. As we transition from the Navy Marine Corps Intranet network to a Government Owned, Government Operated network, we are implementing enterprise network management processes with associated tools that will permit our Marine Corps Network Operations and Security Center, our Regional Network Operations and Security Centers, and our Marine Air Ground Task Force IT Support Centers to operate and defend the network and provide services in an enterprise construct, while still regionalizing the network for optimal local support and local control during emergencies or crises. Our Next Generation Enterprise Network contract will provide the necessary support for us to achieve full regionalization and ultimately Marine Corps Enterprise Network unification. Our Marine Corps Enterprise IT Services provides enterprise-wide application hosting with the Marine Air Ground Task Force IT Support Centers hosting regional and local applications to better support users. We are currently assessing whether our enterprise-level Marine Corps Enterprise IT Services data center will be designated as a DOD Enterprise Core Data Center so that other DOD users and the Joint Information Environment can leverage it.

The Marine Corps will participate fully in the Joint Information Environment while retaining our service unique capabilities and maintaining control of the Marine Corps Enterprise Network down to the desktop. As Joint Information Environment enterprise services are developed, tested, certified, and accredited for use, we will assess their applicability to our mission and adopt those services that meet our requirements.

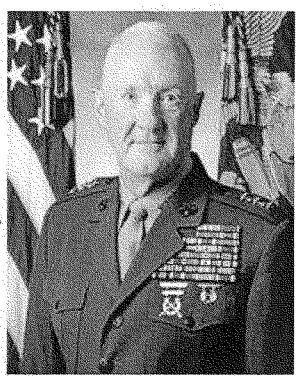
*Current and Future Capability*

The Marine Corps recently conducted a comprehensive Cyberspace Operations Capability Based Assessment (CBA) across all lines of operation (Department of Defense Information Network Operations, Defensive Cyber Operations and Offensive Cyber Operations) to determine our requirements for the full spectrum of cyberspace operations. The Marine Corps Cyberspace Operations Initial Capabilities Document (ICD) prioritizes non-materiel and materiel Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Policy solutions to address identified cyber capability gaps. We are now initiating actions to close these gaps and update the USMC Cyberspace Operations Concept.

Conclusion

We are taking a deliberate and joint approach to cyber requirements; and we continually strive for the right balance in supporting the requirements of U.S. Cyber Command and our Service requirements. We work closely with U.S. Cyber Command to build the necessary mission capabilities, and we will adjust our approach as we learn more about the challenges and opportunities ahead. With the support of the Congress and the American people we can ensure the Marine Corps, along with the other Service components and U.S. Cyber Command, is ready for the current fight and is well prepared to secure our Nation and national interests in an uncertain future. Again, I thank you for the opportunity to discuss cyberspace operations.

# Lieutenant General Richard P. Mills
## Deputy Commandant for Combat Development and Integration



A native of Huntington, New York, Lieutenant General Mills was commissioned via Officer Candidates School. As a Lieutenant he served at the battalion level in two Marine Divisions as a rifle platoon commander, weapons platoon commander, rifle company executive officer, and adjutant. As a Captain he attended Amphibious Warfare School, served at Parris Island as a recruit company commanding officer before commanding Alpha Company, 6th Marines.

As a Major, he was assigned to Headquarters Marine Corps, attended the Marine Corps Command and Staff College, was a Military Observer with the United Nations Truce Supervision Organization in Palestine, and served with Marine Air Group 29, 2d Marine Aircraft Wing.

Lieutenant Colonel Mills served as Operations Officer, 26th Marine Expeditionary Unit (Special Operations Capable) (MEU SOC) taking part in operations off Bosnia and Somalia, was assigned to the staff of the Commander, United States Sixth Fleet in Gaeta, Italy, and as Commanding Officer, 3d Battalion, 6th Marines.

While a Colonel, he studied at the Royal College of Defense Studies, London, England, was the Officer-In-Charge of the Special Operations Training Group, II MEF and commanded 24th MEU (SOC). While under his command the 24th MEU (SOC) participated in Operations Joint Guardian in Kosovo, and combat operations ashore in Iraq as part of Task Force Tarawa.

Colonel Mills served at United States European Command (EUCOM) in Stuttgart, Germany as the Assistant Chief of Staff. Upon selection to Brigadier General, he served as Deputy Director of Operations for EUCOM.

From 2007 to 2009 Brigadier General Mills served as Assistant Division Commander and Division Commander, 1st Marine Division and upon promotion to Major General as Commander, Ground Combat Element, Al Anbar Province, Iraq. Upon returning from Iraq he again assumed command of the 1st Marine Division and then was selected to command the I Marine Expeditionary Force (Forward) which deployed to Afghanistan as part of the International Security Assistance Force (ISAF). In June 2010, he assumed command of the newly-created ISAF Regional Command (Southwest) in Helmand Province. Lieutenant General Mills is the first Marine Corps General Officer to command NATO forces in combat. In July 2011 and upon promotion to Lieutenant General he assumed the duties as the Deputy Commandant for Combat Development and Integration.

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

DEPARTMENT OF THE AIR FORCE

PRESENTATION TO THE SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

HOUSE ARMED SERVICES COMMITTEE

U.S. HOUSE OF REPRESENTATIVES

SUBJECT: IMPROVING MILITARY CAPABILITIES FOR CYBER OPERATIONS

STATEMENT OF: MAJOR GENERAL SUZANNE M. VAUTRINOT
COMMANDER, AIR FORCES CYBER (TWENTY-FOURTH AIR FORCE)

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

July 25, 2012

***Introduction***

Chairman Thornberry, Ranking Member Langevin, and distinguished members of the Subcommittee, thank you for the opportunity to represent the exceptional men and women of Air Forces Cyber before this panel. I am proud to lead over 17,000 Active Duty, Reserve, Guard Airmen, government civilians, and contractors delivering cyberspace capabilities around the world for our military forces and our Nation. Air Forces Cyber will celebrate its three year anniversary next month, and from day one our Airmen have been instrumental in cyber operations across the globe. We have made great strides toward normalizing and operationalizing cyber capabilities to match the rigor and discipline of its Air and Space counterparts. The Air Force is working with other Services to develop capable and structured forces to execute Defense Department cyberspace policies, and employ those forces to achieve effects across the full range of military operations. While Air Forces Cyber continues to evolve, one thing remains constant: our Airmen's dedication to the mission and commitment to providing the best capability to our Combatant Commanders and the Nation.

I would like to thank you and your Congressional colleagues for your ongoing support of our military, particularly the support you provide to the members of the Service Cyber Components represented here today. Success in this domain is not possible without the direction of Congressional, Department of Defense (DoD), Combatant Command (COCOM), and Air Force leadership in providing clear guidance and operational imperatives. The Chairman of the Joint Chiefs of Staff, General Martin Dempsey, recently remarked to an audience at Offutt Air Force Base that cyberspace is "our greatest opportunity and our greatest vulnerability." Your support is vital to ensuring this Nation is prepared to take advantage of that opportunity while defending against ever-changing cyber threats.

A strategic discussion on cyber is no longer simply a DoD activity; it is a national imperative. We did not arrive at this point overnight. For many decades, leaders in engineering, cryptology, computer science, information technology, and many other contributing disciplines expanded and then integrated these technologies. Yet although the technical disciplines were varied, the application of cyber now follows a path similar to ground, sea, air, and space in their early inceptions. Akin to the Wright Flyer's relationship to the F-22, mainframes and eventually personal computers were the harbingers of our cyber capabilities. Continued platform

development led to aircraft being used as a ground forces and intelligence enabler during Army Air Corps operations. Similarly, integrated networks enabled the rapid dissemination of information for defense and intelligence operations…but now we recognize that these capabilities are foundational to mission success. Code-breaking and cryptology applied to secure communications foreshadowed today's cyber information assurance and exploitation capabilities. The application of cyber capability to enable or enhance ground, sea, air, and space operations continues to accelerate; but as with airpower, we should similarly expect cyber to emerge as a strategic alternative.

We are at a nexus regarding future cyberspace operations providing for the National Defense. In order for the Air Force to fulfill our commitment to provide Global Vigilance, Reach, and Power, we must do what Airmen have always done -- innovate. To accomplish our goals and to meet the requirements articulated by USCYBERCOM, and in support of the strategic initiatives in DoD's Strategy for Operating in Cyberspace, we have developed three integrated strategies: deliver a robust, defensible, trusted network; operationally leverage cyberspace capabilities; and build and deliver combat power.

***Deliver a Robust, Defensible, Trusted Network***

As you have discussed and are working to address through legislation; cyberspace is not simply the internet; rather, it is a network of interdependent information technologies, including the internet, telecommunications networks, computer systems, and embedded processors. Its use has become ubiquitous and every public, industrial, academic, and military organization expects reliable access. The Nation and our Air Force, working in collaboration with all Services, have increased weapon system performance, extended operational capabilities, and enhanced command and control by leveraging cyberspace. At the same time, we are fully cognizant that our adversaries will continue to use this common ground to steal, compromise, degrade or destroy information, disrupt networks or communications, or deny service. The dynamic nature of cyberspace means that as technology advances and expands, so does our adversaries' ability to exploit and attack. Hacktivists, terrorists, cyber criminals and state-sponsored hackers are active in cyberspace networks across the globe; our military networks are no exception. DoD networks are probed millions of times per day: beyond the defensive contribution of the DoD gateway actions, the Air Force blocks roughly two billion potential threats and denies two million spam

e-mails each week; however, as General Alexander has previously articulated, passive defenses are necessary, but not sufficient. Armed with an understanding of the growing threat to and our dependency on the network, Air Force leaders directed a Service-wide movement to increase defensibility by creating the AFNet Migration and applying a "defense-in-depth" alignment.

In order to create this defensible construct, Air Force Space Command, through its subordinate units at 24th Air Force and the Air Force Network Integration Center, is addressing the limitations resident in the current Air Force heterogeneous network architecture and its underlying technologies. By "heterogeneous" network, we mean there are many variances in hardware, software, and configurations. As the network expands, updating and maintaining various systems becomes problematic. Inevitably, devices are not properly configured and vulnerabilities arise. Very few of these processes are automated, and we have challenges meeting the training and manpower requirements of this heterogeneous network.

The process of moving from this dispersed, installation-managed network architecture to a single, homogeneous and centrally managed Air Force network is called the AFNet Migration, the number one cyberspace initiative in the Air Force. Industry counterparts like AT&T preceded us in this endeavor, applying significant up-front capital and no small measure of draconian change management. Their conclusion, and ours, is that without the initial homogeny, we cannot implement the necessary sensoring and automation to robust and defend network operations at the scale required for a global industry or military operations.

There are many advantages to be gained by the AFNet Migration, with the most important being the opportunity to now increase sensoring and automation and introduce situational awareness. In the U.S. Central Command's Combined Air Operations Center, walls are filled with screens depicting operational status and providing battlefield video feeds for real-time analysis and decision-making. The corresponding cyber information depicting network operational status and enabling real-time analysis does not currently exist, nor was it possible prior to the re-architecting of the AFNet. Operators in the 24th AF's command and control unit manually perform the task of data synthesis after distant-end units enter status information into the system. There is no common operating picture of activity across our networks, making it more difficult to assess and respond to the threat environment. Yet there are innovators; cyber professionals from many career fields who apply capabilities and leverage new tactics,

techniques, and procedures daily to successfully provide mission assurance, threat detection and response, and network operations and defense. The capabilities for sensoring, status monitoring, and automation of operational activities will continue to expand, and so must the capacity elements necessary to reach and execute full spectrum cyber operations globally. Migration to a single architecture provides the opportunity for Air Force-wide network situational awareness -- an awareness that enables robust, defensible and trusted air, space, and cyber operations.

When major weapon systems build cyber technologies into their programs, they often fail to design components to integrate with the Air Force network. Frequently, these systems introduce cyber vulnerabilities into the network and cannot be patched or updated using established capabilities and processes. Networks can't just be the domain of cyber folks; they must be central in development and operation of every weapon system. This requires application and enforcement of network standards for any weapon system that will traverse our network.

In that pursuit, we're striving to increase our awareness of rapid technological advances and best practices through partnerships with academia, industry, sister Services, and government agencies. General Alexander outlined in his recent remarks to the Senate Armed Services Committee that, in his view, there are three key players that make up a cross-government team to mature and implement an effective cyber strategy for the Nation: Department of Homeland Security, Federal Bureau of Investigation, and DoD/Intelligence Community/National Security Agency/USCYBERCOM. Through USCYBERCOM, we have teamed with cyberspace Law Enforcement counterparts, leaders like Mr. Steve Shirley at the DoD Cyber Crime Center and the Air Force Office of Special Investigations to share information on current threats and tactics, as well as leverage their unique forensics expertise. Via Air Forces Cyber, the Air Force participates in the Defense Industrial Base Initiative, an agreement with over 30 industry partners, including many of the larger corporations in this country, to collaborate with the Departments of Defense and Homeland Security to share sensitive threat information and thereby improve the collective cyberspace defense. Moving forward, we will continue to leverage the great capacity and unique capabilities of not only Air Forces Cyber and Air Force Space Command, but also the expertise of Airmen in our Intelligence, Law Enforcement, and engineering development communities.

The Air Force also partners with university and Department of Energy national laboratories. Our collaboration with Lawrence Livermore National Laboratory delivered one of the first network defense systems in the early 1990s. We continue to develop and expand those core relationships today; we are working with Lawrence Livermore to field a network situational awareness capability that can be leveraged by other government organizations. These channels for cooperation increase the flow of information and create a higher level of awareness across all levels of academia, industry and government.

Improving our defensive network posture is not only about changing equipment and infrastructure; it is also about adopting a proactive defense mindset. Instead of waiting until an adversary penetrates our networks to assess our vulnerabilities, we have created specialized teams that search our networks and seek out those vulnerabilities before they are exploited. Major David Neuman, 92nd Information Operations Squadron Commander, led the creation of our first team and the tactics this precision capability employs to identify, pursue, and mitigate threats impacting critical links and nodes. These efforts were tested at the first Cyber Flag exercise last year, fusing cyberspace across the full spectrum of operations against a realistic enemy in a virtual environment. We focus on identifying and defending those interfaces that are essential to mission success. A key facet of this mission is identifying and focusing on a Combatant Command's prioritized "defended asset list," those critical areas that must be able to operate through an attack. In creating these teams, we partnered with U.S. Transportation Command to protect against some of our adversaries' priority targets. As yet a nascent capability, this team may represent one of the most viable missions for expansion.

Proactive defense also reduces the need for human-in-the-loop processes; it is far superior to our current reactive process. When we detect an intrusion attempt, our primary defensive organization, the Air Force Computer Emergency Response Team (AFCERT), identifies the characteristics of that attack and updates our active sensors, which are located at multiple defensive levels within the network, with the "learned" information so they can deter existing threats and repel the next attack using the same method. We formally report all information to the USCYBERCOM Joint Operations Center, and also share information with our academia, industry, and government partners so similar methods of attack can be thwarted across the domain. Our goal is to move away from this reactive process and develop a heuristic capability.

Instead of our operators having to inform the sensors about each new attack attribute, the sensors themselves will recognize and repel similar attack patterns. Automating this process would further allow us to devote capacity to expanding defensive or mission assurance operations.

Previously, we did things for the sake of the network itself as if it were the end objective. Our defensive architecture was deployed to defend critical mission systems, core services and business systems equally. The AFCERT could not easily distinguish critical mission systems from routine business systems at a base. Today, this is changing. The emphasis is on supporting operational missions dependent on cyberspace. The focus is on mission achievement, not solely network performance.

***Operationally Leverage Cyberspace Capabilities***

Cyberspace operations encompass more than the management and configuration of hardware and software. The Air Force can leverage cyberspace to create integrated effects to respond to crises and conduct uninterrupted operations. When we think about cyberspace operations, we tend to compare them to operations in the air, land and sea domains. However, the cyberspace domain is different in one significant way: it is man-made. Mother Nature does not control it, people do. Instead of responding to the environment, we can change it to our advantage and our enemies' disadvantage. This provides us with a myriad of opportunities to develop and provide new capabilities to the warfighter, but at the same time offers our adversaries new avenues of attack if we do not fully understand the environment we have created. The repercussions of this new environment must be considered when developing tools and extending the domain to austere locations.

We have come a long way in changing our priority from network assurance to mission assurance. A great example of our efforts in this area is our support to Remotely Piloted Aircraft (RPA) missions. In order to provide mission assurance, we had to conduct extensive front-end mapping to understand the various links from the U.S. to the overseas flight. We found the system was designed with roughly 180 touch points, many of which are not military-controlled, across several different networks making it critical to establish relationships with commercial organizations. The forward commander of Joint air assets prioritizes the most critical RPA missions, and then our Operations Center identifies links and takes proactive steps to ensure the

availability of key nodes and reinforce failure points along the network infrastructure. We focus our resources on the highest priority of RPA missions to deliver the greatest downrange advantage. This provides a stark contrast to previous net-focused priorities that resulted in equal defense across the network.

In addition to mission assurance, we are engaged in global operations through our role as the Air Force cyber force provider to U.S. Cyber Command. Over the past two years, our units have conducted 17,000 computer network operations in support of Combatant Command and National Agency taskings. We have directly supported U.S. Central Command and U.S. Africa Command objectives to disrupt terrorist command and propaganda efforts. In response to USCYBERCOM and Agency tasking, Air Forces Cyber continues to support U.S. Strategic Command, U.S. European Command and U.S. Pacific Command by providing full spectrum cyber operations.

COCOMs are beginning to recognize cyber as its own element of combat power, rather than viewing it as merely a support function for operations in the other domains. In a recent Operations Directive, the Commander, USCYBERCOM directed that each Service Component engage and conduct mission analysis with aligned Combatant Commands, and while we have found unique requirements and focus in each, the common desire of senior commanders is to have a variety of non-kinetic cyberspace capabilities available so they can integrate those into their planning processes. Cyber capabilities are driving a change in the way we plan, and they require both flexibility and a focused, detailed understanding of the cyber environment. We are leveraging the expertise and integral capability from our Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) counterparts in order to achieve full spectrum mission objectives.

The complexity of the tasks Air Forces Cyber encounters are typically not a limiting factor to engagement, but recognizing and leveraging the necessary authorities to accomplish the mission continues to be a challenge. Recently, we acted upon these authorities after notification by the Federal Bureau of Investigation, through work conducted at the Air Force Office of Special Investigations and the Navy Cyber Defense Operations Command, that multiple Air Force ROTC computers on a single campus had been compromised. Collaborative efforts between Air Forces Cyber and AFISRA units performing incident and attribution analysis led to

the identification of the malware and leveraging that information to defend the Air Force Global Information Grid. Further collaborative investigation identified potential architectural weaknesses through which compromised accounts could be used to access Air Force networks. This broader understanding will allow our cyber engineering and acquisition communities to modify our architecture to mitigate similar types of risks. Additionally, the analytic capabilities of the Rhode Island Air National Guard's 102nd Information Warfare Squadron will be leveraged in the continuing investigation of this incident. These relationships allow the Air Force to engage along non-warfighting avenues and build, scale and deliver capabilities for USCYBERCOM and in defense of the Nation.

***Build and Deliver Combat Power***

A proper foundation is critical to building a strong structure. As articulated in your recent legislation, and by all Service leaders, it starts with early exposure to Science, Technology, Engineering, and Mathematics (STEM). For cyber professionals, the Air Force adds to this foundation with formal training creating the skilled technical workforce required to manage and protect our cyber resources, and facilitate mission users.

A successful STEM program requires collaborations and partnerships with local and national academia and civic leaders. At the high school level, CyberPatriot was initiated by the Air Force Association, through extensive partnerships with the Center for Infrastructure Assurance and Security at the University of Texas in San Antonio, creator of the National Collegiate Cyber Defense Competition, along with Northrop Grumman and other defense and private industry leaders. It has become a premier national cyber defense competition which inspires students toward careers in cyber security and other STEM disciplines. Last year's competition grew to over 1600 teams from schools in all 50 states and 2 U.S. Department of Defense Dependent Schools overseas, and this year's event hopes to redouble that participation. The students gain specialized instruction, industry and government internships and the benefit of realistic application of their newfound expertise in a competitive environment. Major John Picklesimer of our 92nd Information Operations Squadron was an instructor and mentor to the San Antonio-area CyberPatriot team, and we could not have been prouder when that same team placed first at the national competition on defensive principles and campaign planning. At the collegiate level, students compete at the National Collegiate Cyber Defense Competition and

future cyber defenders test their acumen in the National Security Agency's Cyber Defense Exercise. In a separate program, selected ROTC cadets like distinguished graduate and 24 AF's own Captain Mike Stamat, attend the Air Force Research Laboratories' Advanced Course in Engineering summer program that provides aspiring cyber professionals hands-on internships and cyber officer development. In every one of these program, global excellence starts with local commitment and nationwide government, industry and academic collaboration.

In such a dynamic environment, a STEM background is one avenue for continued success; however, the Air Force has also established deliberate processes for training and certification of our cyberspace professionals. Undergraduate Cyber Training is a rigorous six-month program to provide foundational training for new cyber professionals, both officer and enlisted. Mission qualification training provides unit and position-essential instruction. Last month, the Air Force launched a Weapons Instructor Course conducted at the Air Force Warfare Center at Nellis Air Force Base, Nevada. This course will teach our cyber professionals to integrate capabilities across air, space, and cyberspace to deliver precise effects. In an effort to increase Joint capacity, our sister Services have also been invited to participate in future classes.

Intermediate Network Warfare Training, taught by certified and accredited instructors like Capt Matthew Takanen at the 39th Information Operations Squadron, delivers qualified operators that are prepared to serve in a wide range of positions. In a recent visit, I received a brief from Lieutenants Andrew Cook and Stephanie Stanford, two accomplished graduates. Together, they showcased ground-breaking advancements in script writing, programming, and redirecting. They also designed a full scale virtual environment to test cyber capabilities. These cyber warriors are graduating this course with formal qualifications and certifications that less than 6,800 personnel worldwide have obtained.

The pace of cyber means that a member cannot always wait until training is convenient. An initiative from our 3rd Combat Communications Group is our ability to connect expeditionary cyber to the Joint Cyber Operation Range. Senior Airmen Adam Letteer and Douglas Traumer conceptualized and led the proof of concept for this 24/7 user capability to connect to a simulated network. Their innovation dramatically advanced the way we train to defend the expeditionary cyber domain by allowing our Airmen to learn to detect adversarial

probes and malicious activity. This training has been benchmarked and is available to all expeditionary cyber Airmen.

Moreover, this specialized training is then combined with continuing education opportunities, unique to cyber, throughout the member's career. Air Force officers, enlisted and civilians, and as of last year, their Joint Service cyber professional counterparts, can attend Cyber 200 and 300 taught by the Air Force Institute of Technology.

The organized Reserve Corps was formally established in 1948 by the Truman Administration, but it wasn't until 1973 when Secretary of Defense James Schlesinger declared the Total Force concept policy. We have many Guard and Reserve Total Force units assigned to the cyber mission; therefore, we must leverage the Air Reserve Component differently than in the past, enabling associations that allow Guard and Reserve to perform ongoing real-world cyber and related intelligence missions, not merely training scenarios. With the dynamic cyberspace environment, continued engagement is the best way to keep a Total Force prepared to take up the defense of our Nation. That continued engagement with bona fide mission experience becomes real knowledge that our citizen Airmen will take back to their local communities and use to improve the defenses of industry and government. This fuels collaboration between DoD and the private sector, and raises the level of national cyber security.

Within the strategy document titled Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, the Secretary of Defense, The Honorable Leon Panetta, makes clear that cyberspace forces are a key component to the Nation's ability to project combat power. Specifically, "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space." To provide resilient and cost-effective cyberspace capabilities for the Joint warfighter, an innovative rapid tool development process must be accompanied by an acquisition program that reflects an immediate, medium and a long term systems approach.

We continue to require foundational acquisition programs to develop and field large-scale capabilities. However, a factor that hinders the rapid development of cyber capability is the outmoded acquisition practices, policies, and rules that guide cyber acquisition from the top down. The current acquisition system was constructed and optimized to support the acquisition

of large weapon and training systems. These programs are built from requirements that are defined years in advance and remain relatively static throughout the programming process. The end result is the acquisition of outdated equipment and inflexibility that prevents us from adapting leading edge technology while it is still leading edge.

One acquisition innovation involves the Air Force Materiel Command (AFMC) working with Air Force Space Command to establish a center of cyber innovation for rapid acquisition in providing cutting edge capabilities for the Joint warfighter. It expands the innovations achieved by the Research Topic of Interest under Colonel Paul Welch, Commander of the 688th Information Operations Wing by locally partnering with science and technology expertise from the Air Force Research Laboratory and simultaneously joining with their acquisition counterparts like Colonel Chris Kinne, from AFMC in San Antonio, to expand local acquisition authority delegated from the Secretary of the Air Force for Acquisition. A diverse, co-located knowledge set is required to complement the resident cyber development expertise. Lieutenant Colonel Jim Smith leads the Air Force Operational Test and Evaluation Center's presence in this new organization to test and verify the effectiveness of proposed capabilities in an operational environment. This team of acquisition, technical, and operational experts is integrated with the daily operations of Air Forces Cyber and becomes a powerful engine for innovation that greatly increases the Air Force's ability to create and integrate new and innovative technologies.

This rapid acquisition process is facilitating the development of a capability that will increase threat sharing between the multiple layers of our defense-in-depth methodology. Currently, this posture does not allow for timely vertical integration between machine, base, Air Force and ultimately national levels. This capability would allow automatic information sharing on attack methods between these boundaries, even between an individual machine and national systems. The co-location of these experts has also allowed for the development of a common platform that will allow multiple capabilities to be utilized from a standard construct. Instead of using a phone to place a call, a computer to send an e-mail, and a camera to take a picture, a single smartphone can perform all these functions; this common platform will perform the same role for Air Forces Cyber capabilities.

The Air Force culture of innovation continues in Air Forces Cyber. We continue to leverage a new "tech refresh" methodology that focuses on implementing new capabilities rather

than incremental system upgrades. Instead of maintaining an aging "wired" infrastructure, Air Force Space Command and 24th Air Force are pursuing the potential of commercial wireless technology to lower base infrastructure costs and increase situational awareness on critical infrastructure. Entire nations have skipped "wires" and leapfrogged generations of IT, and the Air Force is exploring how to incorporate this rapidly emerging technology to increase our return on network infrastructure investment.

The Air Force has also initiated a "pilot" program for implementing reliable commercial mobile technologies. The application of these technologies will fundamentally change how the Air Force conducts business; however, we are just beginning to understand their operational impacts. The ramifications of security of this new technology must be explored further before a more comprehensive roll-out program can be considered. In our investigation of the feasibility of this technology, the Air Force has driven a change in the commercial vendor space. Instead of receiving disparate functionality from a vendor, we have pushed for increased integration across a broad range of requirements. Recognizing the efforts we have made in this area, the Defense Information Systems Agency initiated a dialogue with our experts and is benchmarking Air Force efforts regarding their task to implement commercial mobile technologies across the DoD.

The Air Force continues to innovate to enhance its capability to extend, operate and defend the cyber domain. As a cyber engineer, Mr. Billy Keith, 5th Combat Communications Group, is a driving force in our network extension development. He has engineered an "always on" solution for expeditionary network devices used to execute cyber operations for contingency response. This architecture will standardize expeditionary communications connectivity while in-garrison in order to automate security compliance and facilitate training. Additionally, this effort will allow each system to maintain a standard configuration regardless of geographic location, significantly reducing the preparation time for deployment. This enhanced capability increases our cyber defense posture and deployed efficiency through improved readiness and response capability.

***Conclusion***

I am extremely proud of the part our Airmen play in defending the Nation in cyberspace at the "speed of cyber," i.e. Mach 880,000. Offensive, defensive and enterprise services are inextricably connected in this domain. We all rely on cyber to be there and we have a personal interest, a corporate interest and a national security interest in making sure it remains available for our use while denying our enemies the ability to use it against us. We have made great advances and will continue to do so…that's our innovative culture as Airmen.

# BIOGRAPHY

UNITED STATES AIR FORCE

## MAJOR GENERAL SUZANNE M. "ZAN" VAUTRINOT

Maj. Gen. Suzanne M. "Zan" Vautrinot is the Commander, 24th Air Force; and Commander, Air Forces Cyber; and Commander, Air Force Network Operations, Lackland Air Force Base, Texas. General VautrinotShe is responsible for the Air Force's component numbered air force providing combatant commanders with trained and ready cyber forces which plan and conduct cyberspace operations. Twenty-fourth Air Force personnel extend, maintain and defend the Air Force portion of the Department of Defense global network. The general directs the activities of three operational cyber wings, two headquartered at Lackland, and one at Robins AFB, Ga., as well as the 624th Operations Center at Lackland.

General Vautrinot entered the Air Force after graduating from the U.S. Air Force Academy in 1982. She has served in various assignments, including cyber operations, plans and policy, strategic security, space operations and staff work. The general has commanded at the squadron, group, and wing levels, as well as the Air Force Recruiting Service. She has served on the Joint Staff, the staffs at major command headquarters and Air Force headquarters. Prior to assuming her current position, General Vautrinot was the Director of Plans and Policy, U.S. Cyber Command, Fort George G. Meade, Md., and the Special Assistant to the Vice Chief of Staff of the U.S. Air Force, Washington, D.C.

**EDUCATION**

1982 Bachelor of Science degree, U.S. Air Force Academy, Colorado Springs, Colo.
1986 Distinguished graduate, Squadron Officer School, Maxwell AFB, Ala.
1989 Master of Science degree, University of Southern California, Los Angeles
1992 Air Command and Staff College, with honors, Maxwell AFB, Ala.
1996 Joint and Combined Staff Officer School, Armed Forces Staff College, Norfolk, Va.
1998 Air War College, by correspondence
2000 National Security Fellow, John F. Kennedy School of Government, Harvard University, Cambridge, Mass.

**ASSIGNMENTS**

1. June 1982 - October 1986, Chief, Operations and Requirement Analysis Branches, Secretary of the Air Force Office of Special Projects, Los Angeles, Calif.
2. January 1987 - July 1989, Program Manager, Command, Control and Communications Systems, Headquarters U.S. Air Forces in Europe, Ramstein Air Base, West Germany
3. July 1989 - July 1990, space systems requirements officer, Headquarters Air Force Space Command, Peterson AFB, Colo.
4. July 1990 - May 1992, Manager, Advanced Space Systems Surveillance Command, Peterson AFB, Colo.
5. May 1992 - June 1993, student, Air Command and Staff College, Maxwell AFB, Ala.
6. June 1993 - May 1995, operations officer, 4th Space Operations Squadron, Falcon AFB, Colo.
7. May 1995 - March 1996, joint requirements planner, Joint Staff, the Pentagon, Washington, D.C.

MAJOR GENERAL SUZANNE M. "ZAN" VAUTRINOT

8. March 1996 - June 1996, student, Joint and Combined Staff Officer School, Armed Forces Staff College, Norfolk, Va.
9. June 1996 - December 1996, joint warfighting capabilities analyst, Joint Staff, the Pentagon, Washington, D.C.
10. December 1996 - November 1997, deputy executive assistant to the Chairman of the Joint Chiefs of Staff, the Pentagon, Washington, D.C.
11. December 1997 - July 1999, Commander, 11th Space Warning Squadron, Schriever AFB, Colo.
12. August 1999 - June 2000, National Security Fellow, Harvard University, Cambridge, Mass.
13. June 2000 - July 2002, Chief of Operations, 14th Air Force; Commander, 614th Space Operations Group; and Director of Aerospace Operations Center, Vandenberg AFB, Calif.
14. July 2002 - June 2003, Deputy Director of Air and Space Operations, Headquarters Air Force Space Command, Peterson AFB, Colo.
15. June 2003 - April 2005, Commander, 50th Space Wing, Schriever AFB, Colo.
16. April 2005 - July 2006, Deputy Director of Strategic Security, Office of the Deputy Chief of Staff for Air, Space and Information Operations, Plans and Requirements, Headquarters U.S. Air Force, Washington, D.C.
17. July 2006 - June 2008, Commander, Air Force Recruiting Service, Headquarters Air Education and Training Command, Randolph AFB, Texas
18. June 2008 - May 2010, Deputy Commander, Joint Functional Component Command - Network Warfare, U.S. Strategic Command, Fort George G. Meade, Md.
19. May 2010 - Dec 2010, Director of Plans and Policy, U.S. Cyber Command, Fort George G. Meade, Md.
20. Dec 2010 - April 2011, Special Assistant to the Vice Chief of Staff of the U.S. Air Force, Washington, D.C.
21. April 2011 - present, Commander, 24th Air Force, Commander, Air Forces Cyber, and Commander, Air Force Network Operations, Lackland AFB, Texas

**SUMMARY OF JOINT ASSIGNMENTS**
1. May 1995 - March 1996, joint requirements planner, Joint Staff, the Pentagon, Washington, D.C., as a major
2. June 1996 - December 1996, joint warfighting capabilities analyst, Joint Staff, the Pentagon, Washington, D.C., as a major
3. December 1996 - November 1997, deputy executive assistant to the Chairman of the Joint Chiefs of Staff, the Pentagon, Washington, D.C., as a major and lieutenant colonel
4. June 2008 - May 2010, Deputy Commander, Joint Functional Component Command - Network Warfare, U.S. Strategic Command, Fort George G. Meade, Md., as a brigadier general and major general
5. May 2010 - Dec 2010, Director of Plans and Policy, U.S. Cyber Command, Fort George G. Meade, Md., as a major general

**MAJOR AWARDS AND DECORATIONS**
Defense Superior Service Medal with oak leaf cluster
Legion of Merit with two oak leaf clusters
Defense Meritorious Service Medal with oak leaf cluster
Meritorious Service Medal with three oak leaf clusters
Air Force Commendation Medal
Joint Service Achievement Medal
National Defense Service Medal with bronze star

**OTHER ACHIEVEMENTS**
2000 Women in Aerospace Leadership Award
2007 Aerospace Citation of Honor, Air Force Association
2007 'Women Worth Watching' Issue, Profiles in Diversity Journal

**PROFESSIONAL MEMBERSHIPS AND ASSOCIATIONS**
Board of Directors, Uniformed Services Benefits Association
2006 - 2008 Board of Directors, Museum of the U.S. Air Force
Advisory Board, The Warrior Tours

**EFFECTIVE DATES OF PROMOTION**
Second Lieutenant June 2, 1982
First Lieutenant June 2, 1984
Captain June 2, 1986

MAJOR GENERAL SUZANNE M. "ZAN" VAUTRINOT

Major May 1, 1993
Lieutenant Colonel Jan. 1, 1997
Colonel April 1, 2000
Brigadier General Sept. 2, 2006
Major General Nov. 2, 2009

(Current as of July 2012)

t

## QUESTIONS SUBMITTED BY MEMBERS POST HEARING

JULY 25, 2012

## QUESTIONS SUBMITTED BY MR. THORNBERRY

Mr. THORNBERRY. One of the main tools you have for defending your networks is something called the Host-Based Security System (HBSS).

a. How has your experience been in implementing this system and what improvements might you recommend for similar programs in the future? b. Have you implemented the necessary tactics, techniques and procedures to maximize the use of this tool? c. What capabilities would you like to see integrated into future generations of HBSS?

General HERNANDEZ. Our experience has shown the technology provides significant host protection from threats, internal and external and will only improve as our operational use matures. Programs of this magnitude require a clear implementation, training, and sustainment strategy to provide resources, people and money and we have worked to close gaps in initial fielding tactics, techniques, and procedures, sustainment training and manning requirements to establish a baseline that will enable us to fully leverage the capabilities of the tool. While we continue to assess our capability gaps, the ability of HBSS to deliver Cyber SA with minimum latency and the capability to develop custom modules to address unique requirements improves our defensive stance. The inclusion of HBSS event data into existing IA/CND processes will further enhance our capability to defend All Army networks.

Mr. THORNBERRY. How are your Services leveraging in-house graduate educational facilities, like the Air Force Institute of Technology (AFIT) or the Naval Postgraduate School (NPS), as well as DOD accredited programs, such as the National Centers of Academic Excellence in Cyber Operations, in order to improve workforce training and education?

General HERNANDEZ. ARCYBER continues to take a holistic approach by leveraging the constellation construct for both training and development to improve workforce training and education. The construct consists of U.S. Government, Academia and Industry elements, each are discussed below in both current and future actions, and will complement each other to provide a more capable workforce.

Currently ARCYBER is leveraging U.S. Government developmental activities and capabilities to take advantage of efficiencies and future requirements. These activities include: The DOD Joint Information Operations (IO) Range, Government Laboratories (such as: Sandia, Army Research Laboratories, Johns Hopkins applied Physics Laboratory, Adelphi, and Aberdeen Proving Ground Cyber Test Laboratory), and continuous coordination with United States Cyber Command, U.S. Strategic Command (USSTRATCOM), and Office of the Secretary of Defense (OSD) Cyber initiatives. Future activities will include increased partnerships with DHS, FBI, DARPA, DOD, and the Intelligence community. Examples of early successes include five USMA faculty and cadets summer internships with ARCYBER through the Advanced Individual Academic Development (AIAD) program. Shortly, ARCYBER will benefit from more than 14 interns from the Army Civilian Training, Education Development System (ACTEDS). Moreover, ARCYBER will be an active contributor to the Service and USG cyber lessons learned programs.

Current Academic developmental activities include: Cooperation with the Air Force Institute of Technology (AFIT) and its Masters Program, and the ARCYBER scholarship program. This program is a two-year, degree-producing program open to regular Army (RA) captains and majors in the maneuver, fires & effects, operations support, and force sustainment branches. Three officers per year pursue a master's degree in cyber security at the University of Maryland (with additional universities to be added). Though we are still assessing how best to integrate and execute the NSA/DHS National Centers of Academic Excellence training, it is a key component of our future training and developing way ahead. We have two students attending the Naval Post Graduate School and ARCYBER will receive three second-year masters candidates in the NSA Information Assurance Scholarship Program (IASP) in the spring of 2013. ARCYBER is continuing to address organizing cyber within the Army e-Learning and Continuing Education Program. For example, ARCYBER supports Civilian Career Program 34's, Information Technology Management, and Cyber Academy Training Framework through partnerships with University of Mary-

land University College (national policy and law), University of Maryland Baltimore County (secure S/W engineering), George Mason University (ethical hacking/analysis) and Carnegie Mellon University (operational security). Future activities will include Senior Service college "Cyber fellows," RAND Cyber Fellowships, and efforts to identify and recruit cyber talent from ROTC programs and the USMA.

Industry is the third leg in training and development. It is critical in providing additional current and future capabilities/requirements as well as leveraging emerging trends and capabilities and will assist in ensuring our DOD programs and in-house educational activities are developed accordingly. Current developmental activities with industry include: Coordination with Defense contractor Laboratories, Training with Industry (e.g. MIT/Lincoln Labs, Lockheed Martin, and Cisco), and participation in trade conferences (e.g. the Armed Forces Communications and Electronics Association [AFCEA] and the Association of the U. S. Army [AUSA]). Future activities will include: Establishing additional industry research partners; Science and Technology (S&T) outreach; Leveraging partner expertise to manage problems; and increased recruiting and cyber training with industry.

Conclusion: A key attribute of the ARCYBER vision is to develop a trained, professional team to complete our roles as the Army Service Component to U.S. Cyber Command; To train, organize, and equip forces; To provide Cyber Education, Training, and Leader Development; and Execute Cyber Proponent functions. The three part constellation approach is our way of getting at the issues of developing a workforce in a dynamic environment. Our approach continues to evolve.

Mr. THORNBERRY. One of the main tools you have for defending your networks is something called the Host-Based Security System (HBSS).

a. How has your experience been in implementing this system and what improvements might you recommend for similar programs in the future? b. Have you implemented the necessary tactics, techniques and procedures to maximize the use of this tool? c. What capabilities would you like to see integrated into future generations of HBSS?

Admiral ROGERS. HBSS is a complex suite of cyber security tools that is a critical element of the Navy's cyber defense posture. Implementing this system throughout the Navy's afloat and shore-based environments has presented unique challenges.

Our primary challenge has been its implementation in the afloat environment. Navy modernization and fielding processes were not developed with today's constantly evolving Cyber threats and vulnerabilities in mind; thus, it can take up to three years to place a new capability onboard an afloat platform. In contrast, updates to HBSS are released by the Defense Information Systems Agency (DISA) every six months. As a result, the Navy continues to lag in installs and updates mandated by United States Cyber Command (USCC). While the Navy has strived to address the problem for our most vulnerable systems and deployed HBSS to Secure Internet Protocol Network (SIPRNET) on all Navy and Military Sealift Command (MSC) platforms in 2011, the complexity of installs, current processes, and funding constraints have delayed installs of HBSS on Sensitive but Unclassified (SBU) IP Data (also known as NIPRNET), which will not be completed before FY14.

In our shore-based environment, the Navy has encountered challenges with scalability of HBSS. Our Navy and Marine Corps Intranet (NMCI) networks are larger than most networks encountered in the private sector, and we have had difficulty configuring HBSS to accommodate larger network environments. While the vendor has responded to technical problems, these issues have challenged the Navy's ability to be fully compliant with USCC orders for installation of HBSS. For any future similar programs, scalability should be a key factor when designing solutions.

The Navy is leveraging HBSS Tactics, Techniques and Procedures (TTPs) developed by USCC and continuing Service-specific efforts to develop additional TTPs. Additionally, we are leveraging best practices within the Service, such as those developed by Naval Air Systems Command (NAVAIR), to better manage HBSS and ensure it meets our operational needs. The Navy also continues to develop Standard Operating Procedures (SOPs) and other documentation and training that aid in operationalizing HBSS to provide actionable and timely information to Cyber decisionmakers and operational commanders. Future capabilities we would like integrated in future HBSS generations should account for legacy hardware/software network environments. Capabilities should also address low-bandwidth operations and upgrade installment flexibility to account for the unique requirements of the U.S. Navy. We continue to work closely with our partners at USCC and DISA to further refine operational concepts, and ensure follow on versions and acquisition efforts take advantage of lessons learned. We remain especially focused on ensuring acqui-

sition efforts and system release schedules are tied closely to operational requirements and are sensitive to operational environments.

Mr. THORNBERRY. How are your Services leveraging in-house graduate educational facilities, like the Air Force Institute of Technology (AFIT) or the Naval Postgraduate School (NPS), as well as DOD accredited programs, such as the National Centers of Academic Excellence in Cyber Operations, in order to improve workforce training and education?

Admiral ROGERS. Navy is leveraging in-house graduate educational facilities and DOD accredited programs through close coordination with these institutions and a focus on a smart post-education placement process to ensure our most recently educated Sailors and civilians are detailed to positions which will benefit the Navy most. We recognize that affording our personnel graduate educational opportunities is critical to maintaining our expertise as we drive advancements in Navy cyberspace operations. With the quickly evolving nature of cyber, it is absolutely critical that the educational partners and programs we leverage keep pace with the changing cyber landscape.

To that end, the U.S. Navy leverages education and training from six major programs:

Air Force Institute of Technology (AFIT) and Naval Postgraduate School (NPS) In 2002, AFIT and the Naval Postgraduate School formed an educational alliance to eliminate duplicate degree programs in the fields of Oceanography and Aeronautical Engineering, and consolidate educational resources. Navy continues its close coordination with AFIT to refine course requirements, explore potential resource consolidations, and improve quality.

NPS

NPS offers an 18-month Master of Science degree in Cyber Systems and Operations that addresses a broad range of cyberspace operations such as computer network attack, defense, and exploitation; cyber analysis, operations, planning and engineering; and cyber intelligence operations and analysis. Navy will graduate 14 officers from this program in FY12 and is programmed to send 14 officers in FY13 per the approved Officer Graduate Education Quota Plan.

NPS's Graduate School of Operational and Information Sciences offers an Information Systems and Operations (ISO) Certificate Program. This warfighter-oriented degree program focuses on integrating information technologies, command and control processes, and Information Operations (IO) methods and elements into innovative operational concepts for IO in the context of Network Centric Warfare. Since the program's inception in 2002, 318 officer, enlisted and civilian personnel have completed this certificate program.

The Information Systems and Technology (IST) certificate program provides an educational opportunity that is essential to helping the U.S. military reach information superiority in the operational environment. It offers advanced education in areas essential to enabling global networked communications, including: databases, systems analysis and design, decision support systems, and network security. Since the program's inception in 2003, approximately 96 officer and enlisted personnel have completed this certificate program. Both programs are taught via asynchronous Web-based media (i.e., the Internet). The asynchronous nature of these certificates has allowed us to deliver these certificates to deployed forces at sea and ashore.

Additionally, NPS will offer a 12-month Enlisted Cyber Master's Degree in September 2012 that provides selected Navy Sailors a Master of Science in Cyber Systems and Operations; Security and Technology. Selectees are assigned to a Navy-funded education program as full-time students under permanent change of station orders to Monterey, CA. Navy is sending five sailors through this program this year.

Finally, NPS just completed the approval process for a resident Master of Science, Network Operations and Technology degree that begins this fall and has eight officers scheduled to attend in 2013.

Masters of Information Technology Strategy (MITS)

In 2010, the Chief of Naval Operations directed the creation of the Masters of Information Technology Strategy (MITS) pilot program in partnership with Carnegie Mellon University (CMU). This program affords civilian and military IDC personnel the opportunity to attend CMU for a 16-month Master's degree program in cyber-related disciplines. The degree conferred is a Master's Degree in Information Technology and Strategy (MITS) and is a cooperative endeavor between of the College of Engineering (CIT), School of Computer Science (SCS), and College of Humanities and Social Sciences (H&SS). The initial cohort of two military and three civilians students commenced August 2011, and the second group of four commenced in August 2012.

National Defense University (NDU)

NDU's Government Information Leadership (GIL) Master of Science is a 39-credit hour curriculum of the GIL Master of Science Degree Program and offers a combination of information management, technology, and leadership intensive courses. Navy currently has 36 Master's degree enrollments and 497 certificate enrollments.

NDU's "iCollege" Chief Information Officer (CIO) Program is the recognized leader in graduate education for Federal CIO leaders and agency personnel. It directly aligns with the Federal CIO Council-defined CIO competencies and addresses the Clinger-Cohen Act and other relevant legislation mandates. It is sponsored by the DOD CIO.

United States Naval Academy (USNA)

Although an undergraduate program, USNA's Center for Cyber Security Studies is an important investment as it enhances workforce education and training at the Service academy level. Established in 2009, the Center provides support for the proposed curricular and professional reforms across the Naval Academy and encompasses support for all programs that contribute to the knowledge, study and research of cyber warfare.

NSA/DHS National Centers of Academic Excellence

National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Information Assurance (IA) Education (CAE/IAE), IA 2-year Education and Training (CAE/2Y) and IA Research (CAE/R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines. Students attending CAE/IAE or CAE/R designated schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program (IASP) and the Federal Cyber Service Scholarship for Service Program. NPS is a participant in this program.

To date, 84 uniformed and civilian Navy personnel have participated in the DOD IASP from commands across the Navy.

Mr. THORNBERRY. One of the main tools you have for defending your networks is something called the Host-Based Security System (HBSS).

a. How has your experience been in implementing this system and what improvements might you recommend for similar programs in the future? b. Have you implemented the necessary tactics, techniques and procedures to maximize the use of this tool? c. What capabilities would you like to see integrated into future generations of HBSS?

General MILLS. a. The Marine Corps had little trouble implementing HBSS as directed by USCYBERCOM. Challenges to the installation of HBSS included anticipating and mitigating the potential impacts that various modules could have on specific applications within the Marine Corps Enterprise Network (MCEN). We recommend that future programs of this type are designed and implementation timelines determined with Service involvement at the earliest stages of development.

b. The Marine Corps continuously strives to improve our Tactics, Techniques, and Procedures in an effort to maximize our defense in depth strategy and enhance our security posture. There is more work to be done in order to realize the benefits of HBSS—we need to train more marines on the various modules and their employment, baseline, and tuning. We need to educate commanders on the benefits of full implementation and utilization of HBSS.

c. The Marine Corps recommends four areas of improvement for HBSS:

(1) HBSS lacks the redundancy provided by other critical IT systems. The capability for production HBSS server suites to mirror each other does not exist. The strength of the HBSS architecture could be greatly improved if clients could seamlessly fail-over between geographically separate servers.

(2) HBSS could be utilized to assist in the Information Assurance Vulnerability Management (IAVM) program by analyzing systems for critical vulnerabilities. Ideally, the DOD HBSS Program Manager could obtain or develop benchmarks within HBSS to detect vulnerabilities of interest published by the IAVM program.

(3) The number of local events logged at the local machine should be pushed up to the enterprise level. Enterprise logging will allow Computer Network Defense Service Providers (CNDSPs) to more effectively respond to incidents and therefore better defend networks. (Examples are of Data Loss Prevention (DLP) which identifies USB usage on DOD Networks and Host Intrusion Prevention System (HIPS) which monitors traffic for anomalies.

(4) We would like to see the continued integration of industry best practice solutions into the management console to provide a single optimized interface for operators. It is also important that the DOD fully employ HBSS and the associated exist-

ing modules. Once those efforts are complete, a true gap analysis can be conducted and specific areas within our network architecture that lack coverage can be identified, addressed, and mitigated.

Mr. THORNBERRY. How are your Services leveraging in-house graduate educational facilities, like the Air Force Institute of Technology (AFIT) or the Naval Postgraduate School (NPS), as well as DOD accredited programs, such as the National Centers of Academic Excellence in Cyber Operations, in order to improve workforce training and education?

General MILLS. The Marine Corps actively participates in the Department of Defense Information Assurance Scholarship Program, which provides access for both enlisted and officer students to AFIT, NPS, the National Defense University, Capitol College, George Mason, and other National Centers of Academic Excellence in Cyber Operations for graduate degrees in cyberspace security, information assurance, and computer security fields.

Through the National Intelligence University, marines with intelligence-related military occupational specialties are able to complete a Master of Science of Strategic Intelligence. Although this curriculum does not include cyber-specific courses as part of the core requirement, students are able to tailor their electives and focus thesis topics to include cyber operations.

The Marine Corps is currently in discussions with Northern Virginia Community College to establish a program to provide college credit for marines receiving military training and experience within the cyberspace operations workforce.

The Marine Corps University has initiated additional curricula in its educational programs that include topics in cyberspace operations, cyberspace planning, cyberspace law, and cyberspace implementation theories. Thus far, the Marine Corps University has had one class complete its program of instruction with this additional material. Initial feedback is that it was well received, and the Marine Corps University is evaluating comments to refine its curricula for future courses.

The Marine Corps also leverages cyber and cyber-related courses through NSA's National Cryptologic Schools for personnel serving at the Marine Cryptologic Support Battalion and the operating forces' Radio Battalions which provide Signals Intelligence and cyber related support to the Marine Air Ground Task Force, USCYBERCOM through MARFORCYBER, and the National Security Agency. Additionally, the Marine Corps uses the U.S. Navy's Joint Cyber Analysis Course (JCAC) and the Joint Network Attack Course to train enlisted marines and officers in cyber and cyber-related skill sets for MOS development.

Mr. THORNBERRY. One of the main tools you have for defending your networks is something called the Host-Based Security System (HBSS).

a. How has your experience been in implementing this system and what improvements might you recommend for similar programs in the future? b. Have you implemented the necessary tactics, techniques and procedures to maximize the use of this tool? c. What capabilities would you like to see integrated into future generations of HBSS?

General VAUTRINOT. a. The Air Force continues to address the challenges of integrating and sustaining HBSS within existing architecture as well as incorporating it within the numerous critical mission systems operating on the Air Force provisioned portion of the Global Information Grid. In addition to the challenges with fixed HBSS implementations, expeditionary environments present additional risks in HBSS employment, such as saturating downrange bandwidth and remaining compliant. HBSS is critical to our Net Defense posture and we will continue to review its fielding, operating, training and sustaining needs.

b. The Air Force has taken significant action to maximize the HBSS capability's effectiveness in increasing the defensive posture of our network and IP-capable assets. We use the capability to generate enterprise-wide situational awareness information, which is critical for enabling and maintaining Command and Control across the network. Expeditionary systems are now deployed with current patches and policies to reduce or eliminate the initial unresponsive period when updates were installed. Additionally, we continue to establish key Net Defense policies, which are implemented across the Air Force and shared with our DOD partners, to defend against active, future and existing threats.

c. The HBSS capability has numerous critical network defense capabilities that can identify existing vulnerabilities and report that information for action to our operators who then must take intensive, manual remediation and mitigation actions. The next step is integrating into HBSS the capability to identify vulnerabilities and executing automatic actions to remediate and mitigate the deficiency. This would increase our capacity to leverage capabilities in support of the Joint fight.

Mr. THORNBERRY. How are your Services leveraging in-house graduate educational facilities, like the Air Force Institute of Technology (AFIT) or the Naval Postgraduate School (NPS), as well as DOD accredited programs, such as the National Centers of Academic Excellence in Cyber Operations, in order to improve workforce training and education?

General VAUTRINOT. Air Force Space Command (AFSPC) and Air Education and Training Command (AETC) have established a full-range cyber training and education construct that begins in Basic Military Training and follows a challenging path that includes specialized cyber-focused graduate degrees.

In addition to cyber-focused graduate programs (MS/PhD) in Computer Science, Computer Engineering and Electrical Engineering with research focused on such areas as encryption algorithms, botnet disruption, network intrusion detection, and wireless network security, AFIT offers two Master's programs in cyber operations and cyber warfare. The 18-month Cyber Operations Master's Program provides extensive hands-on laboratory experience with both offensive and defensive measures and countermeasures, and is open to officers, enlisted, and civilians. The 12-month Cyber Warfare Degree Program for Majors and civilian equivalents provides a developmental education opportunity that addresses technical as well as policy and doctrine aspects of cyber operations.

The Information Assurance Certificate Program (IACP) is a subset of the Master of Science program. Students completing the required coursework are eligible for certificates under National Training Standards as an Information Security Professional, Senior System Manager, and Senior Risk Analyst.

On June 19, 2008, the Secretary and Chief of Staff of the Air Force designated AFIT and the Center for Cyberspace Research (CCR) as the Air Force's Cyberspace Technical Center of Excellence (CyTCoE). The Center serves as a bridge between the operational AF cyber forces and various cyber research, education, and training communities across the Air Force, the DOD, and national organizations.

The Center provides cyberspace professional continuing education for currency and professional development of the cyberspace workforce. The Air Force's Cyber 200 and 300 are Joint-accredited professional development courses designed to increase the depth and breadth of cyber operations understanding and to prepare individuals to apply cyber capabilities and concepts in Joint military operations. These courses are available to and attended by our Joint brethren in an effort to standardize training and proficiency across the DOD. The Air Force is also in the process of establishing disclosure guidance that will allow our international partners to send individuals to Cyber 200 and 300.

The Air Force also utilizes graduate-level educational opportunities offered by our DOD and Agency partners such as the Information Assurance Scholarship Program (IASP) and the Computer Network Operations Development Program (CNODP). The IASP is open to all Air Force officers and is designed to retain a corps of highly skilled IA professionals to accommodate diverse warfighting and mission requirements. The CNODP is an intense, 3-year graduate-level internship at the National Security Agency that develops technical leaders who will lead the DOD and Services' employment of cyber capabilities. Graduates of this program receive focused follow-on assignments that capitalize on their breadth and depth of knowledge.

---

## QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. How are your Services leveraging both in-house graduate educational facilities and DOD accredited programs, such as the NSA/DHS National Centers of Academic Excellence?

General HERNANDEZ. ARCYBER continues to take a holistic approach by leveraging the constellation construct for both training and development to improve workforce training and education. The construct consists of U.S. Government, Academia and Industry elements, each are discussed below in both current and future actions, and will complement each other to provide a more capable workforce.

Currently ARCYBER is leveraging U.S. Government developmental activities and capabilities to take advantage of efficiencies and future requirements. These activities include: The DOD Joint Information Operations (IO) Range, Government Laboratories (such as: Sandia, Army Research Laboratories, Johns Hopkins applied Physics Laboratory, Adelphi, and Aberdeen Proving Ground Cyber Test Laboratory), and continuous coordination with United States Cyber Command, U.S. Strategic Command (USSTRATCOM), and Office of the Secretary of Defense (OSD) Cyber initiatives. Future activities will include increased partnerships with DHS, FBI, DARPA, DOD, and the Intelligence community. Examples of early successes include five USMA faculty and cadets summer internships with ARCYBER through the Ad-

vanced Individual Academic Development (AIAD) program. Shortly, ARCYBER will benefit from more than 14 interns from the Army Civilian Training, Education Development System (ACTEDS). Moreover, ARCYBER will be an active contributor to the Service and USG cyber lessons learned programs.

Current Academic developmental activities include: Cooperation with the Air Force Institute of Technology (AFIT) and its Masters Program, and the ARCYBER scholarship program. This program is a two-year, degree-producing program open to regular Army (RA) captains and majors in the maneuver, fires & effects, operations support, and force sustainment branches. Three officers per year pursue a master's degree in cyber security at the University of Maryland (with additional universities to be added). Though we are still assessing how best to integrate and execute the NSA/DHS National Centers of Academic Excellence training, it is a key component of our future training and developing way ahead. We have two students attending the Naval Post Graduate School and ARCYBER will receive three second-year masters candidates in the NSA Information Assurance Scholarship Program (IASP) in the spring of 2013. ARCYBER is continuing to address organizing cyber within the Army e-Learning and Continuing Education Program. For example, ARCYBER supports Civilian Career Program 34's, Information Technology Management, and Cyber Academy Training Framework through partnerships with University of Maryland University College (national policy and law), University of Maryland Baltimore County (secure S/W engineering), George Mason University (ethical hacking/analysis) and Carnegie Mellon University (operational security). Future activities will include Senior Service college "Cyber fellows," RAND Cyber Fellowships, and efforts to identify and recruit cyber talent from ROTC programs and the USMA.

Industry is the third leg in training and development. It is critical in providing additional current and future capabilities/requirements as well as leveraging emerging trends and capabilities and will assist in ensuring our DOD programs and in-house educational activities are developed accordingly. Current developmental activities with industry include: Coordination with Defense contractor Laboratories, Training with Industry (e.g. MIT/Lincoln Labs, Lockheed Martin, and Cisco), and participation in trade conferences (e.g. the Armed Forces Communications and Electronics Association [AFCEA] and the Association of the U. S. Army [AUSA]). Future activities will include: Establishing additional industry research partners; Science and Technology (S&T) outreach; Leveraging partner expertise to manage problems; and increased recruiting and cyber training with industry.

Conclusion: A key attribute of the ARCYBER vision is to develop a trained, professional team to complete our roles as the Army Service Component to U.S. Cyber Command; To train, organize, and equip forces; To provide Cyber Education, Training, and Leader Development; and Execute Cyber Proponent functions. The three part constellation approach is our way of getting at the issues of developing a workforce in a dynamic environment. Our approach continues to evolve.

Mr. LANGEVIN. Could each of you explain the Command and Control Relationships between your respective Service Cyber Components and CYBERCOM, regional combatant commanders, and other command structures?

General HERNANDEZ. Army Cyber Command (ARCYBER) operates under the Operational Control (OPCON) of USCYBERCOM (USCC). As the Army's Service component to USCC, Army Cyber Command exercises the designated command and control authority and responsibility over trained and ready Army forces, in support of Unified Land Operations, to ensure U.S./Allied freedom of action in cyberspace.

A significant example is the 780th Military Intelligence Brigade (780th MI BDE) (Cyber), which supports USCYBERCOM and combatant command cyberspace operations. ARCYBER has OPCON of the brigade, which conducts signals intelligence and computer network operations, and enables Dynamic Computer Network Defense of Army and Department of Defense networks.

The Army's Network Operations Security Centers and the Regional Computer Emergency Response Teams are also under the OPCON of ARCYBER. Control of these units has increased unity of command for the operation and defense of our networks. Additionally, Reserve Component cyber and information operations organizations are now OPCON to ARCYBER.

The Army has delegated OPCON of the Network Enterprise Technology Command (NETCOM) to ARCYBER and the Secretary of the Army has delegated OPCON of the 1st Information Operations Command.

There is no command relationship between ARCYBER and the Regional Combatant Commands. To facilitate seamless integration, USCYBERCOM directed the establishment of Cyber Security Elements (CSEs) to support each of the Combatant Commands. The CSEs function under the OPCON of USCYBERCOM in direct support of the respective Combatant Commands. USCYBERCOM provides direct support to Regional Combatant Commanders through its Service components.

ARCYBER leads the Joint effort for USCYBERCOM to provide cyber support to U.S. Central Command and U.S. Northern Command.

Headquarters Department of the Army (HQDA) retains administrative control over ARCYBER and is responsible to man, train, and equip Army cyber forces. While ARCYBER provides support to both Joint and Army commands, it currently has no established command relationship with other Army Major Commands (MAJCOMs), Army Service Component Commands (ASCCs), or Army Direct Reporting Units (DRUs).

Mr. LANGEVIN. The value of red-teaming—threat emulation—was proven perhaps most clearly in the Vietnam War with the establishment of Top Gun. The Director for Operational Test and Evaluation (DOT&E) has identified a shortfall in threat emulation and red teaming capabilities across the FYDP. What is each of the Services doing to address these shortfalls? Is the DOD investing adequately in the test capabilities and range environments that will be needed to remain current with advancing technologies?

General HERNANDEZ. Army Cyber Command established the World Class Cyber Opposing Force (WCCO) to provide live, interactive, expert, and realistic adversarial emulation in support of Army Training and Leader Development activities at the National Training Center and in support of COCOM exercises. The WCCO builds upon and compliments existing red team capability in 1st Information Operations Command and 780th Military Intelligence Brigade, extending its mission beyond traditional Information Assurance focused activities to include broader training and leader development. The WCCO supports the Army's Opposing Force program, providing a wide range of adversary "Information Warfare" activities during training events, to include Computer Network Attack and Exploitation, Deception, and Propaganda.

Recognizing overall Army shortfalls in cyber capacity, we are increasing our investment in all Defensive Cyber Operations (DCO) forces which, in addition to adversary emulation, includes advanced capabilities for adversary hunting and cyber vulnerability assessments. While they support Army units from a blue perspective, they provide many of the same benefits as traditional red teams. Beginning in FY14, the planned growth in DCO capability will significantly improve our ability to both protect Army systems and information and better incorporate red team activity into training activities.

DOD leverages numerous cyber range capability for the purpose of training and leader development, capability test and evaluation, and modeling and simulation.

Mr. LANGEVIN. How are your Services leveraging both in-house graduate educational facilities and DOD accredited programs, such as the NSA/DHS National Centers of Academic Excellence?

Admiral ROGERS. Navy is leveraging in-house graduate educational facilities and DOD accredited programs through close coordination with these institutions and a focus on a smart post-education placement process to ensure our most recently educated Sailors and civilians are detailed to positions which will benefit the Navy most. We recognize that affording our personnel graduate educational opportunities is critical to maintaining our expertise as we drive advancements in Navy cyberspace operations. With the quickly evolving nature of cyber, it is absolutely critical that the educational partners and programs we leverage keep pace with the changing cyber landscape.

To that end, the U.S. Navy leverages education and training from six major programs:

Air Force Institute of Technology (AFIT) and Naval Postgraduate School (NPS) In 2002, AFIT and the Naval Postgraduate School formed an educational alliance to eliminate duplicate degree programs in the fields of Oceanography and Aeronautical Engineering, and consolidate educational resources. Navy continues its close coordination with AFIT to refine course requirements, explore potential resource consolidations, and improve quality.

NPS

NPS offers an 18-month Master of Science degree in Cyber Systems and Operations that addresses a broad range of cyberspace operations such as computer network attack, defense, and exploitation; cyber analysis, operations, planning and engineering; and cyber intelligence operations and analysis. Navy will graduate 14 officers from this program in FY12 and is programmed to send 14 officers in FY13 per the approved Officer Graduate Education Quota Plan.

NPS's Graduate School of Operational and Information Sciences offers an Information Systems and Operations (ISO) Certificate Program. This warfighter-oriented degree program focuses on integrating information technologies, command and control processes, and Information Operations (IO) methods and elements into innova-

tive operational concepts for IO in the context of Network Centric Warfare. Since the program's inception in 2002, 318 officer, enlisted and civilian personnel have completed this certificate program.

The Information Systems and Technology (IST) certificate program provides an educational opportunity that is essential to helping the U.S. military reach information superiority in the operational environment. It offers advanced education in areas essential to enabling global networked communications, including: databases, systems analysis and design, decision support systems, and network security. Since the program's inception in 2003, approximately 96 officer and enlisted personnel have completed this certificate program. Both programs are taught via asynchronous Web-based media (i.e., the Internet). The asynchronous nature of these certificates has allowed us to deliver these certificates to deployed forces at sea and ashore.

Additionally, NPS will offer a 12-month Enlisted Cyber Master's Degree in September 2012 that provides selected Navy Sailors a Master of Science in Cyber Systems and Operations; Security and Technology. Selectees are assigned to a Navy-funded education program as full-time students under permanent change of station orders to Monterey, CA. Navy is sending five sailors through this program this year.

Finally, NPS just completed the approval process for a resident Master of Science, Network Operations and Technology degree that begins this fall and has eight officers scheduled to attend in 2013.

Masters of Information Technology Strategy (MITS)

In 2010, the Chief of Naval Operations directed the creation of the Masters of Information Technology Strategy (MITS) pilot program in partnership with Carnegie Mellon University (CMU). This program affords civilian and military IDC personnel the opportunity to attend CMU for a 16-month Master's degree program in cyber-related disciplines. The degree conferred is a Master's Degree in Information Technology and Strategy (MITS) and is a cooperative endeavor between of the College of Engineering (CIT), School of Computer Science (SCS), and College of Humanities and Social Sciences (H&SS). The initial cohort of two military and three civilians students commenced August 2011, and the second group of four commenced in August 2012.

National Defense University (NDU)

NDU's Government Information Leadership (GIL) Master of Science is a 39-credit hour curriculum of the GIL Master of Science Degree Program and offers a combination of information management, technology, and leadership intensive courses. Navy currently has 36 Master's degree enrollments and 497 certificate enrollments.

NDU's "iCollege" Chief Information Officer (CIO) Program is the recognized leader in graduate education for Federal CIO leaders and agency personnel. It directly aligns with the Federal CIO Council-defined CIO competencies and addresses the Clinger-Cohen Act and other relevant legislation mandates. It is sponsored by the DOD CIO.

United States Naval Academy (USNA)

Although an undergraduate program, USNA's Center for Cyber Security Studies is an important investment as it enhances workforce education and training at the Service academy level. Established in 2009, the Center provides support for the proposed curricular and professional reforms across the Naval Academy and encompasses support for all programs that contribute to the knowledge, study and research of cyber warfare.

NSA/DHS National Centers of Academic Excellence

National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Information Assurance (IA) Education (CAE/IAE), IA 2-year Education and Training (CAE/2Y) and IA Research (CAE/R) programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines. Students attending CAE/IAE or CAE/R designated schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program (IASP) and the Federal Cyber Service Scholarship for Service Program. NPS is a participant in this program.

To date, 84 uniformed and civilian Navy personnel have participated in the DOD IASP from commands across the Navy.

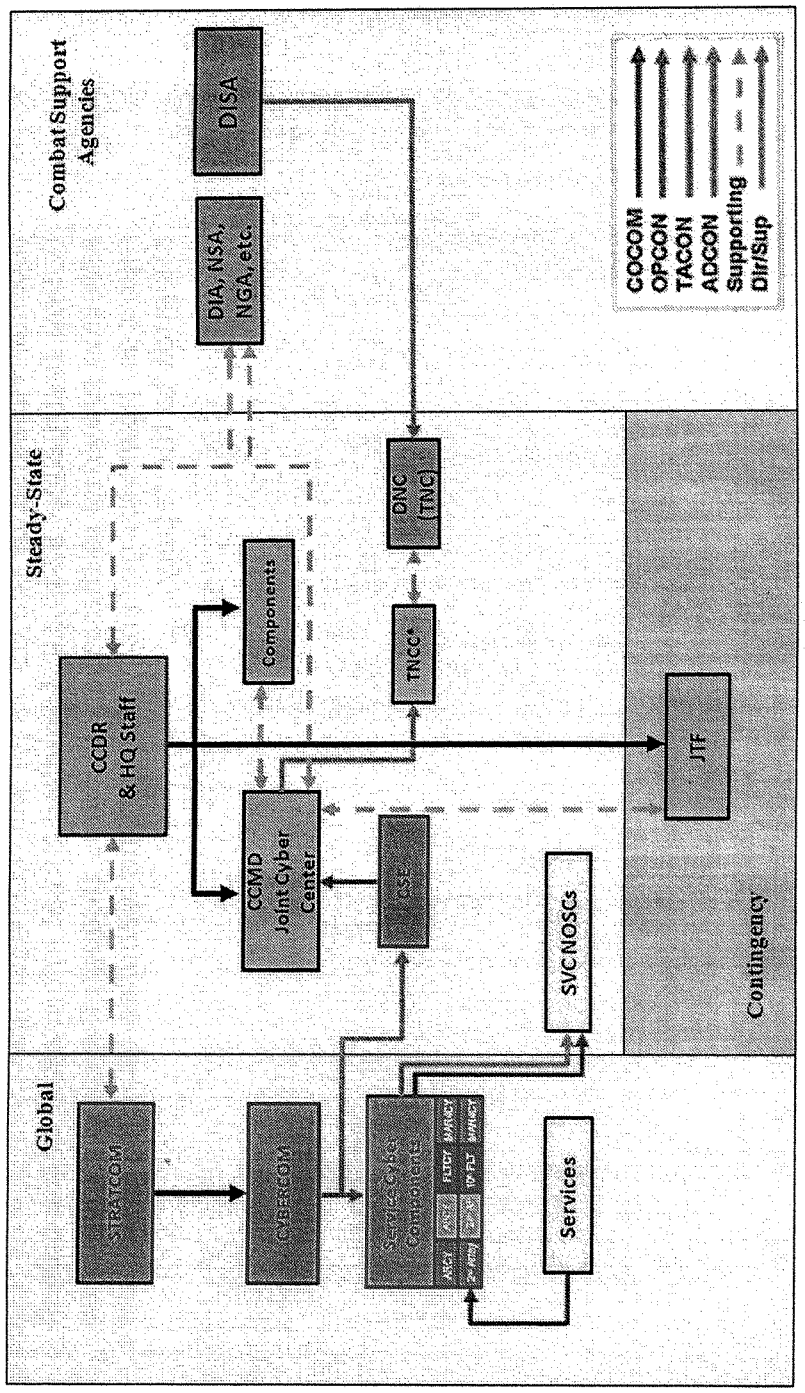
Mr. LANGEVIN. Admiral Rogers, your predecessor Admiral McCullough previously testified that much of the power and water systems for naval bases are served by single sources and have very limited backup capabilities. Can you provide an update on how the Navy is addressing threats to both its critical infrastructure and its secure and unsecure networks? Are you sharing information with critical infrastructure operators, and if so, through what channels does this information flow?

Admiral ROGERS. In an effort to correct vulnerabilities/deficiencies identified during recent critical infrastructure assessments the Navy is coordinating efforts with OSD to prioritize and fund the most urgent issues with FY13 Defense Critical Infrastructure Program (DCIP) resources.

U.S. Navy Defense Critical Assets (DCA) and Task Critical Assets (TCA) have been identified. The Naval Criminal Investigative Service (NCIS) provides all DCAs, validated through the Joint Staff, comprehensive counterintelligence support plans to identify foreign entity threats. TCAs, recently validated by the U.S. Navy, will receive similar coverage as required in DOD Instruction 5240.19. Identified threat information to the critical assets is provided to the asset operators through the most expeditious methods, however, generally through the identified NCIS representative assigned to the facility.

Mr. LANGEVIN. Could each of you explain the Command and Control Relationships between your respective Service Cyber Components and CYBERCOM, regional combatant commanders, and other command structures?

Admiral ROGERS. The below figure **(on page 99)** from the Joint Staff Transitional Cyberspace Operations Command and Control (C2) Concept of Operations signed on 1 May 2012, depicts the C2 structure. The C2 relationships follow command relationships as defined in Joint Doctrine unless otherwise specified in supplemental orders or directives. The framework establishes a standardized baseline for cyberspace operations C2 by documenting Joint Cyber Center (JCC) and Cyber Support Element (CSE) command relationships, missions, functions, and tasks. In addition, USCYBERCOM Operational Directive 12–001 specifies that Service Components have Direct Liaison Authorized (DIRLAUTH) with other Service Components, COCOMs, DOD Organizations, the Interagency, and foreign and commercial partners, to plan and execute assigned cyber operations.




*Representational of JCC's relationship with DISA's sub-element

U.S. Fleet Cyber Command/U.S. TENTH Fleet is the Navy's Component Command to United States Cyber Command, and an Echelon Two Navy Command, subordinate to the Chief of Naval Operations. Fleet Cyber Command has unique responsibilities as the central operational authority for networks, cryptology, signals intelligence, information operations, cyber, electronic warfare and space in support of forces afloat and ashore. As such, we organize and direct Navy cryptologic operations worldwide and integrate information operation and space planning and operations as directed.

Mr. LANGEVIN. The value of red-teaming—threat emulation—was proven perhaps most clearly in the Vietnam War with the establishment of Top Gun. The Director for Operational Test and Evaluation (DOT&E) has identified a shortfall in threat emulation and red teaming capabilities across the FYDP. What is each of the Services doing to address these shortfalls? Is the DOD investing adequately in the test capabilities and range environments that will be needed to remain current with advancing technologies?

Admiral ROGERS. Fleet Cyber Command also values the impact of red teaming. We believe that the issue is not one of capacity, but rather how we better use the capacity that already exists within the cyber domain. To make more efficient use of red teams, we have concentrated improving coordination across all DOD red teams to increase support to our cyber forces and help standardize red team activity.

The ongoing development and maturation of the USCYBERCOM and USFLTCYBERCOM staffs has allowed broader and timely coordination during the planning and execution phases of red team activity. As cyber actions are becoming more common events in major exercises, early planning and incorporation of cyber effects and training objectives have allowed improved synchronization across Navy and all DOD red teams. This early planning allows the capabilities of Service and DOD teams to be synchronized to best stimulate local, theater and global responses and allows the command and control structure of Defensive Cyber Operations to be exercised under real world conditions. The inventory and capabilities of Navy and joint test ranges is sufficient to meet current demand. However, range environments and test capabilities must be continually evaluated as technologies advance and as cyber policies and doctrine allow increased application in the joint planning and execution.

Mr. LANGEVIN. How are your Services leveraging both in-house graduate educational facilities and DOD accredited programs, such as the NSA/DHS National Centers of Academic Excellence?

General MILLS. The Marine Corps actively participates in the Department of Defense Information Assurance Scholarship Program, which provides access for both enlisted and officer students to AFIT, NPS, the National Defense University, Capitol College, George Mason, and other National Centers of Academic Excellence in Cyber Operations for graduate degrees in cyberspace security, information assurance, and computer security fields.

Through the National Intelligence University, marines with intelligence-related military occupational specialties are able to complete a Master of Science of Strategic Intelligence. Although this curriculum does not include cyber-specific courses as part of the core requirement, students are able to tailor their electives and focus thesis topics to include cyber operations.

The Marine Corps is currently in discussions with Northern Virginia Community College to establish a program to provide college credit for marines receiving military training and experience within the cyberspace operations workforce.

The Marine Corps University has initiated additional curricula in its educational programs that include topics in cyberspace operations, cyberspace planning, cyberspace law, and cyberspace implementation theories. Thus far, the Marine Corps University has had one class complete its program of instruction with this additional material. Initial feedback is that it was well received, and the Marine Corps University is evaluating comments to refine its curricula for future courses.

The Marine Corps also leverages cyber and cyber-related courses through NSA's National Cryptologic Schools for personnel serving at the Marine Cryptologic Support Battalion and the operating forces' Radio Battalions which provide Signals Intelligence and cyber related support to the Marine Air Ground Task Force, USCYBERCOM through MARFORCYBER, and the National Security Agency. Additionally, the Marine Corps uses the U.S. Navy's Joint Cyber Analysis Course (JCAC) and the Joint Network Attack Course to train enlisted marines and officers in cyber and cyber-related skill sets for MOS development.

Mr. LANGEVIN. Could each of you explain the Command and Control Relationships between your respective Service Cyber Components and CYBERCOM, regional combatant commanders, and other command structures?

General MILLS. The Service Cyber Component to USCYBERCOM is MARFORCYBER. MARFORCYBER is assigned to USSTRATCOM and USSTRATCOM has delegated OPCON of MARFORCYBER to USCYBERCOM. There is no direct command relationship between MARFORCYBER and the geographic combatant commanders. That being said, USCYBERCOM tasked MARFORCYBER to, in conjunction with USCYBERCOM, lead the joint effort to conduct cyber support of U.S. Special Operations Command (USSOCOM). MARFORCYBER was also tasked to provide a recommendation to USCYBERCOM on the requirements and support structure for a joint Cyber Support Element (CSE) at USSOCOM. In anticipation of approval of the CSE recommendation provided to USCYBERCOM for USSOCOM, MARFORCYBER staffed a colonel at USSOCOM as the USCYBERCOM Liaison Officer and Officer-in-Charge of the CSE. Additionally, a major, a captain, and two staff sergeants have orders to USSOCOM to form the nucleus of the CSE for USSOCOM.

Mr. LANGEVIN. The value of red-teaming—threat emulation—was proven perhaps most clearly in the Vietnam War with the establishment of Top Gun. The Director for Operational Test and Evaluation (DOT&E) has identified a shortfall in threat emulation and red teaming capabilities across the FYDP. What is each of the Services doing to address these shortfalls? Is the DOD investing adequately in the test capabilities and range environments that will be needed to remain current with advancing technologies?

General MILLS. The Marine Corps Network Operations and Security Center (MCNOSC) is task organized with organic red team and intelligence sections. The Marine Corps Information Assurance Red Team (Red Team) is tasked with finding new exploits and with emulating threat vectors/adversary tactics, techniques, and procedures (TTPs). This includes penetration testing, phishing, remote exploitation of network devices, exploitation of website vulnerabilities, wireless exploitation, close access, and insider threats. The Red Team operations in cyberspace are based on two distinct operational requirements: (1) internal and external exercise support and (2) MCNOSC directed operations. The Marine Corps will continue evaluating its red team requirements as added emphasis is placed on red team utilization within the Department.

On behalf of the Department, the Marine Corps manages the DOD Information Assurance Range—which is located in Quantico, Virginia. The DOD Information Assurance Range was initiated and funded by the Comprehensive National Cyber Initiative in 2009. This range emulates DOD networks—to include computer network defense (CND) capabilities, support to cyber exercises, and testing and evaluation of CND products and TTPs. It can operate in a standalone mode or can be integrated with other ranges (such as the Joint IO Range). The Marine Corps is participating in a Department-wide effort to evaluate an appropriate construct for cyber range governance to more effectively integrate, resource, and utilize these capabilities in the future.

Mr. LANGEVIN. How are your Services leveraging both in-house graduate educational facilities and DOD accredited programs, such as the NSA/DHS National Centers of Academic Excellence?

General VAUTRINOT. Air Force Space Command (AFSPC) and Air Education and Training Command (AETC) have established a full-range cyber training and education construct that begins in Basic Military Training and follows a challenging path that includes specialized cyber-focused graduate degrees.

In addition to cyber-focused graduate programs (MS/PhD) in Computer Science, Computer Engineering and Electrical Engineering with research focused on such areas as encryption algorithms, botnet disruption, network intrusion detection, and wireless network security, AFIT offers two Master's programs in cyber operations and cyber warfare. The 18-month Cyber Operations Master's Program provides extensive hands-on laboratory experience with both offensive and defensive measures and countermeasures, and is open to officers, enlisted, and civilians. The 12-month Cyber Warfare Degree Program for Majors and civilian equivalents provides a developmental education opportunity that addresses technical as well as policy and doctrine aspects of cyber operations.

The Information Assurance Certificate Program (IACP) is a subset of the Master of Science program. Students completing the required coursework are eligible for certificates under National Training Standards as an Information Security Professional, Senior System Manager, and Senior Risk Analyst.

On June 19, 2008, the Secretary and Chief of Staff of the Air Force designated AFIT and the Center for Cyberspace Research (CCR) as the Air Force's Cyberspace Technical Center of Excellence (CyTCoE). The Center serves as a bridge between the operational Air Force cyber forces and various cyber research, education, and training communities across the Air Force, the DOD, and national organizations.

The Center provides cyberspace professional continuing education for currency and professional development of the cyberspace workforce. The Air Force's Cyber 200 and 300 are Joint-accredited professional development courses designed to increase the depth and breadth of cyber operations understanding and to prepare individuals to apply cyber capabilities and concepts in Joint military operations. These courses are available to and attended by our Joint brethren in an effort to standardize training and proficiency across the DOD. The Air Force is also in the process of establishing disclosure guidance that will allow our international partners to send individuals to Cyber 200 and 300. The Air Force also utilizes graduate-level educational opportunities offered by our DOD and Agency partners such as the Information Assurance Scholarship Program (IASP) and the Computer Network Operations Development Program (CNODP). The IASP is open to all Air Force officers and is designed to retain a corps of highly skilled IA professionals to accommodate diverse warfighting and mission requirements. The CNODP is an intense, 3-year graduate-level internship at the National Security Agency that develops technical leaders who will lead the DOD and Services' employment of cyber capabilities. Graduates of this program receive focused follow-on assignments that capitalize on their breadth and depth of knowledge.

Mr. LANGEVIN. Could each of you explain the Command and Control Relationships between your respective Service Cyber Components and CYBERCOM, regional combatant commanders, and other command structures?

General VAUTRINOT. U.S. Cyber Command is the warfighting Sub-Unified Command for cyber. Each of the Services provides component cyber forces to the Joint fight through USCYBERCOM. For the Air Force, the 24th Air Force Commander is also designated the Commander of AFCYBER, the Service Component to U.S. Cyber Command. This direct command and control relationship stems from the authorities laid out in Title 10, USC. Operational orders flow from the President through the Secretary of Defense to the Combatant Commander to the Sub-Unified Commander and then to the Service Components. Under this authority, AFCYBER forces support Joint missions as directed by USCYBERCOM. AFCYBER, which is collocated with 24th Air Force in San Antonio, TX, has its Deputy Commander and a portion of AFCYBER personnel collocated with USCYBERCOM at Ft Meade, MD.

AFCYBER provides operational-level command and control of AF cyber forces through the 624th Operations Center. The Operations Center coordinates offensive, defensive and exploitation activities, provides daily reporting of operations, and manages network operations on the AF portion of the DOD network in accordance with USCYBERCOM guidance, as well as acting as a Continuity of Operations Plan for USCYBERCOM. AFCYBER supports regional combatant commanders through reachback or in-place participation in the Cyber Support Elements at the Combatant Command or AF Component (e.g., AF Central Command) level as tasked by USCYBERCOM.

The Command and Control (C2) Transitional Concept of Operations (CONOPS) and the Operational Directive (OPDIR) were released and provided guidance for USCYBERCOM and Service Components, specifying standard tasks and mission responsibilities for each of the Services. Based on these two documents, AFCYBER is tasked with leading the Joint effort to provide cyber support to USTRANSCOM, USEUCOM and USAFRICOM. AFCYBER works with these COCOMs to ensure cyber effects are presented to the Combatant Commanders as required. We continue to provide planning and characterization efforts in support of future operations through Operations/Concept of Operations Plans and Crisis Action Planning tasks from USCYBERCOM.

We also work, via SECDEF direction through USCYBERCOM tasking, with organizations and agencies while operating in support of authorities other than our traditional Title 10 role. Through USCYBERCOM, we have teamed with the Defense Cyber Crime Center and the Air Force Office of Special Investigations, as well as the Federal Bureau of Investigation, to work specific tasks under Title 18 authority. We use cyberspace operations to support the National Intelligence mission under Title 50. Additionally, we work with our Guard and Reserve personnel under Title 32 to add capacity and capability to AFCYBER.

Mr. LANGEVIN. The value of red-teaming—threat emulation—was proven perhaps most clearly in the Vietnam War with the establishment of Top Gun. The Director for Operational Test and Evaluation (DOT&E) has identified a shortfall in threat emulation and red teaming capabilities across the FYDP. What is each of the Serv-

ices doing to address these shortfalls? Is the DOD investing adequately in the test capabilities and range environments that will be needed to remain current with advancing technologies?

General VAUTRINOT. The cyber red team concept focuses on vulnerability assessments and intrusion missions of DOD networks. AFCYBER's Opposing Force (OPFOR) construct enhances the red team concept by providing a standard process for identifying vulnerabilities in a realistic threat environment, as well as capturing lessons learned and improving specific cyber tactics, techniques and procedures. The AF OPFOR team's goal is to allow commanders to objectively assess mission effectiveness and validate lessons learned to improve mission readiness.

AFCYBER employs the Air Force cyber range operated by the 346th Test Squadron at Lackland AFB, Texas, to support the full spectrum of cyber activities. These activities span capability development and tactics, techniques and procedures validation through employment of the OPFOR concept in support of Combatant Command exercises like Terminal Fury and Vigilant Shield. These ranges are already supporting the newly validated USAF Weapons School's Cyber Operations Weapons Instructor Course's capstone defensive mission and mission employment exercise, allowing for advanced weapons and tactics employment. AFCYBER also uses the Joint Information Operations Range to access and leverage the latest threat environments and emulations available from other DOD organizations, academia, and industry.

We continue to streamline the procurement process to facilitate nation-state capabilities ensuring Air Force Cyber Test & Evaluation infrastructure and personnel are able to reflect the changing nature of benign and contested cyber environments.

---

## QUESTIONS SUBMITTED BY MR. FRANKS

Mr. FRANKS. It is my belief that manmade and natural electromagnetic pulse is the ultimate cybersecurity threat. For example, an EMP attack on the U.S. would render our communications and computer systems useless, and disrupt virtually everything reliant on electricity. Furthermore, the DOD relies on a commercial electric grid, which is butterfly wing delicate to EMP, for approximately 99% of its military installations power requirements. What action is CYBERCOM taking to ensure its electricity is not disrupted by a manmade or natural EMP event, and how important is protecting the civilian electric grid from EMP for CYBERCOM's mission effectiveness?

Admiral ROGERS. Fleet Cyber Command does not have a specific program to address EMP scenarios. We have very few facilities that are hardened against an EMP event, and even those facilities are not fully hardened. However, we have an aggressive program to manage power outages, regardless of cause, across our domain. We have robust, well managed, critical power systems that provide continuity of operations to our mission critical systems. The critical power infrastructure includes standby generators, automatic transfer switches, and UPS (Uninterruptable Power Supply) systems. For most sites, this infrastructure results in zero loss of power or mission when commercial power is lost. This equipment is maintained, tested, and replaced as needed. Facilities across the domain are routinely evaluated for areas where the capacity or redundancy are insufficient, or mission growth now requires critical power, and these recommendations are balanced against other installation funding needs.

Given the criticality of the civilian electric grid, the Navy, through its DOD leadership, continues to work closely with the Department of Homeland Security on how to best to protect critical infrastructure in the commercial sector.

Mr. FRANKS. Over the years the DOD has invested billions of dollars hardening critical components against electromagnetic pulse. My efforts to protect the civilian grid against EMP have had a mixed reception. Most realize the enormity of the threat and the necessity to take action; but others have expressed opposite convictions, and feel that EMP is not the threat described in numerous scientific studies and reports. Do you assess this investment to be wise or unnecessary? If wise, should Congress make efforts to expand EMP protections to the civilian grid?

Admiral ROGERS. As stated in the question, science and studies indicate EMP is a valid threat to the civilian power grid. Given the criticality of the civilian power grid, it is prudent to consider the protection of this infrastructure against EMP and all other threats. The Navy, through its DOD leadership, continues to work closely with the Department of Homeland Security on how to best to protect critical infrastructure in the commercial sector.

## QUESTION SUBMITTED BY MR. CONAWAY

Mr. CONAWAY. During the hearing, you referenced a direct accessions program in the Navy. I would suggest that there could be a large number of highly skilled cyber warriors that may not see the military as an option. Can you expand on the direct accessions program for cyber?

Admiral ROGERS. There are three specific cyber-related skills sets the U.S. Navy directly accesses to develop and maintain our cyber expertise: Cyber Warfare Engineers (CWE), Information Professionals (IP) and Information Warfare Officers (IW).

Cyber Warfare Engineer: As a means of addressing the increased demand for officers with specific computer network operations (CNO) focused knowledge, skills and abilities, the Secretary of the Navy approved the establishment of the Cyber Warfare Engineer (CWE) designator in June 2010. CWE is a restricted line community within the information Dominance Corps (IDC) and CWE officers use specific cyber expertise to develop CNO capabilities. These CWEs apply the principles and techniques of computer science and computer engineering to research, design, develop, test, and evaluate software and firmware for computer network attack, exploitation, and defense in cyberspace operations. In addition to academic, age, and physical requirements, CWE candidates must meet strict citizenship and security clearance requirements and complete an interview process with Commander, Fleet Cyber Command. The direct accession requirement has been established at five officers per year.

Information Professional: Information Professionals (IP) provide expertise in information, command and control, and space systems through the planning, acquisition, operation, maintenance and security of systems. Their roles include leading the Navy's network warfare missions, developing tactics, techniques and procedures to realize tactical, strategic and business advantages afloat and ashore, and driving interoperability with Joint, Allied and Coalition partners. In addition to academic, age, and physical requirements, IP candidates must meet citizenship requirements, hold one or more active IT certifications and complete a professional review board process. Work experience in the field is strongly preferred. There are approximately 555 IPs in the Navy and we directly access approximately eight officers per year.

Information Warfare: Information Warfare (IW) Officers (IWO) are the DOD's premier force for Signals Intelligence (SIGINT), Electronic Warfare (EW) and CNO. Their mission is to execute the full spectrum of cyber, cryptology, SIGINT, information operations, CNO and electronic warfare missions. This occurs across the cyber, electromagnetic and space domains to deter and defeat aggression, to provide warning of intent, and to ensure freedom of action while achieving military objectives in and through cyberspace. In addition to academic, age, and physical requirements, IW candidates must meet strict citizenship and security clearance requirements and complete a professional review board process. There are 930 IWs in the Navy and we directly access approximately 40 officers each year.