[H.A.S.C. No. 111–180]

OPERATING IN THE DIGITAL DOMAIN: ORGANIZING THE MILITARY DEPARTMENTS FOR CYBER OPERATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

HEARING HELD
SEPTEMBER 23, 2010

U.S. GOVERNMENT PRINTING OFFICE
62–398 WASHINGTON : 2010

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

LORETTA SANCHEZ, California, *Chairwoman*

ADAM SMITH, Washington
MIKE McINTYRE, North Carolina
ROBERT ANDREWS, New Jersey
JAMES R. LANGEVIN, Rhode Island
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
BRAD ELLSWORTH, Indiana
BOBBY BRIGHT, Alabama
SCOTT MURPHY, New York

JEFF MILLER, Florida
FRANK A. LoBIONDO, New Jersey
JOHN KLINE, Minnesota
K. MICHAEL CONAWAY, Texas
THOMAS J. ROONEY, Florida
MAC THORNBERRY, Texas
CHARLES K. DJOU, Hawaii

Kevin Gates, *Professional Staff Member*
Kari Bingen, *Professional Staff Member*
Jeff Cullen, *Staff Assistant*

CONTENTS

CHRONOLOGICAL LIST OF HEARINGS

2010

THURSDAY, SEPTEMBER 23, 2010

OPERATING IN THE DIGITAL DOMAIN: ORGANIZING THE MILITARY DEPARTMENTS FOR CYBER OPERATIONS

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS

WITNESSES

APPENDIX

OPERATING IN THE DIGITAL DOMAIN: ORGANIZING THE MILITARY DEPARTMENTS FOR CYBER OPERATIONS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL
THREATS AND CAPABILITIES,
Washington, DC, Thursday, September 23, 2010.

The subcommittee met, pursuant to call, at 2:05 p.m., in room 2212, Rayburn House Office Building, Hon. Loretta Sanchez (chairwoman of the subcommittee) presiding.

OPENING STATEMENT OF HON. LORETTA SANCHEZ, A REPRESENTATIVE FROM CALIFORNIA, CHAIRWOMAN, SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

Ms. SANCHEZ. Good afternoon. I am sorry for being delayed. But I would like to welcome all of you and thank you for joining us here today.

The recent announcement by the Department of Defense [DOD] that they had suffered a major compromise of classified military computer networks has renewed discussions about what more DOD and the government should do to operate in the digital domain. The establishment of the United States Cyber Command [USCYBERCOM] and the announcement of a new cybersecurity strategy by Deputy Secretary of Defense William Lynn are important milestones, but we all know that more needs to be done.

Today the subcommittee is looking to discuss three main objectives for this hearing: One, to understand the plan to organizational structure for the military services' cyber component organizations and how they will present forces to the U.S. Cyber Command; understand—two, understand services' challenges to recruiting, retraining, to training a cadre of cyber operations professionals; and three, to discuss initiatives supporting service-specific requirements for cyber operations.

The purpose of this hearing is for the members of this subcommittee to learn what progress the services are making and organizing to carry out the full range of cyber operations, including computer network defense, offense, and exploitation functions. We also hope that the witnesses before us will be able to flesh out the doctrinal training and recruiting needs that will enable service concepts.

So today we have four distinguished witnesses before us. First we have Vice Admiral Bernard McCullough, III, of the U.S. Navy, the Commander of the U.S. Fleet Cyber Command and the U.S. 10th Fleet. Welcome.

Lieutenant General George J. Flynn, U.S. Marine Corps, is the Deputy Commandant for Combat Development and Integration.

Major General Rhett Hernandez, the U.S. Army, is the Assistant Deputy Chief of Staff, G3/5/7. I know what that means. Oh, hi.

And Major General Richard Webber, U.S. Air Force, is the Commander of the 24th Air Force.

Once again, I want to thank all of the witnesses for being here today. I look forward to hearing your testimony. Without objection, we will take your written testimonies and submit them for the record. And what I would like to have you all is to summarize or tell us what you think we should be taking away from your testimonies, or what you haven't told us that is important for us to know.

And we will be observing the 5-minute rule for questions from the Members. As you see, I have our ranking member here Mr. Miller, very diligent. And we probably will be joined by some others, but what this will allow us to do is probably ask as many questions as we probably want to, Mr. Miller.

So I will now yield to the ranking member from Florida Mr. Miller for his opening statement.

[The prepared statement of Ms. Sanchez can be found in the Appendix on page 21.]

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

Mr. MILLER. Thank you, Madam Chairman. I have a full statement I would like entered into the record.

And as you know, we had a full committee hearing this morning with General Alexander. And I think it is appropriate that we take an opportunity to visit with each of the services today and see where they are going, what their issues are that they need to bring before us, because we know this is an operational area that we cannot cede to anybody. Our forces are too reliant on its capability, and its effectiveness is only enhanced by the sophisticated and expert application of its benefits.

So in view of time, knowing that we have votes coming up, I would like to again ask that my full statement be entered into the record.

[The prepared statement of Mr. Miller can be found in the Appendix on page 23.]

Ms. SANCHEZ. Great. I thank my ranking member.

And I have just been notified that we are looking at votes maybe in—starting in about another 20 or 30 minutes, so I think that it is incredibly important that we begin and at least get the testimony in of our witnesses.

Again, gentlemen, thank you so much for taking the time to be before us today. And maybe we will begin with Vice Admiral McCullough of the U.S. Navy.

STATEMENT OF VICE ADM. BERNARD J. MCCULLOUGH III, USN, COMMANDER, U.S. FLEET CYBER COMMAND/U.S. 10TH FLEET, U.S. NAVY

Admiral McCullough. Chairman, thanks for holding this hearing. We think it is incredibly important to the defense of the United States.

Chairwoman Sanchez, Ranking Member Miller, thank you for the opportunity to discuss the United States Fleet Cyber Command and the U.S. 10th Fleet.

Madam Chairwoman, on 29 January, 2010, I assumed command of the United States Fleet Cyber Command and the United States Navy 10th Fleet. As the Navy's component command to the United States Cyber Command, Fleet Cyber Command directs cyberspace operations to deter and defeat aggression, ensure freedom of action, and achieve military objectives in and through cyberspace. While much of our mission parallels those of the other services' cyber components, Fleet Cyber Command has unique responsibilities as a central operational authority for networks, cryptology, signals intelligence, information operations, cyber, electronic warfare and space operations in support of forces afloat and ashore.

The Navy's vision is to fully develop our ability to operate in cyberspace and to accomplish this task by fusing and developing our capacity across all networks, signals intelligence systems, and electronic warfare systems. As such, we organize and direct Navy cryptologic operations worldwide and integrate information operation and space planning and operations as directed.

Tenth Fleet was originally established during the Second World War to develop and implement antisubmarine warfare capability and capacity. Today the reestablishment of the 10th Fleet is built upon the same principles. The operational focus of the 10th Fleet in the U.S. Fleet Cyber Command will enable us to accomplish our mission across all ranges of cyber operations.

To succeed we must be able to operate freely across the electronic spectrum while facing threats that range from the mundane, such as atmospheric interference, to highly advanced threats, such as network intrusion and malicious attack. It is Fleet Cyber Command's responsibility to analyze this advanced threat and develop the tactics, techniques, and procedures necessary to defend our network and be ready to take whatever steps are necessary to freely operate across all domains.

As Fleet Cyber Command continues to mature, we are finding ways to capitalize on the expertise of our sister services, working together to identify threats and establish a unified response.

Operationally we are moving out. Since our standup in January, we have partnered with USCYBERCOM—CYBERCOM's service components that are with me here today, as well as the U.S. Coast Guard, in support of United States Pacific Command and Pacific Fleet exercises. We are viewing—we are reviewing our network operations to enhance shared situational awareness and the inherent security that comes from cooperative oversight. We have also partnered with industry, academia and federally funded research and development centers during these exercises and routinely to take advantage of their knowledge and capability. The commercial sector drives this domain, and we must leverage their capacity and investment.

None of our efforts will provide mission accomplishment without effective recruiting and training of sailors who are technologically savvy and able to apply their skills to the defense of the fleet's networks. I have visited all but one of my subordinate operational commands, and I can assure the subcommittee that the Navy has an outstanding force of sailors ready to support the Nation across the entire range of cyber operations.

We have initiatives to create new officer specialties, including cyber warfare engineers and cyber warrant officers. The establishment of a training program at the United States Naval Academy will create new opportunities to train officers dedicated to cyber operations.

With any new operational area or domain, there is always room for tremendous growth. Every day I am amazed at the ability of our sailors to think beyond the traditional operational areas and to apply their expertise to the cyber realm. It is in that environment that we will cultivate and use to help recruit future experts.

There is no way the Department of Defense can compete with industry in the area of monetary compensation, salary if you will, but we can provide our people with expanded opportunities for education, training, and help them build experience as leaders that cannot be matched elsewhere.

My staff in command headquarters at Fort Meade is growing in strength and capacity each month. We currently operate with a headquarter staff of 130 that will grow to approximately 200 personnel over the next year, ensuring that we have the expertise needed to successfully operationalize cyber.

I thank you for this opportunity to discuss U.S. Fleet Cyber Command and the 10th Fleet and appreciate your support of our Navy and the Department of Defense. I look forward to answering your questions.

[The prepared statement of Admiral McCullough can be found in the Appendix on page 25.]

Ms. SANCHEZ. Thank you, Admiral.

We will talk now to—or we will hear from Lieutenant General George Flynn, U.S. Marine Corps, please.

STATEMENT OF LT. GEN. GEORGE J. FLYNN, USMC, DEPUTY COMMANDANT FOR COMBAT DEVELOPMENT AND INTEGRATION, U.S. MARINE CORPS

General FLYNN. Chairwoman Sanchez, Representative Miller, and distinguished members of the subcommittee, thank you for the opportunity to be here today. Let me begin by saying thanks for all you and all the other members of the House Armed Services Committee do to support our service men and women, their families, and especially our marines.

Cyberspace is clearly a new domain, and because it is manmade, it is something we learn more about each day. It is many things to many people. In my view, it is like terrain. It must be defended, and we must use it to gain advantage.

Just like the other traditional domains, our goal in developing our cyber capability is to create the means to maintain our freedom of action, not only in cyber, but in the other domains as well. Our focus initially has been in three areas: to improve our ability to defend our networks; to create a small component command staff to support not only the efforts of U.S. Cyber Command, but also to develop the capabilities needed to be inherent in our service force structure; and also to create the operators needed to support USCYBERCOM efforts.

Accordingly, we are taking a deliberate and joint approach to our cyber requirements, and we are using some of the past lessons to inform our requirement efforts in developing our organizational equipment and training requirements. We are seeking to find the right balance of efficiency and effectiveness in meeting both the U.S. Cyber Command requirements and our service requirements. This is why we are joined at the hip 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 that are assuredly ahead.

I have prepared a written statement. I would request that it be a part of the record. And I am looking forward to answering your questions.

[The prepared statement of General Flynn can be found in the Appendix on page 36.]

Ms. SANCHEZ. Perfect. Thank you so much, General.

Now we will ask Major General Hernandez of the U.S. Army for his 5 minutes or less.

STATEMENT OF MAJ. GEN. RHETT A. HERNANDEZ, USA, ASSISTANT DEPUTY CHIEF OF STAFF, G3/5/7, U.S. ARMY, INCOMING COMMANDING GENERAL, U.S. ARMY FORCES CYBER COMMAND

General HERNANDEZ. Chairwoman Sanchez, Congressman Miller, and members of the subcommittee, thank you for your ongoing support of our military and for the opportunity to appear before this panel with my counterparts from other military services today.

The Army established Army Forces Cyber Command as our service component to the United States Cyber Command. Our mission is to plan, synchronize, direct, and conduct network operations in defense of all Army networks and mission objectives. We stand ready when directed to conduct those cyberspace operations necessary to ensure U.S. and allied freedom of action in cyberspace.

We are organizing, training, and equipping Army forces to support Cyber Command's lines of operation. By providing shared situational awareness of the Army's portion of the Department of Defense information networks, we help the Commander, Cyber Command exercise command and control.

On 1 October, I will become the Commander of Army Cyber Command. I will ensure the Army closely coordinates with other services and the combatant commanders to fully protect our digital infrastructure, and that the combatant commanders receive the cyber support they require to accomplish their joint missions.

The Army organizes, trains, and equips to ensure that we can help protect and defend our Nation. Cyberspace is a domain and dimension of that defense. In cyberspace we know operations occur at net speed routinely and instantly across national boundaries and often involve multiple state and non-state actors. We are challenged to rapidly attribute adversary activity and anticipate collateral effects. We must address these requirements and undertake more robust measures to operate and defend our networks.

The Army Cyber Command construct leverages years of experience and a deliberate approach that will now meld unique cyber operations capabilities from the 9th Signal Command, the Intelligence and Security Command, and the 1st Information Operations Command into one fully integrated command structure to globally command and control all cyber operations for the Army. We will use a single—and are using it today—operations center that is tied to Cyber Command's Joint Operational Center as the focal point for planning, synchronizing, and conducting cyber operations.

In this organization people will be the centerpiece of our efforts to improve cyber operations. To effectively operate, we must change our culture. The first line of defense in cyberspace is the user, and every individual must understand that cyberspace is a contested environment that we must protect.

The second line of defense is our corps of cyber professionals who defend our networks and ensure operations. We will win in cyberspace with the best-trained and most professional personnel. To that end we must increase our capacity to grow cyber professionals, and resources are necessary to train the cyber workforce required for this ever-changing environment. Once trained, we must keep them in the ranks. Retaining highly trained cyber professionals is essential to maintaining our ability to effectively conduct cyber operations.

As our workforce matures, we must continue to quickly identify and acquire new capabilities in this rapidly evolving mission. The Army has multiple initiatives under way to improve our global network operations in defense, as well as expand our cyber capabilities, and Army Cyber Command will drive these efforts.

Chairwoman Sanchez and other members of the subcommittee, as I assume command, I pledge my support to you and to our Nation, and I look forward to our continued relationship. Your Army stands ready to defend and protect our digital infrastructure. I appreciate the opportunity to speak on these important matters and look forward to addressing any questions. Thank you.

[The prepared statement of General Hernandez can be found in the Appendix on page 43.]

Ms. SANCHEZ. Thank you very much.

And next we have Major General Richard Webber, U.S. Air Force. Hello, General.

STATEMENT OF MAJ. GEN. RICHARD E. WEBBER, USAF, COMMANDER, 24TH AIR FORCE AND AIR FORCE NETWORK OPERATIONS, U.S. AIR FORCE

General WEBBER. I would like to thank Chairwoman Sanchez, Ranking Member Miller, and the other distinguished members of the subcommittee for the opportunity to appear before you and represent the dedicated and exceptional men and women of 24th Air Force.

As our Secretary of the Air Force and Chief of Staff of the Air Force stated, our goal is to protect our mission-critical infrastructure, improve our capabilities, and develop greater cyber expertise and awareness to complement the entire Department of Defense cyberspace effort.

Twenty-Fourth Air Force just celebrated its 1-year anniversary, and I would like to take this opportunity to highlight some of the Command's recent accomplishments. On September 11, 2010, the Air Force Space Command Inspector General conducted an assessment and declared 24th Air Force ready for the full operational capability. And as soon as we—and soon we anticipate declaring 24th Air Force fully operational.

There are numerous ways 24th Air Force has made progress towards achieving this major full-operational capability milestone. I would like to touch on four significant examples.

First, we have undertaken extensive collaboration with our fellow air components and other combatant commands to integrate cyber courses of action into their operational plans. This is a distinct transition from our legacy approach in which cyber was relegated to a support role focused on assuring the network, rather than assuring the mission.

Second, we have made strides in obtaining dedicated intelligence resources to support our operations. As a result, we are shifting from a reactive network defense posture to one that is more predictive and dynamic. Ultimately this will facilitate our ability to predict and deter attacks before they take place.

Third, we have worked with Air Force Space Command to restructure and train our cyber professional workforce to produce capable, vigilant personnel with an operational rather than a maintenance-only mindset.

Finally, we have streamlined our cyber acquisition processes. This gives our airmen the tools they need when they need them to rapidly deliver capabilities for operations in an increasingly dynamic and contested domain.

Let me summarize by saying that the Air Force is committed to producing professional cyber warriors dedicated to assuring the joint mission and preserving our freedom of action in cyberspace. Because operating in cyberspace is a team sport, I, the men and women of 24th Air Force are proud to work alongside our teammates in USCYBERCOM and our sister services.

I would like to thank the subcommittee for your continued support as we endeavor to meet the challenges of defending cyberspace for the joint warfighter. I look forward to your questions.

[The prepared statement of General Webber can be found in the Appendix on page 58.]

Ms. SANCHEZ. Thank you, General. Thank you to all you gentlemen.

I will remind my colleagues that we will go by the 5-minute rule, and I will begin by asking some questions.

The first thing I would like to ask you all is there is somewhat of a difference of opinion. I have been, as you know, chairwoman since about the end of January with respect to this subcommittee, and the issues that go before it, cybersecurity being one of the more newer, difficult—you all know it is a very complex issue. So some have told me that with respect to the military, everybody has got a different system; even within each department, every ship, every plane, every unit, everybody has got different—they are operating under all different systems.

So my question is, is it your experience or your thought that the more consolidated our networks become, the more sameness we have across our networks within a service or across—or even across all services, that the easier it will be to defend that, or are we so stuck in legacy systems and upgrades and everything to all of that that we are never going to see that, and it would be easier for you all to defend all the different systems that you each have under you?

Maybe we will start with the admiral over there.

Admiral MCCULLOUGH. Chairwoman, as you suggest, as we built the network inside the military, we all sort of built it in our own way. The Navy, for instance, has three different systems. We have the Navy-Marine Corps Intranet that is transitioning to Next Generation Enterprise Network for our CONUS [continental United States] in Alaska and Hawaii part of our organization. OCONUS [outside the continental United States], we have something called ONE–NET, and then on ships we have something called IT–21. So we have got three networks inside what I will call our service enterprise network, and it is by nature the way the system was developed.

I think it is beneficial—and as General Alexander explained earlier this morning about moving to a different type of network, and he called it “computing on the edge” or “cloud computing.” And I think it is advantageous as we move forward that we do it as a united joint—in a united joint manner.

I also think it is imperative as we develop dynamic situational awareness of the networks that we—all the services do it in a manner that is interoperable, compatible, and takes advantage of what USCYBERCOM does under STRATCOM [Strategic Command] to develop that situational awareness so we don’t go on a divergent path. I think if we gain that ability and capability, that the network will be much easier to defend and maintain.

Ms. SANCHEZ. Anybody have a differing approach or something you all want to add?

And this is my concern. My concern is, of course, that we not only have to worry about what is inside the services’ network or networks, but we also have to worry about the fact that we interact with outside networks, let us just say contractors who are providing for us, and that the more we are one joint, the more openings there are, if we are all looking at—if we are working with contractors and others. And, of course, that seems to me in talking to everybody, that is one of the easiest ways to break into a system is the weakest link, which is individuals sometimes inside the military, but, of course, you know, we are exponentially creating even larger avenues into our networks.

Do you all have a concern about that, or do you think just concentrating—if we really had one network that worked across everything, that concentrating all our efforts just to protect one thing would be easier than walling off into different sections everything that we do?

Yes, General.

General WEBBER. If I could add, our legacy within the Air Force was essentially a separate network for each of our major commands. So Air Combat Command, Space Command, Air Mobility Command, they each had their own approach. And each of those systems were made up of a collection of hardware and software, each with their strengths and their weaknesses.

But in this arena, you are only as strong as your weakest link. And so what we are doing is we are migrating over several years to a single, more homogeneous Air Force network that will be much better designed in terms of giving us situational awareness, as well as allowing us efficiencies to operate, because when your system is not working and you pick up the phone, you want to call the help desk that knows how your system operates.

Now, once you have done that, then you need to consider how you defend things in depth. If you try to defend everywhere, in essence you defend nowhere. And so what we are asking our warfighters to do is identify to us what are those crown jewels, those mission-critical things that you must have to do your mission; for example, air mobility. You must have this op center, these key links, this hardware, this software, this data in motion, this data at rest. And then we are going to design a defense in depth for those crown jewels.

Ms. SANCHEZ. Let me ask one more question, and then I will let my colleague Mr. Miller ask some questions.

As you are moving and evolving towards this larger network, do you feel that you have the right acquisition process that allows you to meet those needs? And I will give you an example. When we—on another committee when we were looking at a particular project—it was a very big project—we did not have the right acquisition people within a particular department, so we all—what happened was that the contractor was allowed to almost act as the contract officer within the department, because, you know, information and this—and this technical skill sometimes can be easier found outside than brought in house.

So do you feel that you—and we know it from engineers and STEM [Science, Technology, Engineering and Mathematics] and everything, but there is also the acquisition process which sometimes has some of those people, but a lot of times doesn't have somebody so well-versed in what we are actually looking to acquire. So my question to you is do we have—do you have the ability to build an acquisition process, or do you have it in place, that will allow us to know what we are asking for and really get the best systems that we need as we evolve to the future? Anybody?

Yes. General.

General WEBBER. I can tell you the three-step approach that my boss for the organize, train, and equip side of the business, General Kehler at Air Force Space Command, has put in place, and I think it gets at all the challenges of this domain. And if you would envision a pyramid, and at the tip of the pyramid are those things that you literally need in hours or days. That is done for us by our 688th Information Operations Wing. And if you see a piece of malware, and you need a response to it now, these are the professionals that take care of that for us.

The second stage are things you would need in the 12-, 18-, 24-month timeframe, and in that arena, we are looking towards things like a Cyber Safari, which is a version of Big Safari, or even to a certain extent the Air Force TENCAP [tactical exploitation of national capabilities] Program that is skilled at matching these kind of rapid acquisitions.

And then the foundation of the pyramid is the classic acquisition where you have your PEO [Program Executive Officer], and you go to your product center. Although in that arena, because this domain changes so rapidly, you need to spiral develop. You need to consider block updates, and you need to make sure that you can spiral in new technologies, as well as be able to spiral the requirements as the threat changes.

Ms. SANCHEZ. Thank you, General.

Mr. Miller.

Mr. MILLER. Reading an article from Under Secretary Lynn in a recent Foreign Affairs magazine, he identified ways to effectively defend the networks from attacks and exploitation. And what I want to know is, yes, as we continue to defend, are we combining offensive actions with our current defensive actions? And can you talk about it in this setting?

Admiral MCCULLOUGH. I will take a stab at that, sir.

General Alexander talked about this morning to some degree, and—when he explained what we did in response to Buckshot Yankee, and how previous to that time we had an offensive team which was Joint Force Combined Command Network Warfare and Joint Task Force Global Network Operations. So the operations and the defense were under Global Network Operations, and other capability was resident in Network Warfare. And they had different levels of security clearance and access to different levels of information. And we found when we went to Buckshot Yankee that you had to combine those teams to be able to conduct full-spectrum cyber operations to both defend and operate and deter. And so within the confines of this room, we are working across a full spectrum of network operations, sir.

Mr. MILLER. We have got some budget constraints upon us and I think the chairman and I both want to make sure that we are efficiently spending all the funds that you have at your disposal. The question would be if we need to cut any programs or any initiatives, have you identified those that we can afford to cut?

General FLYNN. Sir, are you talking in the area of cyber or—that is real difficult to answer right now because we are in the middle of standing up what we are doing right now. And right now we are not looking at cutting what we are doing in cyber because this really has become something new that we are doing. We are increasing our defensive capabilities because we are more reliant on the Net than we ever were. And in addition to that, we need to increase the number of people that we have assigned to work at U.S. Cyber Command on network operations.

So the question, I think, is not so much what you would cut within Cyber Command, it would be more recognizing this as something new that is happening out there. It is what is old that would be the trade-off. And, for example, what we are doing in our service, in the Marine Corps, right now, we are conducting a force structure review group. It is to take a look at what structure you are going to need in the future. And this—I think cyber would be one of those fact-of-life changes that is new. So what—because this is new, and what is legacy then could go away. And that is a detailed process, that is what we are doing.

But in cyber, if you—off the top of my head, what would you—what would you do in a fiscally informed environment? I think right now this is where the growth is, because this is where—this is something new, and it is something that changes every day. So I don't have one off the top of my head to offer on that, sir.

Mr. MILLER. I have got four more questions that I just want to submit for the record since we have got a vote.

Ms. SANCHEZ. Certainly.

We just had a vote call. We probably have about 10 minutes before we have to stop. I would like to give the opportunity to Mr. Langevin to ask his questions for 5 minutes or less. The gentleman from Rhode Island.

Mr. LANGEVIN. I thank the Chair.

Gentlemen, thank you for being here, for the outstanding work that you are doing, and really talking about a critical issue, I think, that in many ways has been and in many ways still is overlooked, an overlooked element of our national defense. Obviously cybersecurity is going to become a growing and more complex challenge as time goes on, and we are never going to be able to get to the point where we are fully secure because it is such a moving target. So we all have our work cut out for us, and I thank you for the outstanding work you are doing.

Having chaired the subcommittee that oversaw our Federal cybersecurity efforts, this is certainly a long—both a professional and personal interest of mine. And securing our critical data and information infrastructure is an immensely challenging and complex task, one which the Department of Defense has really confronted head on. And DOD obviously is viewed as a standard bearer not just for its technical abilities, but also due to a keen appreciation of the seriousness of the threat that faces our Nation.

For me, this is the—our cyber challenges are—some of the vulnerabilities are the kind of things that certainly keep me up at night. However, there is obviously still room for improvement, despite the advances we have made and the steps we have taken, especially at the individual service level.

Now, earlier this morning, General Alexander touched on one of the important issues, and that is the protection of our physical critical infrastructure. My question for you all is many military bases are reliant on outside, privately controlled power plants, water systems. Recently—the recent public attacks, such as the Stuxnet worm, demonstrated a growing interest in targeting industrial control devices such as SCADA [Supervisory Control and Data Acquisition] systems. So my question is how are your individual services working to address these types of threats? And have there been any damage assessments performed on cyber, including control system vulnerabilities to individual bases?

General FLYNN. Sir, one of the additional hats I wear is I oversee a base a little bit south of here, and one of the key things we have done is we have identified all our critical infrastructure. So we know where the critical nodes are, whether it be in power, water supply, or anything else that may pass through the base. So the first step has been throughout not only the base down at Quantico, but throughout the Marine Corps, we have identified those critical nodes.

In the area of communications, where necessary we have created the redundancy that we need to be able to do that. But the first step in coming up with a solution is we have identified where those critical nodes are, and we are taking the steps to do what we can to mitigate them if it is possible.

Mr. LANGEVIN. Very good.

General.

General WEBBER. The Air Force is partnering with the national labs that are also working very hard on this issue, and our objective is to take each one of these vulnerabilities that are based on industrial control systems, understand how they work. And then my intent is to put out a direct—a Commander's direction that would be throughout the Air Force that says if you have this fuel system, or this HVAC [Heating, Ventilation and Air Conditioning] system, or this water system, or this power system, it will be installed in this way, it will be protected with a firewall this way, the settings will be set up very specifically. But right now those systems are very much wide open, and we haven't even taken the low-hanging fruit steps that we need to start taking now.

Mr. LANGEVIN. Admiral McCullough.

Admiral MCCULLOUGH. Congressman, I mean, as you well know, the systems that you discuss are very vulnerable to attack. The Navy has worked through the Commander of Navy Installations Command to identify critical nodes in that infrastructure. Do we have a plan for alternate power sources or alternate water sources? A lot of this is single source into a basin. If you take that capacity away, you have some capability on backup electric-power generation, but very little in other resources, such as water, sewer, et cetera.

And so it is—our mission sets DOD networks, but we are very well aware that given the vulnerabilities of various systems, that we have to work with DHS and others to get at the root issue, and we are working in that direction, sir.

Mr. LANGEVIN. And General Hernandez.

General HERNANDEZ. Congressman, that is a great question. I am not aware of the level of detail that the Army has gone into identifying critical infrastructure and vulnerabilities. I will gladly take that as part of my assessment and take it as a statement and question for the record and come back to you as soon as I have completed that.

[The information referred to was not available at the time of printing.]

Mr. LANGEVIN. I hope we can pay particular attention to all of this. I just—in closing, when I chaired the subcommittee on emerging threats and cybersecurity at Homeland Security, one of the vulnerabilities to critical infrastructure that came to light as a result of work done at Idaho National Labs was the threat to our electric grid. And again, so much of our—so many of our bases are dependent on local power systems, maybe off base. And if they are not secure, then clearly our bases are not going to be secure. Idaho National Labs, through this Aurora test, was able to actually blow up a—cause a generator through a SCADA attack to blow up and take the generator out.

These things aren't just sitting on a shelf somewhere where you can just plug them in. They are going to take months to build, ship and install. So again, I hope we can redouble our efforts to pay attention to our vulnerabilities, particularly in that area and other areas in critical infrastructure, especially as it affects our bases.

Thank you.

Ms. SANCHEZ. I thank the gentleman from Rhode Island.

We have six votes on the floor, and so we will have to wrap up this hearing, unfortunately. And I say that because I know how much you all prepared to be before us today, and I am sorry that it is, you know, crazy season in the Congress and that we have floor votes.

But I would like to ask a question before we close, and I have a feeling that many of the Members will submit for the record some questions, and we would love to have—if you could answer those for us.

I recently had Dr. Regina Dugan out—the Director of DARPA [Defense Advanced Research Projects Agency]—out in my district, and we went to schools to talk to young people about how important and—to motivate them to be in the science, technology, engineering, mathematics arena because, as we know, that really is the future for a lot of what we are talking about.

Can you talk about—one of you mentioned, and I think it was the Vice Commandant—that—how you motivate people to come and actually work for the military when the salary is not comparable and the benefit package obviously is not comparable to what we see in Silicon Valley or even in my area of Orange County, California, where we have so much of this going on in the private sector? What are the challenges? And what can we do to help you to ensure that we are getting the right talent to help us with such an incredibly important issue? Any of you?

Yes, General.

General WEBBER. I think the first step has to be how do you get the young folks hooked on the idea of working in the cyber environment and paying attention to their math and science skills. One thing that I would commend to you and I have already commended to my fellow component commanders is an Air Force Association program called Cyber Patriot. And basically what it is is a program that teaches junior ROTC [Reserve Office Training Corps] folks—so this is high-school age—how to build and operate and then defend a network. And then they compete in a nationwide shoot-out in terms of how well did they build their network, how well did they operate it, and then how well did they defend it. So far we are anticipating at least 300 high schools across the Nation are going to compete in this. So that is one of the good ways to get these folks hooked.

I think they are attracted to the training that we offer them. For each of us, these are going to be high-skill jobs. It is going to take probably a minimum of 24 months of training, and we are all looking for ways that we can keep them at least back-to-back assignments in the mission area. But then should they decide that they—that they want to leave the Air Force and perhaps work for a contractor or another government agency, I think that is where the Total Force comes in. And I think we collectively need to place our Guard units and our Reserve units in the right locations—and we in the Air Force have done that—where they can just take off that suit maybe once a month and walk across the street and do these exciting missions in cyber that they have been trained in.

Ms. SANCHEZ. Great.

Anybody else?

General FLYNN. One of the key parts here is we are also going to take a Total Force look. And the challenge is not only getting the Active Duty, but, as General Webber said, also the Reserves.

So the Total Force does have a piece to play here, and it is something that we can take a look at as we right now try to define what an operational reserve is. And this is one area to take a look at. And we also have to also attract the professional civilian workforce as well.

The other part I would say is we have to take a look at some of our personnel practices within the services. A lot of what we do, we have never did it for money anyway, so there is a motivation that comes to cause a young man or woman to join any of the Armed Forces. So we have to continue to capitalize on that.

But one thing that we have to take a look at is once you get somebody schooled in this area, and they become an effective operator, they need to stay in it. And so we are going to have to take a look at career progression that—you know, is it going to be acceptable to somebody not to have to do out-of-occupational-specialty assignment to get promoted? This may be the case where once you are in cyber, you never leave cyber, something like we do with some of our Special Operations units.

And then the other part is the training investment. We are going to have to take a look at maybe the length of our enlistment contracts. If it takes you 2 years to get somebody to be a skilled operator, then in most cases you only have 2 years left on Active Duty. So we have to take a look at that, and then, I think, what would be the appropriate incentive package. And in some cases, for—just like we see with young marines now returning again and again to Afghanistan, sometimes it is just the opportunity to do what you like doing and being part of something that is bigger than yourself.

Ms. SANCHEZ. Thank you.

Admiral MCCULLOUGH. If I could pile on.

Ms. SANCHEZ. Yes, Admiral. Pile on, pile on. Go ahead.

Admiral MCCULLOUGH. Okay. I think you can recruit the young men and women based on their excitement about the opportunities that are given, the educational opportunities that are given in this field, the opportunities to have a broad scope of responsibility that you don't necessarily get in the commercial sector. And once we educate them in the Navy—ours are 6-year contracts for these folks. Once you educate them, you have got to get them out into the field to practice this art, and then I think you have them.

But we do understand monetary compensation and what the limits that we have in that area. In the Navy we provide selective reenlistment bonuses for our cryptology technicians that do most of this work for us, up to $75,000 for a 6-year reenlistment. We also have broader educational opportunities for these folks.

And so I think, with satisfaction of mission and excitement about the opportunity that they have, that you can generate a stable workforce in the military for this. Now, the problem is how much does the general population bear in this type of folk, and we are all—the four services are competing with industry, with academia and other Federal agencies. And so does the Nation, as you suggest, have the right capacity to support what we are doing in this area?

Thank you.

Ms. SANCHEZ. Thank you.

General.

General HERNANDEZ. Chairwoman, my piling on would be that—in my testimony, and I firmly believe that the centerpiece and the center of gravity to our ability to operate in cyberspace is ensuring we can grow, retain, and train the right personnel. So I sign up for everything that everyone has said.

The only piece I would add to this is that I think it is going to take even more than that, and we are going to have to use our imagination to think about what other things might we be able to do or need to do. And I would re-echo the Air Force comments that we need to do it earlier and do it with more scholarships earlier in school programs to identify that special talent that is critical in this field.

Ms. SANCHEZ. Great.

Thank you, gentlemen, for your testimony. Again, I am sure that some of the other Members and I also will be submitting for the record some more questions for you. I know your time is valuable. As soon as you can get those answers back to us would be great.

And with that, I believe that the committee is adjourned. Thank you.

[Whereupon, at 2:51 p.m., the subcommittee was adjourned.]

APPENDIX

SEPTEMBER 23, 2010

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

SEPTEMBER 23, 2010

The Honorable Loretta Sanchez
Committee on Armed Services
Subcommittee on Terrorism and Unconventional Threats and Capabilities
"Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations"
September 23, 2010

Opening Statement

Good Afternoon,

I would like to welcome you all and thank you for joining us here today.

The recent announcement that the Department of Defense (DOD) suffered a major compromise of classified military computer networks has renewed discussions about what more DOD and the government should do to operate in the digital domain. The establishment of U.S. Cyber Command and the announcement of a new cybersecurity strategy by Deputy Secretary of Defense William Lynn are important milestones, but more needs to be done.

Today, the Subcommittee is looking to discuss three main objectives for this hearing:

1) Understand the planned organizational structure for the Military Services cyber component organizations, and how they will present forces to U.S. Cyber Command (CYBERCOM).
2) Understand Service challenges to recruiting, retaining and training a cadre of cyber operations professionals.
3) Discuss initiatives supporting Service-specific requirements for cyber operations.

The purpose of this hearing is for Members of this Subcommittee to learn what progress the Services are making in organizing to carry out the full range of cyber operations, including computer network defense, offense and exploitation functions. We also hope that the witnesses will be able to flesh out the doctrinal, training and recruiting needs to enable Service concepts.

Today, we have four distinguished witnesses before us:

- First, we have Vice Admiral Bernard J. McCullough, III of the U.S. Navy, the Commander of U.S. Fleet Cyber Command and U.S. 10th Fleet

- Lieutenant General George J. Flynn, U.S. Marine Corps is the Deputy Commandant for Combat Development and Integration

- Major General Rhett Hernandez, U.S. Army is the Assistant Deputy Chief of Staff, G3/5/7

- Major General Richard Webber, U.S. Air Force is the Commander of Twenty-Fourth Air Force

Once again I would like to thank all of our witnesses for being here today and I look forward to hearing your testimonies.

Without objection, we will accept your written statements as part of the official record. I'd also like to remind the witnesses that we'd like for you to briefly sum up your statements, and we will be observing the 5 minute rule for questions from the members.

I will now yield to the Ranking Member from Florida, Mr. Miller for his opening statement.
Thank you

Mr. Miller Opening Statement for Hearing on Organizing the Military Departments for Cyber Operations

September 23, 2010

"This morning, the Full Committee heard testimony from General Keith Alexander regarding the establishment of U.S. Cyber Command (CYBERCOM). As the command is slated to become fully operational next month, this morning's discussion and this afternoon's subcommittee hearing will do much to provide myself, and the members who have been following these development very closely over recent months, a full understanding of the expected outcomes, and hurdles, to CYBERCOM's ability to coordinate cyber activities across the Department.

"The 2010 Quadrennial Defense Review recommended that the Department centralize command of cyberspace operations as a means to better coordinate activities ranging from cyber operations to manning and investments; CYBERCOM achieves this centralization, bringing the military's full range of cyber capability under General Alexander. Additionally, Deputy Secretary of Defense Lynn, in his recent Foreign Affairs article, stated that the Department formally recognizes cyberspace as a new domain of warfare, making the role of CYBERCOM and the services all the more important in providing the appropriate capability into the future.

"The services will continue to play a critical role in providing needed capability. While CYBERCOM will coordinate and guide activities, your investments in training cyber-warriors, developing new technologies, and building infrastructure are the meat to the structure that General Alexander's vision will provide. And you will have to fight the daily fight as the ones who must execute and implement the Department's cyber strategy.

"This subcommittee has held a series of events this year, and in previous years, looking at cyber space and cyber operations. Your testimony today will continue our analysis and oversight into the Department's activities in this increasingly critical area.

"I have several concerns I hope our witnesses can address today:

- "It is beneficial to combine both defensive and offensive cyber capabilities. What are the challenges or impediments in successfully doing this?

- "How are the services ensuring compatibility and interoperability while also reducing redundancies across their respective cyber systems, programs, and research portfolios?

- "Our defense acquisition process is designed to build large quantities of hardware systems. What efforts have the services undertaken to adapt their acquisition processes to the dynamic nature of the cyber domain?

- "And finally, how do the services implement this dynamic and demanding mission, build and maintain a technically proficient workforce, and make the investments necessary to protect our cyber infrastructure while under such enormous budget constraints?

"Cyber space is an operational area we cannot cede. Our forces are too reliant on its capability, and our effectiveness is only enhanced by the sophisticated and expert application of its benefits. We want to walk away today confident that the service plans will fit into the vision for CYBERCOM and that the Department, and the nation, have the appropriate capability to bring to the table when the need arises."

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED
SERVICES COMMITTEE

Statement of

VADM BERNARD J. McCULLOUGH, III

Commander, United States Fleet Cyber Command

Before the

Terrorism and Unconventional Threats and Capabilities Subcommittee

of the House Armed Services Committee

Digital Domain: Organize the Military Departments for Cyber Operations

September 23, 2010

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED
SERVICES COMMITTEE

Chairwoman Sanchez, Ranking Member Miller and distinguished members of the Subcommittee, thank you for the opportunity to discuss the United States Fleet Cyber Command and TENTH Fleet.

Madame Chairwoman, on January 29, 2010, I assumed command of the United States Fleet Cyber Command and United States Navy TENTH Fleet. As 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 directs cyberspace operations in defense and support of our forces to deter and defeat aggression and ensure freedom of action. While much of our mission parallels those of the other Services' cyber components, 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. The Navy's vision is to fully develop our ability to operate in cyberspace by fusing old – and developing new – capabilities and capacities across our networks, signal intelligence systems, and electronic warfare systems. As such, we organize and direct Navy cryptologic operations worldwide and integrate information operation and space planning and operations as directed.

History

TENTH Fleet was established during World War II to develop and implement anti-submarine warfare in the Atlantic Ocean. At that time, we faced a threat much improved in capability and capacity over those possessed in World War I. This threat had enormous game changing potential. TENTH Fleet, which had no permanently assigned ships, defeated the German Submarine threat through integration of intelligence and the development of advanced tactics, techniques, and procedures. Today, the re-established TENTH Fleet is built upon the same principles. We conduct operations, with information warfare specialists, intelligence specialists, cryptologic and electronic warfare specialists, and traditional war fighters, to ensure freedom of maneuver against an advanced, game changing threat. The operational focus of Fleet Cyber Command will enable us to immediately respond to threats on our networks and maintain information assurance for our Navy. This operational framework allows us to accomplish our mission for defense of our network operations.

To succeed on the modern battlefield we must be able to operate freely across the electronic spectrum defeating threats that range from the mundane, such as atmospheric interference, to the highly advanced, such as network intrusion and malicious attack. It is Fleet Cyber Command's responsibility to analyze this advanced threat and develop the tactics, techniques and procedures necessary to defend our network and ensure our freedom of operation.

Structure

The Navy is operationally dynamic and our networks are complicated by distance and time. The Navy not only has Sailors stationed across the earth's oceans, but is also supporting ground operations in Afghanistan, Iraq, and many other locations around the globe. We currently have more than 10,000 sailors involved in these ground operations.

Fleet Cyber Command is a global command with locations around the world able to maintain and operate networks both ashore and afloat, guaranteeing our ability to conduct full spectrum cyber operations wherever our mission takes us. With Commander U.S. TENTH Fleet as the operational level commander, our structure is built around a typical Navy Task Force

Organization. This structure assigns regional responsibilities to subordinate task groups and provides support for specific cryptologic requirements. This Task Force Organization allows for a diverse dissemination of intelligence, technology and responsibilities and provides us with the ability to respond quickly to tasking in support of fleet requirements. It also facilitates our interaction with U.S. Cyber Command and service cyber components at the local level. We have continued to develop a robust structure within our Task Forces that will continue to provide rapid direct support across the spectrum of operations.

Navy network operations are provided by Network Warfare Command (CTF1010). Its subordinate units include Naval Computer and Telecommunications Area Master Station (NCTAMS) Atlantic and Pacific, which provide network direction, maintenance and shore based relay to the Fleet. Network defense is performed by Navy Cyber Defense Operation Command (CTF 1020). This organization works to detect network threats and to secure network responses.

Our information operations are overseen by the Navy Information Operation Command (NIOC) Norfolk (CTF 1030), with detachments in San Diego and Whidbey Island. Fleet and Theater operations are coordinated through NIOC Texas (CTF 1040), NIOC Georgia (CTF 1050), NIOC Maryland (CTF 1060), NIOC Colorado (CTF 1080) and their subordinate commands located around the world. Our cryptologic component operations are maintained at these locations under the CTF1000 structure.

CTF 1090 (Naval Information Operation Center Suitland) is established as our research and development group. It is tasked with developing technologies that are ready-to-field in response to supported Fleet and Joint tasking.

External and internal organization charts are included for your review.

None of our efforts will provide mission accomplishment without effective recruiting and training of Sailors who possess the technological acumen and the ability to apply their skills to the defense of the Fleet's networks. I have visited all but one of my operational commands, and I can assure the sub-committee that the Navy has an outstanding force of Sailors ready to support the Nation across the entire range of cyber operations. Given the dynamic nature of the cyberspace domain, we must continue to evolve our force. We have initiatives to create new officer specialties including cyber Engineers and Warrant Officers. The establishment of a cyber curriculum at the United States Naval Academy will create new opportunities to educate the officers who will command Naval cyber components and capabilities.

Mission

As Fleet Cyber Command continues to mature, we are finding ways to capitalize on the expertise of our sister Services. As a supporting command to U.S. Cyber Command, we are using the commonalities between service components to build a network defense-in-depth architecture, allowing our diverse capabilities to create robust and adaptable global cyber defense. If one service discovers, analyzes and defeats a threat, that information can be rapidly disseminated to the other Services to minimize any intrusion effort and create a unified response.

Operationally we are moving out. Since our standup in January, we have partnered with U.S. Cyber Command's Service components in support of United States Pacific Command and Pacific Fleet exercises. We are reviewing our network operations to enhance shared situational awareness and the inherent security that comes from cooperative oversight. We have also partnered with industry, academia, and Federally Funded Research and Development Centers to take advantage of their knowledge and capability. The commercial sector drives this domain and we must leverage their capacity and investment.

Coordination across domains is critical. Efforts to secure one system or provide a network defense must be coordinated to prevent unintentional interference with friendly systems. From navigational systems, to internet access and from the EA-18G Growler aircraft to shipboard SLQ-32 jammers, TENTH Fleet is working quickly to integrate with and complement the mission requirements of the other numbered Fleets and geographical Navy component commanders. The cooperation between Fleet staffs, is one of the key concepts behind TENTH Fleet's effort and one of the reasons for our rapid initial success.

My staff and command headquarters at Ft. Meade are growing in strength and capacity each month. We currently operate with a headquarters staff of 130 that will grow to approximately 200 billets over the next few years. The staffing rate ensures that our command will acquire not only technologically skilled Sailors, but also those who have a wealth of operational experience that they can draw from as we face the myriad challenges associated with cybersecurity.

Some of these challenges include: developing and maintaining a mindset that views the Network as an operational space; providing support across the Services to maintain our freedom of maneuver within cyberspace; developing cyber operations as a functional area, and creating a detailed concept of operations.

As we continue our operational development, we will be able to better support Fleet and Joint Exercises, which will provide required feedback on our ability to operate in a denied or contested cyber environment. This feedback is critical to enable us to assess and improve our capabilities to support freedom of operations in the face of ever adapting threats. These future threats are not just faced by Navy or DOD systems, but can affect civilian users as well, and they may come from non-traditional sources. Non-state actors, will no doubt, seek greater capability to affect our networks, and as a Nation, we must be ready to challenge this asymmetric threat.

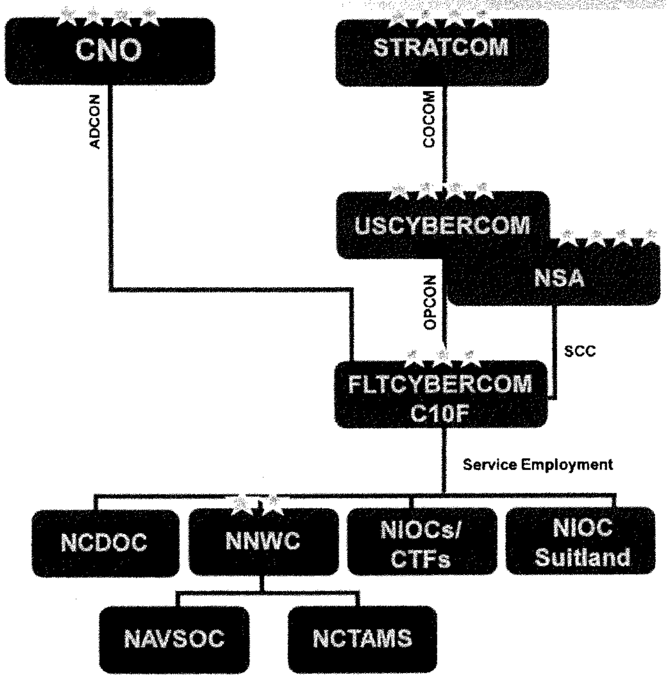
U.S. Fleet Cyber Command is also the Navy's operational authority on Electronic Warfare and Electromagnetic Spectrum Operations. In conjunction with the other Services, we are working to develop a comprehensive joint electromagnetic spectrum operation plan to ensure that our networks can operate within a spectrum in which maneuver space is restricted not only by adversary and competitor, but also by the expanding commercial enterprise allotment of radio frequency bands. The sheer number of radio frequency users proves that it is not enough to be able to defend ourselves from kinetic and directed network attacks, but we must be able to secure our network operations that take place over the air.

Every day, I am amazed at the ability of our Sailors to think beyond the traditional areas and to apply their expertise to the cyber realm. It is that environment that we will cultivate and use to help recruit future experts. There is no way the Defense Department can compete with industry in the area of monetary compensation, but we can provide our people expanded opportunities for education and training and help them build experience as leaders that cannot be obtained elsewhere.

With the cooperation of industry partners, Federally Funded Research and Development centers throughout the DOD, and academia, we will be able to better assess, understand and respond more rapidly to a wider variety of threats.

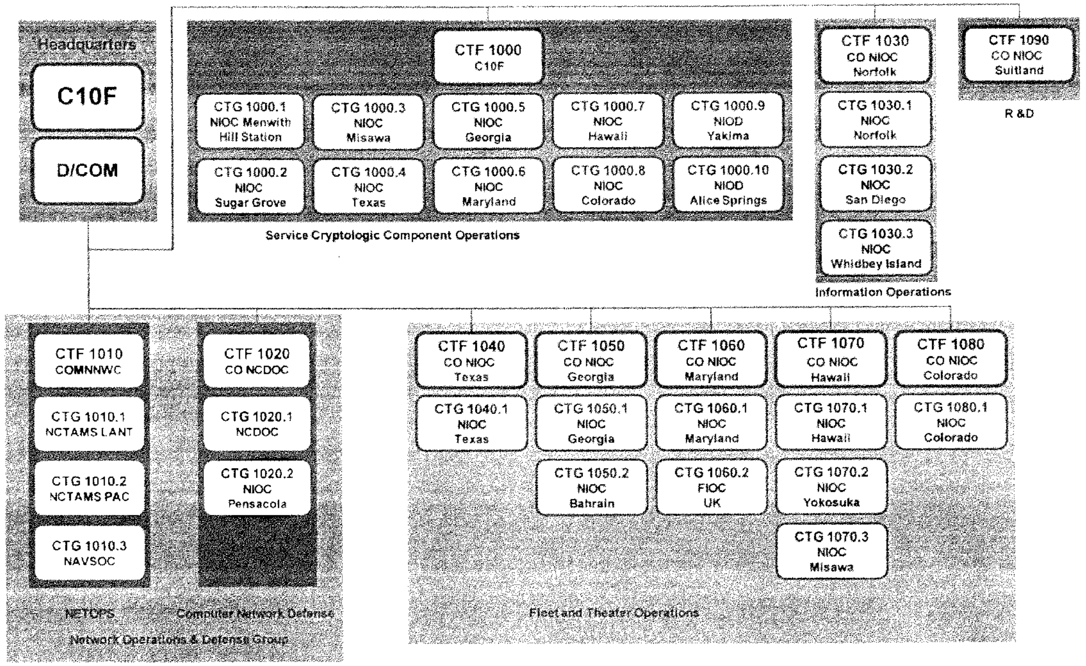
I thank you for this opportunity to present the U.S. Fleet Cyber Command and TENTH Fleet, and appreciate your support of our Navy and the Department of Defense. I look forward to answering your questions.

External C2 Relationships



UNCLASSIFIED

C10F Standing Task Organization



Headquarters

C10F

D/COM

CTF 1000
C10F

CTG 1000.1
NIOC Menwith Hill Station

CTG 1000.2
NIOC
Sugar Grove

CTG 1000.3
NIOC
Misawa

CTG 1000.4
NIOC
Texas

CTG 1000.5
NIOC
Georgia

CTG 1000.6
NIOC
Maryland

CTG 1000.7
NIOC
Hawaii

CTG 1000.8
NIOC
Colorado

CTG 1000.9
NIOD
Yakima

CTG 1000.10
NIOD
Alice Springs

Service Cryptologic Component Operations

CTF 1030
CO NIOC
Norfolk

CTG 1030.1
NIOC
Norfolk

CTG 1030.2
NIOC
San Diego

CTG 1030.3
NIOC
Whidbey Island

Information Operations

CTF 1090
CO NIOC
Suitland

R &D

CTF 1010
COMNNWC

CTG 1010.1
NCTAMS LANT

CTG 1010.2
NCTAMS PAC

CTG 1010.3
NAVSOC

CTF 1020
CO NCDOC

CTG 1020.1
NCDOC

CTG 1020.2
NIOC
Pensacola

NETOPS

Computer Network Defense

Network Operations & Defense Group

CTF 1040
CO NIOC
Texas

CTG 1040.1
NIOC
Texas

CTF 1050
CO NIOC
Georgia

CTG 1050.1
NIOC
Georgia

CTG 1050.2
NIOC
Bahrain

CTF 1060
CO NIOC
Maryland

CTG 1060.1
NIOC
Maryland

CTG 1060.2
FIOC
UK

CTF 1070
CO NIOC
Hawaii

CTG 1070.1
NIOC
Hawaii

CTG 1070.2
NIOC
Yokosuka

CTG 1070.3
NIOC
Misawa

CTF 1080
CO NIOC
Colorado

CTG 1080.1
NIOC
Colorado

Fleet and Theater Operations

UNCLASSIFIED — FLTCYBERCOM ★ ★ ★ TENTH FLEET —

9

Vice Admiral Bernard J. "Barry" McCullough, III

Commander, U.S. Fleet Cyber Command/
Commander, U.S. 10th Fleet

From Weirton, W.Va., Vice Admiral Bernard J. "Barry" McCullough graduated from the United States Naval Academy with a Bachelor of Science in Naval Architecture and was commissioned on June 4, 1975. Additionally, McCullough completed Naval Nuclear Power Training and received a Master of Science in Strategic Resource Management from the Industrial College of the Armed Forces at National Defense University.

McCullough's sea tours include serving as commander, Carrier Strike Group 6/commander, John F. Kennedy Strike Group. He also served as commander, Carrier Strike Group 14/commander, Enterprise Strike Group. McCullough's major command was aboard USS Normandy (CG 60) from February 1999 until February 2001.

Prior to commanding Normandy, he served as commanding officer aboard USS Scott (DDG 995) and USS Gemini (PHM 6). Other sea assignments were: operations officer for commander, 2nd Fleet/Striking Fleet Atlantic, engineer officer aboard USS Enterprise (CVN 65), engineer officer aboard USS Virginia (CGN 38), and main propulsion assistant aboard USS Texas (CGN 39).

McCullough's shore tours include serving as deputy chief of Naval Operations for Integration of Capabilities and Resources (N8), director, Warfare Integration and Assessment Division (N8F), director, Surface Warfare Division, (N86), commander, Navy Region Hawaii and Naval Surface Group Middle Pacific, the director for Strategy and Analysis, J5, at U.S. Joint Forces Command, 1st Battalion officer at the United States Naval Academy and as the department head for the D1G Prototype Nuclear Power Plant at Nuclear Power Training Unit, Ballston Spa, N.Y. McCullough assumed his current responsibilities as commander, U.S. Fleet Cyber Command/Commander, U.S. 10th Fleet in December 2009.

His decorations and awards include: Navy Distinguished Service Medal, Defense Superior Service Medal, Legion of Merit, Defense Meritorious Service Medal, Meritorious Service Medal, Navy Commendation Medal, and Navy Achievement Medal. Additionally, he is authorized to wear numerous unit and campaign awards.

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICE COMMITTEE

STATEMENT OF

LIEUTENANT GENERAL GEORGE J. FLYNN

DEPUTY COMMANDANT

FOR

COMBAT DEVELOPMENT AND INTEGRATION

BEFORE THE SUBCOMMITTEE ON

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

OF THE

HOUSE ARMED SERVICES COMMITTEE

CONCERING

OPERATING IN THE DIGITAL DOMAIN: ORGANIZING THE MILITARY

DEPARTMENTS FOR CYBER OPERATIONS

ON

SEPTEMBER 23, 2010

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED SERVICE COMMITTEE

Chairwoman Sanchez, Ranking Member Miller, and distinguished members of the subcommittee, I am honored to appear before you today. On behalf of all Marines, I want to thank you for your continued support to our Marines and their families. I appreciate the opportunity to discuss the Marine Corps Cyberspace Command (MARFORCYBER) with you. The Marine Corps has taken a very deliberate approach to the establishment of MARFORCYBER.

I would like to begin by providing you an overview of our view and approach to cyberspace as well as a synopsis of the support we provide to US Cyberspace Command (USCYBERCOM). I will also expand on our known and anticipated challenges; planning efforts; and finally, where I believe help is needed for execution of our cyberspace mission.

Cyberspace View and Approach

Cyberspace is many things to many people: a marketplace, a schoolyard, a library, a neighborhood, a base for criminal activity, a command and control infrastructure. The Marine Corps has established the MARFORCYBER to focus its cyber efforts. In coordination with USCYBERCOM, MARFORCYBER will plan, coordinate, integrate, synchronize and direct *defensive* cyberspace operations to *preserve* the Marine Corps ability to use and function within the Marine Corps Enterprise Network (MCEN).

The Marine Corps is continuing its deliberate approach to cyber by exercising diligence in the standup of effective cyber organizational structures and the application of both "pure" and "related" cyber resources. Pure cyber resources are comprised of an operational headquarters activity, the MARFORCYBER Command Element; the Marine Corps Network Operations

Security Center (MCNOSC); and finally, the Marine Corps Cryptologic Support Battalion's (MCSB) Company L. Related cyber functional resources are information technology Marines who support or affect the MCEN but are not directly within the MARFORCYBER. The Marine Corps is currently reviewing the application of these resources.

In building our cyberspace capabilities, the Marine Corps will dedicate approximately 800 personnel to the "pure" cyber workforce. The keystone to this relatively small workforce is the vision that all Marines who access and use the MCEN will become Cyber Marines. It is through their collective diligence that the Marine Corps will defend the MCEN, mitigate or eliminate vulnerabilities, and fortify our defensive posture.

As the cyber workforce is recruited, training will be essential to their ability to defend and support cyberspace operations. A typical Cyber Marine will require two years of classroom and on-the-job training to be proficient in cyberspace operations. The Marine Corps envisions a holistic, joint approach to cyber training. Accordingly, our Cyber Marines are attending and providing input to the Joint Cyber Analysis Course (JCAC) and the Joint Network Attack Course (JNAC). Defensive cyberspace resources encompass a number of cyberspace specialties, each with different training requirements.

Consistent with Secretary Gates' recent direction to create efficiencies across the Department by leveraging economies of scale in purchasing information technologies, MARFORCYBER envisions, and is advocating to USCYBERCOM and the other Service Components, a joint approach to equipping the force. Internally, the Marine Corps is currently focusing its cyberspace fiscal resources on Computer Network Defense through investments at the MCNOSC.

US Cyberspace Command Support

MARFORCYBER provides support to USCYBERCOM as the Marine Corps' Service Component. MARFORCYBER is actively engaged with USCYBERCOM at all levels of the organization. From the monthly Cyber Component Commander's Conference to daily interactions and operational planning teams, MARFORCYBER is supporting USCYBERCOM. Operationally, MARFORCYBER and MCSB Company L provide resources for National and Joint kinetic attack requirements; deployed forces in support of ongoing operations in Afghanistan; as well as, direct support to USCYBERCOM collaborative planning efforts.

The Marine Corps is undertaking a significant effort to define cyber capability and capacity. For capacity, the Marine Corps is trying to balance what it needs to do for the provision of cyber expertise and support to USCYBERCOM with its own cyber operational requirements. For capability, we are determining what resources will be required to sustain cyber operations across the cyber spectrum in support of both USCYBERCOM and Marine Corps operational requirements. These considerations together will determine the future shaping of the force, how we man, train and equip our Cyber Marines as well as deliberate preparations to cyberspace operations.

Challenges to Cyberspace Operations

There are operational challenges in cyber defensive activities. The challenges are emerging and not completely known at this time. Flexibility will be paramount to ensure mission and resource effectiveness while process development, doctrine and other modes of operation are developed, trained, and ingrained in our culture.

Being ready to operate successfully in an uncertain environment is a strength of your Marine Corps. Readying Marine Corps cyber forces is critical to success and our top priority. Readying our force includes recruiting, training, equipping and retaining the workforce. I would like to discuss with you the known challenges in each of these areas:

- *Recruiting*: We will achieve our FY10 cyber workforce recruiting goal using competitive enlistment bonuses for enlistment contracts with a minimum five year retention period. Existing Marine Corps policy limits maximum obligation periods to no more than five years. However, with a two year upfront training requirement, a longer service period is needed in order to achieve a return on investment.
- *Training*: As I have previously stated, the keystone to our small cyber workforce is the vision that all persons who access and use the MCEN will be critical to our cyber defense. Our challenge includes creating an acceptance throughout the Marine Corps that each person affects the cyber defensive posture of the Marine Corps. Additionally, as the cyber workforce grows and matures, another challenge will be to provide Marines a comprehensive roadmap for training and career development.
- *Equipping*: In order to be effective, Marines need to be properly equipped. Our cyber forces are no different. The cyber workforce must be equipped with the most appropriate and effective tools and capabilities. In our view, traditional acquisition approaches will likely not support the speed of cyberspace operations.
- *Retaining*: As the economy improves, the Marine Corps will compete for trained cyberspace personnel. Although the Marine Corps can offer these talented professionals something the civilian sector cannot – the opportunity to serve their country with pride, honor, and

distinction in a cutting edge role as a Marine – in some cases the lure of increased salaries and corporate titles/status will not be overcome.

We must be adaptive and provide our Marines with the tools they need to maximize their operational flexibility. To do this, we must remain vigilant and prepared. The threat in cyberspace is persistent, 24 hours a day, 7 days per week, and 365 days per year. With the support of the Congress, the American people, and industry we can ensure our Marines are ready now as well as in the uncertain future. I thank you for the opportunity to report on their behalf.

Lieutenant General George J. Flynn
Deputy Commandant, Combat Development and Integration

Lieutenant General Flynn graduated from the United States Naval Academy in 1975. He holds a Master of Arts Degree in International Relations from Salve Regina College, a Master of Arts Degree in National Security and Strategic Studies from the Naval War College, and a Master of Science Degree in National Security and Strategy from the National War College. He is a Distinguished Graduate of the College of Naval Command and Staff and the National War College.

Lieutenant General Flynn's command assignments include: Commanding Officer, HQ Battery, 2nd Battalion, 12th Marines; (1979-1980); Commanding Officer, L Battery, 2nd Battalion, 12th Marines (1980); Commanding Officer, P Battery, 5th Battalion, 10th Marines (1984-1985); Commanding Officer, 5th Battalion, 10th Marines (1992-1993); Commanding Officer, Officer Candidates School (1999-2001), Commanding General, Training Command (2002-2004), Commanding General, Training and Education Command (2006-2007). Commanding General, Marine Corps Combat Development Command (2008-).

Lieutenant General Flynn's staff assignments include: Forward Observer, Fire Direction Officer, Battery Executive Officer and S-4 A, 2nd Battalion, 11th Marines (1976-1979); Officer Selection Officer, Manchester, New Hampshire, (1981-1984), Operations Officer, 5th Battalion, 10th Marines (1985-1986), Plans Officer, Plans Policies and Operations Department, Headquarters Marine Corps (1987-1989); Junior Aide-de-Camp to the Commandant of the Marine Corps (1989-1991); Assistant Fire Support Coordinator, 2d Marine Division (1991-1992); Future Operations Officer, III Marine Expeditionary Force (1994-1995); Military Assistant to the Executive Secretary to the Secretary of Defense (1995-1997); Military Fellow, Council on Foreign Relations (1997-1998); Head, Strategic Initiatives Group, Headquarters Marine Corps (1998-1999); Military Secretary to the Commandant of the Marine Corps (2001-2002); Deputy Commanding General, Training and Education Command (2002-2004). Chief of Staff and Director, Command Support Center, United States Special Operations Command (2004-2006). Deputy Commanding General Multi-National Corps-Iraq (2008).

RECORD VERSION

STATEMENT OF

MAJOR GENERAL RHETT HERNANDEZ, USA

INCOMING COMMANDING GENERAL,

U.S. ARMY FORCES CYBER COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

2ND SESSION, 111TH CONGRESS

SEPTEMBER 23, 2010

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
HOUSE ARMED SERVICE COMMITTEE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES

Major General Rhett Hernandez, USA
Incoming Commanding General
U.S. Army Forces Cyber Command

Introduction

Chairwoman Sanchez, Ranking Member Miller, and Members of the Subcommittee, thank you for your ongoing support of our military and for the opportunity to appear before this panel with my counterparts from the other Military Services. Your support is important as we strive to mature and enhance our cyber capabilities. As the former Director of National Intelligence stated in his February 2010 annual threat assessment before the Senate Select Committee on Intelligence, "our economic prosperity and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes telecommunications, computer networks and systems, and the information residing within." Freedom of movement in cyberspace is a national security imperative for our Nation and our allies. Information technology, as Deputy Secretary of Defense Lynn stated so succinctly, "enables almost everything the U.S. Military does."

Army Forces Cyber Command (ARFORCYBER) is the Army's service component in support of U.S. Cyber Command (USCYBERCOM), a sub-unified command under U.S. Strategic Command (USSTRATCOM). Our mission is to plan, coordinate, integrate, synchronize, direct, and conduct network operations in defense of all Army networks and mission objectives. We stand ready, when directed, to conduct those cyberspace operations necessary to ensure U.S. and allied freedom of action in cyberspace.

As the Army's service component, my headquarters will coordinate with USCYBERCOM to organize, train, and equip effective cyberspace forces to support all USCYBERCOM Lines of Operation. We will also support USCYBERCOM with prioritization, coordination, and validation of Army mission requirements and force capabilities. This synchronized relationship will enhance situational awareness and achieve more effective coordination across the spectrum of cyberspace operations. Further, when USCYBERCOM directs, we will support establishment of Joint Task

Forces. Finally, ARFORCYBER will provide shared situational awareness of the Army's portion of Department of Defense (DoD) information networks to support cyberspace operations so the Commander, USCYBERCOM, can effectively command and control operations using a common Joint operational cyber picture.

As the incoming commander of ARFORCYBER, I will also work to ensure the Army closely coordinates with the other Services and the Combatant Commanders to ensure the Combatant Commanders receive the cyber operations support they require to accomplish their Joint missions.

Background

Before I discuss the details of where we are and where we are going in the cyberspace mission, I would like to share with you some of the decisions previously made by Army leadership that have positioned us to move forward quickly as we stand up ARFORCYBER. In 2004, recognizing the critical collaboration required between network defenders and providers to secure Army networks, the Army combined the Army Computer Emergency Response Team (ACERT) and the Army Global Network Operations and Security Center (AGNOSC) into a single Threat Operations Center at Fort Belvoir, Virginia. This new and collaborative organization ensured not only a robust defense of the network, but also the ability to protect the integrity and validity of both the networks and the content stored on them.

By September 2006, the Army recognized that computer network operations were evolving into the larger mission set of cyberspace operations. It therefore directed 1st Information Operations Command to integrate, coordinate, and synchronize Army computer operations. There remained, however, a requirement for senior operational leadership to oversee this mission.

To address this requirement, the Army, in January 2008, designated the Commanding Generals for Network Enterprise Technology Command (NETCOM)/9th Signal Command (Army) and U.S. Army Intelligence and Security Command (INSCOM) as Deputies for Network Operations and Network Warfare respectively under the Commanding General, U.S. Army Space and Missile Defense Command/Army Forces

Strategic Command (USASMDC/ARSTRAT). This new structure put an operational three star general in charge of Army computer network operations and provided the capabilities required across the spectrum of computer network operations.

On June 23, 2009, the Secretary of Defense issued a memorandum directing each of the Services to identify before the targeted fully operational capacity date of October 2010 an appropriate component to support USCYBERCOM. In response to that memorandum, this past year the Army named USASMDC/ARSTRAT as its Service Component in support of USCYBERCOM.

Foreseeing, however, the increasing global scope of the cyberspace mission, the Army determined it needed an organization focused solely on cyberspace operations. In February 2010, the Army approved the recommendation to stand up a separate command focused on the cyber mission. On October 1, 2010, ARFORCYBER assumes the cyber mission and brings unprecedented unity of effort and synchronization of all Army forces operating within the cyber domain.

In summary, over the past decade various elements within the Army have undertaken significant initiatives for network, information, and computer network operations. These initiatives, however, lacked the unity of command and control necessary to fully integrate them in support of DoD and National cyberspace operations. ARFORCYBER is organized to link Army networks worldwide, to fully integrate Army Computer Emergency Response Teams, and to draw upon INSCOM's cyberspace forces and capabilities. Reorganizing the Army's existing resources for cyber operations under a single command provides us the ability to serve as an operational arm to USCYBERCOM in support of its mission.

Cyber Operations

Our primary mission is to support USCYBERCOM in its defense of DoD networks and our Nation. To succeed in this endeavor, we must be able to operate in a joint environment that includes not just USCYBERCOM, the Component Commands, and our sister Service Components, but also other departments, agencies, and private entities. Therefore, as USCYBERCOM establishes its operating procedures, ARFORCYBER must concurrently establish and grow effective linkages with our sister Services. I expect to achieve a balance between centralized coordination and planning at USCYBERCOM and the routine exchange of operational data, planning, and resources with our sister Service elements. Internally, the Army must balance the centralized command and control exercised by ARFORCYBER against theater missions, responsibilities and priorities. As an operational force, the Army has strong competencies in the cyber arena: global presence, expeditionary experience and full-spectrum capabilities. We will effectively integrate our capabilities into USCYBERCOM's joint operational and planning efforts so we can fully support USCYBERCOM's joint missions.

The Army excels at achieving traditional military effects to support commanders' objectives. In the global cyber domain, however, with operations occurring at net speed across national boundaries and often involving multiple state and non-state actors, tactical actions can result in unforeseen and grave strategic consequences. Attributing adversary activity creates challenges, and collateral effects are often equally difficult to predict and fully understand. Our adversaries benefit from operating in a relatively unrestrained environment.

These cyberspace concerns and constraints require us to undertake more robust measures to defend our networks and National cyber interests. To effectively defend our networks and deter and oppose our adversaries, we must continue to grow our intelligence and cyber operations capabilities. This will require continued commitment on a national strategic scale. We must also establish internal processes and procedures within and between the Department's cyber organizations to enable cyberspace activities under various authorities to work in concert with each other to more effectively support cyber operations.

Fundamental first steps in achieving these goals include improving our ability to see and understand our networks better. We will do this by collapsing our networks from a disparate, loose federation into one Army enterprise network. This will enable us to establish centralized control of our networks and give us more complete, integrated visibility into them. Having accomplished this, we can then establish an active defense in depth across the network.

People, however, are the centerpiece for all efforts to improve our ability to operate effectively in cyberspace. The first line of defense in cyberspace is the user. To operate effectively, we must change our culture. Every individual must understand cyberspace is a contested environment that must be protected. The second line of defense is our corps of cyber professionals who defend our networks and ensure operations. We will win the contest in cyberspace as we win on traditional kinetic battlefields, with the best trained and most professional personnel. To that end we must increase our capacity to grow cyber professionals and to retain them. Many resources, including time and money, are necessary to train the cyber workforce required for today's environment. Once trained, our challenge is to retain them. Their skills are highly marketable throughout the public and private sectors. The importance of retaining our highly trained cyber professionals cannot be understated – doing so is essential to maintaining our ability to effectively conduct cyber operations.

Organization for Cyber Operations

To efficiently and effectively accomplish its cyberspace missions, ARFORCYBER is organizing as indicated on the attached organizational chart. It will include NETCOM/9th Signal Command (Army), and operational control of cyber forces assigned to INSCOM. The newly formed Army Cyber Operations and Integration Center (ACOIC) will be the focal point of our command and control and synchronization.

The Commanding General, NETCOM/9th Signal Command (Army), will serve as the ARFORCYBER Deputy Commanding General for Network Operations and Defense. In this capacity, she controls four Theater Signal Commands which support respectively, the U.S. Northern and Southern Commands, U.S. Pacific Command, U.S. Central Command, and the U.S. European and Africa Commands, as well as a Signal Brigade in support of U.S. Forces Korea. These forward deployed Signal Commands and the Signal Brigade are unique to the Army and give ARFORCYBER a forward network operations command and control presence in these theaters.

The Commanding General, INSCOM, will serve as the ARFORCYBER Deputy Commanding General for Network Warfare. She will control forces, to include a Cyber Brigade being established to provide dedicated support to ARFORCYBER, which support cyber operations and intelligence requirements.

***Army Cyber Operations and Integration Center* (ACOIC)**

The ACOIC is the command and control center for all Army service-related cyberspace activities. Using current and evolving doctrine and lessons learned from enduring and future operations, the ACOIC will ensure Army personnel at all levels receive clear, concise, and timely direction to execute full spectrum operations in cyberspace. The ACOIC also integrates the process for Army personnel and organizations to report anomalies in the cyberspace domain. The ACOIC is postured to maintain close watch on all Army cyberspace operations that may impact our national security and to share that information with other Army commands, our counterparts in the other Services, and the U.S. Cyberspace Joint Operations Center.

To ensure the ACOIC is fully nested with and able to seamlessly support USCYBERCOM, the ACOIC is physically locating and embedding approximately 25 personnel in the USCYBERCOM joint staff. These embedded personnel will ensure close collaboration with USCYBERCOM and enable the ACOIC to leverage USCYBERCOM's unique resources and capabilities. As the Army continues to seek advancements in cyberspace operating capabilities, the ACOIC will serve as the hub for advancements to materialize. It will include trained personnel dedicated to future planning, capabilities assessment, and exercises and training. This organizational structure will ensure the Army remains prepared with properly trained and equipped personnel to effectively respond to current and future challenges awaiting in cyberspace.

Future challenges will include the speed and consequential global impact of events in cyberspace. The boundaries of cyberspace are, of course, often unclear. Several factors (e.g. ownership of equipment, users of equipment, and location of equipment) influence the interpretation of where cyberspace boundaries lie. To further complicate such determinations, a cyberspace event may simultaneously occur in multiple geographic locations. The ACOIC will assist the USCYBERCOM Joint Operations Center to maximize global availability of cyberspace for the DoD and its coalition partners and allies.

Training

Our national and military dependence on the cyber domain and information technology demands that we invest in cyber capabilities to grow the skills necessary to maintain our ability to operate freely in cyberspace. A significant number of our command and control and logistics systems depend on cyber technologies. We must therefore make significant investments in education, training, and experience to understand emerging trends, develop and deploy new capabilities, and effectively defend against new cyberspace threats.

In addition to training sponsored by Army organizations, such as the Basic Computer Network Operations Planners Course, the Army leverages Joint cyberspace training courses such as the National Security Agency's System and Network Interdisciplinary Program.

Recognizing the Army's unique cyberspace training requirements, the U.S. Army Training and Doctrine Command initiated a formal "Cyberspace/ Electromagnetic Contest" Capabilities Based Assessment in February 2010. This assessment, which is being led by the U.S. Army Combined Arms Center at Fort Leavenworth, Kansas, will provide additional analytic insights for evaluating Doctrine, Organization, Training, Material, Leadership, Personnel, and Facility (DOTMLPF) gaps and solutions across all echelons of the Army. This effort will result in a comprehensive assessment of the training and personnel requirements necessary to conduct effective cyberspace and electromagnetic spectrum operations. We expect to receive the results of the Capabilities Based Assessment over the next year.

Personnel

To fully establish ARFORCYBER's headquarters, the Army will locate the headquarters in the National Capital Region and will realign Soldiers and civilians into essential ARFORCYBER headquarters positions. The total command strength of 21,000 Soldiers and civilians will be located around the globe. ARFORCYBER will include personnel currently assigned to the NETCOM/9th Signal Command (Army), portions of the 1st IO Command (Land), as well as with resources from USASMDC/ARSTRAT. Additionally, cyber operations personnel from INSCOM will support ARFORCYBER for cyber-related actions.

Manning levels for the Headquarters and the ACOIC were determined through an extensive analysis of existing and new mission sets, comparative analysis with other Services' cyber organizations and manpower studies. As the organization matures, manning levels will be evaluated against the "Cyber/ Electromagnetic Contest" Capabilities Based Assessment, as well as a follow-on manpower study that will be conducted within the next 18 months.

Technology

The current Army network is a loose federation of regional and command-centric enterprises with disparate levels of security, network visibility, and control. The first step on our cyber technology roadmap is to have the capability to "see" the network. The Army is achieving this by moving our networks to centralized control, and then instrumenting the network with a common tool set that can produce a predictable and repeatable picture of what is happening. This will transform the Army managed LandWarNet into a single Army Enterprise Network that standardizes security posture, establishes visibility, and allows for seamless transition of forces between the generating force and combat deployments. While these tools are designed to present a picture of the network's health and welfare, they do not completely inform commanders about what is happening in the network.

The next step is to "understand" what is happening on our network through real time situational awareness, single reporting, shared visibility, and a proactive defense.

This will allow operational commanders to make risk-based decisions in the context of complex multi-domain operations. This extended reporting and awareness will, in turn, enable higher level commanders to better assess risk in the context of theater or global implications and then take the appropriate action at the proper level to enable mission assurance within cyberspace.

The final step is to have the capability to "understand" what we "see" and "do" something about it before the threat can gain an advantage in the cyberspace domain. We can achieve this through the integration of full spectrum cyber operations. Once we can see and understand our network environment well enough to proactively operate and defend against threats at "net speed," we can start leveraging cyberspace as a domain in which the joint force commander can maneuver.

To fully leverage cyberspace as a domain, we must constantly strive to harness new technologies. To do this, ARFORCYBER will pursue innovative Army acquisition processes that allow us to keep pace with rapidly changing technologies without risking the fiscal integrity of the acquisition system. Several Congressional, DoD, Combatant Command, and Service studies have shown that developing and refining cyberspace related Rapid Acquisition Processes is critical to achieving and maintaining superiority in cyberspace. For example, acquisition cycles that normally take two or more years will not satisfy critical mission requirements.

The Army must focus on three areas. First, we must establish a cyberspace science and technology program that leverages emerging capabilities from both the private sector and academia. Second, the Army must pursue and implement cyberspace-specific acquisition and procurement policies that allow the warfighter to conduct research, development, testing, and evaluation of promising cyber technologies in an extremely efficient time line. Finally, the Army needs a rapid development and fielding process nested within the Army's Combat Development for Rapid Equipping processes that have been so successful in equipping the force in Afghanistan and Iraq. Without the ability to leverage cyberspace science and technology advancements, the authority to promptly conduct research, development, testing, and evaluation, and the means to rapidly transition successful technologies, the Army and the joint warfighter will struggle with the need to quickly acquire technology and infrastructure necessary for responding to gaps and threats from our adversaries.

Doctrine

As the Army integrates cyberspace into current and future force structure and operational concepts, we must meet the challenge of how to integrate our efforts into full spectrum operations and address both the generating force and the operating force. U.S. Army Training and Doctrine Command has coordinated concept development for cyber with stakeholders across the Army, and in January of this year published a Cyberspace Operations Concept Capabilities Plan (CCP) which outlines the framework under which the Army expects to conduct cyber operations in the timeframe 2016-2028. The CCP was the first step in the ongoing Capabilities Based Assessment for cyber and is nested closely with updates to Army doctrine for command and control and synchronized with the revision of Field Manual 3-0, Operations, the Army's Capstone doctrine for operations.

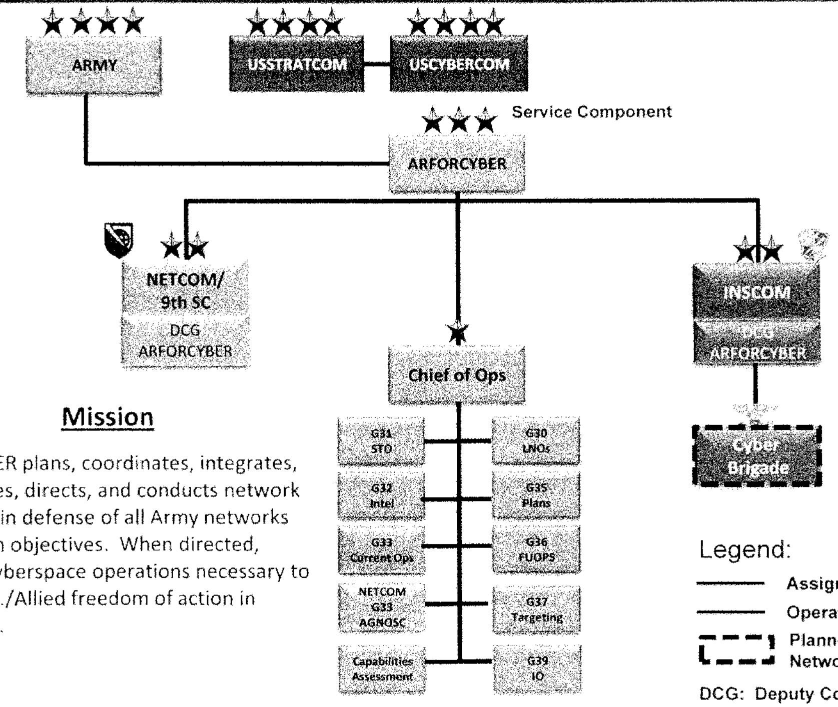
As we gain experience in cyberspace operations and improve our capabilities, Army cyber doctrine development must remain closely nested in broader Joint doctrine. The Army, along with the other Services, has participated in USSTRATCOM's development of a draft Joint Test Publication for Cyberspace Operations. Additionally, the Army has been working very closely with the sister Services and the Joint Staff in support of USSTRATCOM's Cyberspace Joint Operating Concept initiative.

We are at the beginning phase of the process to develop and document operational concepts and a robust doctrinal framework for cyber. Our Nation, the DoD, and the Joint Warfighters will require new and updated policy, concepts, and doctrine to effectively combat intelligent, evolving adversaries who are leveraging cyberspace to enhance their capabilities. To fight and win future battles, we must not only out-maneuver our potential adversaries, we must out-think them strategically, operationally, and tactically.

Conclusion

Ms. Chairwoman and other members of the subcommittee, I want to end by thanking you for your continued support to the Army and our Nation. As I assume command, I pledge my support to you and our Nation. Please rest assured that the Army, in conjunction with the Department and the other Services, stands ready to defend and protect our Nation's digital infrastructure. I appreciate having the opportunity to speak on these important matters and look forward to addressing any questions you or other subcommittee members may have.

ARFORCYBER



Mission

ARFORCYBER plans, coordinates, integrates, synchronizes, directs, and conducts network operations in defense of all Army networks and mission objectives. When directed, conducts cyberspace operations necessary to ensure U.S./Allied freedom of action in cyberspace.

Legend:

——— Assigned

——— Operational Control

▭ Planned (growth of Army Network Warfare Battalion)

DCG: Deputy Commanding General

"Dominate the Digital Battlefield!"

United States Army

Major General Rhett A. Hernandez

Assistant Deputy Chief of Staff, G-3/5/7
United States Army
400 Army Pentagon
Washington,DC20310-0400
Since: May 2009

SOURCE OF COMMISSIONED SERVICE USMA

EDUCATIONAL DEGREES
United States Military Academy – BS – No Major
University of Virginia – ME – Systems Engineering
National Defense University – MS – National Security and Strategic Studies

MILITARY SCHOOLS ATTENDED
Field Artillery Officer Basic and Advanced Courses
United States Army Command and General Staff College
National War College

FOREIGN LANGUAGES German

PROMOTIONS	DATE OF APPOINTMENT
2LT	2 Jun 76
1LT	2 Jun 78
CPT	1 Aug 80
MAJ	1 Aug 87
LTC	1 Mar 93
COL	1 Jun 98
BG	1 Feb 03
MG	7 Apr 06

FROM	TO	ASSIGNMENT
Oct 76	Apr 78	Forward Observer, later Assistant Executive Officer, B Battery, 2d Battalion, 33d Field Artillery, 1st Infantry Division, United States Army Europe and Seventh Army, Germany
May 78	Nov 78	Assistant S-3 (Operations)/Fire Direction Officer, 2d Battalion, 33d Field Artillery, 1st Infantry Division, United States Army Europe and Seventh Army, Germany
Nov 78	Jul 79	Executive Officer, A Battery, 2d Battalion, 33d Field Artillery, 1st Infantry Division, United States Army Europe and Seventh Army, Germany
Jul 79	Dec 80	Commander, B Battery, 2d Battalion, 33d Field Artillery, 1st Infantry Division, United States Army Europe and Seventh Army, Germany
Jan 81	Jul 81	Student, Field Artillery Officer Advanced Course, United States Army Field Artillery School, Fort Sill, Oklahoma
Sep 81	Nov 82	Commander, Service Battery, 1st Battalion, 5th Field Artillery, Fort Riley, Kansas
Nov 82	May 84	S-3 (Operations), 1st Battalion, 5th Field Artillery, Fort Riley, Kansas
May 84	May 85	Student, Department of Systems Engineering, University of Virginia, Charlottesville, Virginia
May 85	Jun 88	Instructor, later Assistant Professor Department of Mathematics, United States Military Academy, West Point, New York
Jun 88	Jun 89	Student, United States Army Command and General Staff College, Fort Leavenworth, Kansas
Jun 89	Mar 91	Brigade Fire Support Officer, later Executive Officer, 2d Battalion, 5th Field Artillery, 1st Infantry Division, United States Army Europe and Seventh Army, Germany
Apr 91	Mar 92	Division Artillery Observer Controller, Mobile Training Team - B, Battle Command Training Program, Fort Leavenworth, Kansas

MG Rhett A. Hernandez

Mar 92	Jun 94	Executive Officer to the Commanding General, United States Army Combined Arms Center, Fort Leavenworth, Kansas
Jun 94	Jun 96	Commander, 1st Battalion, 14th Field Artillery, 2d Armored Division, later redesignated 3d Battalion, 16th Field Artillery, 4th Infantry Division (Mechanized), Fort Hood, Texas
Jun 96	Jun 97	Strategic Planner, Officer Personnel Management System (OPMS XXI) Task Force, Alexandria, Virginia
Jun 97	Jun 98	Student, National War College, Fort Leslie J. McNair, Washington, DC
Jun 98	Jun 00	Commander, Division Artillery, 4th Infantry Division (Mechanized), Fort Hood, Texas
Jun 00	Aug 02	Chief, Operations Division, J-39, The Joint Staff, Washington, DC
Aug 02	Sep 03	Assistant Division Commander (Support), 1st Armored Division, United States Army Europe and Seventh Army, Germany and OPERATION IRAQI FREEDOM, Iraq
Sep 03	Jul 05	Director, Officer Personnel Management Directorate, United States Army Human Resources Command, Alexandria, Virginia
Aug 05	Oct 06	Commanding General, United States Army Human Resources Command, Alexandria, Virginia
Nov 06	May 09	Chief, United States Military Training Mission Saudi Arabia, United States Central Command, Saudi Arabia
May 09	Present	Assistant G-3/5/7, United States Army, Washington, DC

SUMMARY OF JOINT ASSIGNMENTS	DATE	GRADE
Chief, Operations Division, J-39, The Joint Staff, Washington, DC	Jun 00-Aug 02	Colonel
Chief, United States Military Training Mission Saudi Arabia, United States Central Command, Saudi Arabia	Nov 06-May 09	Major General

SUMMARY OF OPERATIONS ASSIGNMENTS	DATE	GRADE
Assistant Division Commander (Support), 1st Armored Division, United States Army Europe and Seventh Army, OPERATION IRAQI FREEDOM, Iraq	May 03-Jul 03	Brigadier General

US DECORATIONS AND BADGES

Distinguished Service Medal
Defense Superior Service Medal (with Oak Leaf Cluster)
Legion of Merit (with Oak Leaf Cluster)
Bronze Star Medal
Meritorious Service Medal (with 4 Oak Leaf Clusters)
Army Commendation Medal (with 4 Oak Leaf Clusters)
Army Achievement Medal (with Oak Leaf Cluster)
Joint Chiefs of Staff Identification Badge

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

DEPARTMENT OF THE AIR FORCE

PRESENTATION TO THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON TERRORISM AND UNCONVENTIONAL THREATS
U.S. HOUSE OF REPRESENTATIVES

SUBJECT: Operating in the Digital Domain: Organizing the Military Departments for Cyber Operations

STATEMENT OF: Major General Richard E. Webber, USAF
Commander
Twenty-fourth Air Force (AFCYBER)

September 23, 2010

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

I would like to thank Chairwoman Loretta Sanchez, Ranking Member Jeff Miller and the other distinguished Members of the Subcommittee for the opportunity to appear before you and represent the dedicated and exceptional men and women of Twenty-Fourth Air Force (24 AF). First, I would like to take this opportunity to highlight some of the Command's recent accomplishments. Twenty-Fourth Air Force just celebrated its one-year anniversary and I am proud of the 15,000 active duty, guardsmen, reservists, government civilians and contractors under my command. It has been an exciting year and we have made significant progress in transforming our Cyber force to operate with the rigor and discipline of their Air and Space counterparts. As our Secretary of the Air Force and Chief of Staff of the Air Force stated, "Our goal is to protect our mission-critical infrastructure, improve our capabilities, and develop greater cyber expertise and awareness to complement the entire Department of Defense cyberspace effort."

In the September issue of *Foreign Affairs* magazine, Deputy Secretary of Defense William Lynn said, "Information technology enables almost everything the U.S. military does." Our reliance on Cyber has gradually increased over three decades and as military operations became increasingly dependent upon Cyber; our Air Force leadership realized the need to "operationalize" Cyber. In the military sense, "operationalize" means applying the rigor, precision and discipline to processes commensurate with their importance. Additionally, it means bringing standardization, operational planning processes, and a "mission-focused" mindset to achieving supported commanders' objectives. In the Air Force, we've operationalized Air and Space operations because we've learned the lessons associated with success and failure in those domains. Often, if we fail in Air or Space, we pay with the lives of our Joint warfighters. Today, with virtually all of our advanced military capabilities reliant upon Cyber, we cannot afford failure in cyberspace.

Air Force Cyber Forces

In October 2008 the Secretary of the Air Force designated Air Force Space Command (AFSPC) as the lead Air Force Major Command to organize, train and equip cyber forces. Twenty-Fourth Air Force was established by the Secretary of the Air Force to "plan and conduct

Cyberspace operations in support of the combatant commands and to maintain and defend the Air Force Enterprise Network." We have established our operations center and we've begun deliberate planning efforts with USCYBERCOM. On September 11, 2010, the AFSPC Inspector General conducted an assessment and declared Twenty-Fourth Air Force "Ready" for Full Operational Capability (FOC). In October, we anticipate declaring 24 AF fully operational.

There are numerous ways that Twenty-Fourth Air Force has made progress towards achieving this major FOC milestone. I would like to touch on four significant examples. First, we have undertaken an extensive effort to collaborate with our fellow Air Force components in other combatant commands in order to integrate cyberspace courses of action into their operational plans. This is a distinct transition from the legacy approach, in which cyber was relegated to only a support role focused on "assuring the network" rather than "assuring the mission." Second, we have made significant strides in obtaining dedicated intelligence resources to directly support our cyberspace operations. As a result, we are shifting from a traditional, reactive network defense posture to one that is more predictive and dynamic. Ultimately, this significantly facilitates our ability to predict and deter attacks before they even take place. Third, we have worked with Air Force Space Command to radically restructure and train our cyberspace professional workforce, both at the officer and enlisted levels, to produce capable, vigilant cyberspace personnel with an operational rather than maintenance-only mindset focused on protecting and advancing the overall mission. Air Force Cyber warriors now have a formal professional development program combining education, training, and experience. Cyber instruction is now an integral part of the Basic Military Training and Professional Military Education curriculum. We have comprehensive mission qualification training for our cyber operators, and consider them "mission ready" on par with our aviators and space operators. Furthermore, we are designating the best of the best to hone our cyber tactics, techniques and procedures by integrating them at Nellis Air Force Base with the preeminent Air Force tacticians from all other air and space disciplines.

Fourth, we have streamlined our acquisition processes to give our Airmen the cyberspace tools they need, when they need them. Our acquisition professionals will have the processes and authorities needed to rapidly deliver Cyber capabilities for operations in an increasingly dynamic and contested environment. Everything we do begins and ends with the needs of the Joint Force Commanders and our measure of merit is how well we contribute to the Joint team.

Twenty-Fourth Air Force units establish, extend, operate, and defend our networks, operate through an attack, and present capabilities to the Joint warfighter that are robust, diverse, and some of the most advanced in the world. We are dedicated to Total Force Integration and are heavily dependent upon the Air Reserve Component for current operations and the future growth of Air Force Cyber capabilities. We are working with the National Guard Bureau and Air Force Reserve Command to identify opportunities to transition guard and reserve units to Cyber mission areas.

Twenty-Fourth Air Force has three subordinate wings, the 67th Network Warfare Wing (67 NWW), located at Lackland AFB, the 688th Information Operations Wing (688 IOW), also located at Lackland AFB, and the 689th Combat Communications Wing (689 CCW) at Robins AFB, Georgia.

The 67 NWW is charged as the Air Force execution element for Air Force Network Operations and provides full spectrum capabilities to Air Force, Joint Task Force and combatant commanders. The 67 NWW operates, manages, and defends global Air Force information networks. Additionally, the 67 NWW performs electronic systems security assessments for the Air Force and Joint community. As the Air Force's only network warfare wing, it has Airmen around the world conducting and supporting Cyber operations.

The 688 IOW delivers proven information operations, engineering and infrastructure capabilities integrated across air, space and cyberspace. The 688 IOW is responsible for creating the information operations advantage for combatant forces through exploring, developing, applying and transitioning counter information technology, strategy, tactics and data. In addition, the 688 IOW trains Airmen in Network Warfare skills, Information Operations, and develops Initial and Mission Qualification Training for Air Force Cyber units.

The 689 CCW delivers combat communications for the Joint and coalition warfighter supporting global combat operations and Humanitarian Relief Operations. They can deliver, at short notice, modern network and voice communications anywhere in the world. They have provided support to domestic and foreign humanitarian response actions including Hurricane Katrina and the recent earthquake disasters in Haiti and Chile. The combat communications mission also includes the largest percentage of 24 AF's aligned reserve component assets, with over 6,000 aligned Air Guard and Reserve members.

The 624th Operations Center (624 OC), collocated with 24 AF at Lackland AFB serves as 24 AF's command and control center to provide robust full-spectrum and integrated cyberspace operations capabilities. The 624 OC directs defense and crisis response for the AF network and issues Cyber orders on my behalf. The 624 OC's organizational structure is aligned with its operational counterparts, theater and functional Air Operations Centers, and USCYBERCOM to facilitate the integration of Air Force Cyber capabilities into the supported COCOM commander's existing structure.

Mission Assurance

Establishing 24 AF created one commander to oversee Cyber operations for the AF and gave that commander authority no previous entity had to enact the changes necessary to operationalize AF Cyber. One of our top priorities has been to change the AF paradigm from network assurance to mission assurance. Airmen must stop thinking of themselves as only compartmented specialists, such as maintainers, communicators, or intelligence experts, and begin thinking of themselves as an integrated team of multi-disciplined professionals with the technical and tactical capacity and responsibility to execute Joint Cyber operations.

Under the mission assurance paradigm, we are no longer communicators; we are "Cyberspace Operators." We have centered the focus on conducting the mission, not just providing a service. We are also conducting deliberate planning with the Component Numbered Air Force (C-NAF) commanders, which are the leaders of the Air Force warfighting units presenting forces to the Combatant Commanders. We are working with them to identify the assets these warfighters must have in order to execute their Joint mission. We then prioritize those critical assets and map their dependencies to capabilities and infrastructure in cyberspace. Once we know where those dependencies lie, we perform analysis to determine what vulnerabilities and failure points in cyberspace threaten those critical assets. These threats can be malicious or simply accidental. Regardless, we take responsibility for identifying, proactively preventing, or in the worst case, rapidly recovering from an incident to avoid mission failure.

Operate Through an Attack

The goal of mission assurance is to develop the ability to operate through a Cyber attack or outage and accomplish the mission. In contrast to the network assurance paradigm's isolationist response, an "operate through" response means we keep the network up during an attack and defend those critical assets the warfighter needs to complete the mission. The mission will not fail because of a lack of freedom of movement in cyberspace. This could mean that we may have to sacrifice less critical assets or even networks during an attack, but we will do so knowingly, in accordance with broader military objectives.

The first critical component required to develop the capability to operate through an attack is to evolve from a perimeter-defense strategy to a defense-in-depth strategy. Our approach to Cyber security in the past had been to build walls around the network higher and thicker. This puts all of our protection at our borders and protects everything inside to the same standard. This perimeter-defense strategy is similar to the Maginot Line strategy applied during World War II. A Cyber perimeter-defense strategy has proven similarly ineffective: once an adversary breaches our defensive barriers, they have the run of our networks and we have difficulty tracking and expelling them. As Frederick the Great is credited with saying, "He who defends everything defends nothing."

Instead, we are pursuing a defense-in-depth strategy that segregates internal assets based on their prioritization as determined during deliberate planning. We build defended asset lists, map our Cyber dependencies, and provide higher levels of security for more valuable, mission-critical resources. Attackers must therefore overcome increasingly greater protections to gain unauthorized access to higher value resources. Moreover, with our situational awareness tools focused on critical assets we can detect important unauthorized access or activities much faster.

Defense in depth requires deliberate planning and an understanding of the missions we are assuring in order to correctly apply risk analysis and mitigation. We will develop close relationships with the other C-NAFs and understand both their missions and the current and upcoming missions of the Combatant Commands (COCOMs) they support. This is an extremely broad body of knowledge for any one organization to tackle. To facilitate the requisite exchange of expertise between mission planners and Cyber planners, we have established a Cyber Operations Liaison Element (COLE) construct.

The COLE is based on the Special Operations Liaison Element (SOLE) concept the Special Forces community developed during Operation DESERT STORM. They found the best way to utilize and integrate Special Forces teams was to inject Special Forces planners at the planning focal point. The COLE applies this concept for Cyber operations and planning. The COLE personnel are expert Cyber planners with a detailed understanding of the Cyber capabilities the Air Force can bring to bear. They integrate with their counterpart C-NAF planners to incorporate commander's intent during the operational planning process. This helps ensure Cyber capabilities are considered when courses of action are developed, analyzed, and chosen. During crisis action, the COLE will work with mission planners in the Air Operations Centers to ensure full spectrum Cyber is integrated into the Air Tasking Order process.

Today, we have established a COLE in the CENTCOM theater in support of Operations ENDURING FREEDOM and NEW DAWN (formerly IRAQI FREEDOM). We are supporting the other C-NAFs virtually with COLEs that interact through remote means with planners and that travel regularly to support planning and crisis response events. Ultimately, we envision permanent COLEs for each of the ten other C-NAFs. We also saw promising results from COLE support to USPACOM/PACAF and USEUCOM/USAFE during Exercises TERMINAL FURY and AUSTERE CHALLENGE.

Cyberspace Situational Awareness

Another critical component required to develop the capability to operate through an attack is robust cyberspace situational awareness. An important characteristic of cyberspace that sets it apart from the other domains is that it is constantly changing, and it does so at the will of the operators. We can expand, contract, or segment cyberspace. Every time we add a server or apply a patch or install a program, we change the domain. This inherent malleability of Cyberspace makes it vitally important for us to have a real-time picture of the cyberspace landscape.

Imagine the consequences for military operations in the traditional domains of Air, Land, and Sea if commanders were blind to significant and continuous changes in their domains. How would we defend a base if the perimeter fence could have sections disappear and our security forces had no way to detect the gap until their next patrol? Or, perhaps a targeted weapons factory could be instantly relocated to a different country by the adversary? And what if an aircraft carrier could be misconfigured and inadvertently placed outside fleet defenses and within torpedo range of enemy submarines? Comparable situations exist in cyberspace and the consequences of a Cyber attack can have impact in microseconds. Therefore, we must be eternally vigilant and globally aware in the cyberspace domain or we risk becoming vulnerable and defensively deficit.

My number one priority for 24 AF is developing and improving cyberspace situational awareness. The Air Force network is one of the largest and most complex networks in the world with over six-hundred-and thirty-thousand computers. We simply cannot monitor every machine all the time. Therefore, we need smart software that can monitor and report on the status of those machines and their interconnections to my operations center. Today, we operate several legacy situational awareness systems which were fielded years ago during the process that created the Air Force network. Those systems only partially meet our current situational awareness needs and we are reliant on manual processes which slow our response time.

We are working to build a single, integrated cyberspace situational awareness picture for the Air Force enterprise. Initially, we're working to bring together a number of existing feeds from Cyber sensors across the Air Force to build a consolidated operational picture. Future efforts will combine, integrate, and enhance these existing data feeds. We plan to fuse situational awareness for our global or regional C-NAFs around their defended asset lists. We will also work to add decision support, planning, assessment, and command and control capabilities. This combination will enable a single operational level, correlated picture to support course of action development and decision making. Ultimately, the operational requirement is for more than just awareness; comprehensive situational awareness is a critical component to global network command and control.

Comprehensive situational awareness also enables the ability to coordinate activities and efforts with other network defenders, such as our sister Services and USCYBERCOM. We are cooperating with USCYBERCOM to provide a Cyber feed to their operations center, and USCYBERCOM plans to share feeds from the sister services with 24 AF. This exchange of Cyber pictures will increase the overall situational awareness for the entire DoD community and allows us to detect, respond to and prevent widespread Cyber attacks and outages. Moreover, as we share our situational awareness planning efforts with USCYBERCOM, their overall understanding of each of the services' efforts will prevent wasteful duplication of effort. A consolidated Cyber picture, coupled with a simplified, standardized architecture ultimately will improve our ability to operate through an attack.

Joint Integration

The integration of cyber capabilities in support of Joint operations is absolutely essential. We integrate operations across domains; we do not integrate domains. Each of these interlocking capabilities must integrate seamlessly to ensure mission success. The Air Force develops capabilities in support of our Service Core Competencies and this holds true for Air Force Cyber capabilities. Since air, space and cyberspace are inextricably linked, both operationally and technically, the potential exists to integrate capabilities across these domains to exponentially increase each other's effectiveness. This integration promises to give Joint force commanders unrivaled global access, persistence, awareness and connectivity capabilities.

Conclusion

Deputy Secretary of Defense Lynn summarized thirty years of cyberspace development when he said, "Information technology in the military has evolved from an administrative tool for enhancing office productivity into a national strategic asset in its own right." In this technology-driven age, it is not feasible to conduct operations without access to cyberspace. In a letter to Airmen, the Secretary of the Air Force and Chief of Staff of the Air Force stated that "[c]yberspace pervades everything we do, in every domain, and extends from your workspace to the battlespace." As such, the Air Force is committed to producing Cyber professionals dedicated to assuring the Joint mission and preserving our freedom of action in cyberspace. Furthermore, because Cyber operations is a team sport, I and the men and women of 24 AF are proud to work alongside our teammates in USCYBERCOM and our sister services. I thank the Committee for your continued support as we endeavor to meet the challenges of defending Cyberspace for the Joint warfighter.

MAJOR GENERAL RICHARD E. WEBBER, USAF

Maj. Gen. Richard E. Webber is the Commander, 24th Air Force and Air Force Network Operations, Lackland Air Force Base, Texas. General Webber is responsible for the Air Force's newest 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 wings, two located at Lackland AFB, and one located at Robins AFB, Ga.

General Webber was commissioned a second lieutenant upon graduation from the U.S. Air Force Academy in 1975. He has commanded a missile squadron, support group, missile operations group, and missile wing equivalent and two space wings. His staff assignments include Headquarters North Atlantic Treaty Organization International Military Staff, the Air Staff, Headquarters Strategic Air Command, Headquarters Air Force Space Command, and Vice Commander of the Aerospace Command and Control & Intelligence, Surveillance and Reconnaissance Center.

General Webber is a command space and missile operator with qualifications in the Minuteman II, Minuteman III, Global Positioning Satellite and Counter Communications System weapon systems. Prior to his current assignment, he served as Assistant Deputy Chief for Air, Space and Information Operations, Plans and Requirements, Headquarters U.S. Air Force, Washington, D.C.

EDUCATION

1975 Bachelor of Science degree in management, U.S. Air Force Academy, Colorado Springs, Colo.
1978 Master's degree in business administration and personnel management, University of Missouri, Columbia
1978 Distinguished graduate, Squadron Officer School, Maxwell AFB, Ala.
1985 Distinguished graduate, College of Command and Staff, Naval War College, Newport, R.I.
1985 Master's degree in national security and strategic studies, College of Command and Staff, Naval War College, Newport, R.I.
1992 Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington, D.C.
1999 Program for Executives, Carnegie-Mellon University, Pittsburgh, Pa.
2002 Capstone, National Defense University, Washington, D.C.
2003 LOGTECH Executive Education, University of North Carolina at Chapel Hill
2006 National Security Leadership Course, Syracuse University, N.Y.

2007 Enterprise Leadership Seminar, University of North Carolina at Chapel Hill
2008 System Acquisition Management, Defense Aeronautical University, Fort Belvoir, Va.

ASSIGNMENTS

1. February 1976 - October 1980, missile combat crew member, instructor missile deputy combat crew commander, instructor missile combat crew commander, wing emergency war order planner and instructor, and emergency rocket communication system emergency war order instructor, 351st Strategic Missile Wing, Whiteman AFB, Mo.
2. October 1980 - October 1981, Air Staff Training Program officer, Strategic Missile Division and Force Analysis Division, Air Force Studies and Analysis, Washington, D.C.
3. November 1981 - August 1984, Chief, Future Intercontinental Ballistic Missile Systems Branch, Directorate of Plans and Operations, Headquarters Strategic Air Command, Offutt AFB, Neb.
4. August 1984 - June 1985, student, College of Command and Staff, Naval War College, Newport, R.I.
5. June 1985 - April 1989, missile operations staff officer, Strategic Offensive Force Division, Air Force Plans Directorate, Washington, D.C.
6. April 1989 - July 1991, Commander, 508th Strategic Missile Squadron, Whiteman AFB, Mo.
7. August 1991 - August 1992, student, Industrial College of the Armed Forces, Washington, D.C.
8. August 1992 - July 1994, Chairman, Allied Data Systems Interoperability Agency, and Chief, Systems Interoperability Branch, Headquarters North Atlantic Treaty Organization and International Military Staff, Brussels, Belgium
9. July 1994 - July 1995, Commander, 341st Support Group, Malmstrom AFB, Mont.
10. July 1995 - July 1996, Commander, 341st Operations Group, Malmstrom AFB, Mont.
11. July 1996 - October 1997, Commander, 321st Missile Group, Grand Forks AFB, N.D.
12. October 1997 - June 1999, Vice Commander, Aerospace Command and Control & Intelligence, Surveillance and Reconnaissance Center, Langley AFB, Va.
13. June 1999 - April 2001, Commander, 50th Space Wing, Schriever AFB, Colo.
14. April 2001 - April 2002, Inspector General, Air Force Space Command, Peterson AFB, Colo. (October 2001 - March 2002, Assistant Combined Air Operations Center Director for Space and Information Warfare, Prince Sultan Air Base, Saudi Arabia)
15. April 2002 - August 2002, Deputy Director, Operations, Headquarters AFSPC, Peterson AFB, Colo.
16. August 2002 - February 2003, Director, Communications and Information Systems, and Chief Information Officer, Headquarters AFSPC, Peterson AFB, Colo.
17. February 2003 - March 2004, Director, Logistics and Communications, Chief Information Officer and Chief Sustainment Officer, Headquarters AFSPC, Peterson AFB, Colo. (March 2003 - May 2003, Deputy Director of Operations for Space and Information Operations, U.S. Central Command, Southwest Asia)

18. March 2004 - November 2005, Commander, 21st Space Wing, Peterson AFB, Colo.
19. November 2005 - January 2008, Director of Installations and Mission Support, Headquarters AFSPC, Peterson AFB, Colo.
20. January 2008 - August 2009, Assistant Deputy Chief for Air, Space and Information Operations, Plans and Requirements, Headquarters U.S. Air Force, Washington, D.C.
21. August 2009 - present, Commander, 24th Air Force, Lackland AFB, Texas

SUMMARY OF JOINT ASSIGNMENTS

1. August 1992 - July 1994, Chairman, Allied Data Systems Interoperability Agency, and Chief, Systems Interoperability Branch, Headquarters North Atlantic Treaty Organization and International Military Staff, Brussels, Belgium, as a colonel
2. October 2001 - March 2002, Assistant Combined Air Operations Center Director for Space and Information Warfare, Prince Sultan Air Base, Saudi Arabia, as a colonel and brigadier general
3. March 2003 - May 2003, Deputy Director of Operations for Space and Information Operations, U.S. Central Command Forward, Southwest Asia, as a brigadier general

MAJOR AWARDS AND DECORATIONS

Distinguished Service Medal
Defense Superior Service Medal
Legion of Merit with two oak leaf clusters
Bronze Star Medal
Defense Meritorious Service Medal
Meritorious Service Medal with four oak leaf clusters
Air Force Commendation Medal
Air Force Achievement Medal
Air Force Outstanding Unit Award with silver oak leaf cluster
Air Force Organizational Excellence Award
Combat Readiness Medal
National Defense Service Medal with bronze star
Global War on Terrorism Expeditionary Medal
Global War on Terrorism Service Medal
Humanitarian Service Medal with bronze star
Air Force Overseas Ribbon-Long
Air Force Expeditionary Service Ribbon with Gold Border and oak leaf cluster
Small Arms Expert Marksmanship Ribbon with bronze star

EFFECTIVE DATES OF PROMOTION

Second Lieutenant June 4, 1975
First Lieutenant June 4, 1977

Captain June 4, 1979
Major Aug. 1, 1984
Lieutenant Colonel July 1, 1988
Colonel Jan. 1, 1992
Brigadier General Jan. 1, 2002
Major General July 14, 2006

(Current as of February 2010)

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

SEPTEMBER 23, 2010

QUESTIONS SUBMITTED BY MS. SANCHEZ

Ms. SANCHEZ. Have DOD and U.S. Cyber Command provided the services with clear doctrine, guidance, policies, and/or requirements to accomplish their cyberspace operations mission?

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. What additional doctrine, guidance, policies, and/or requirements do the services need from DOD and U.S. Cyber Command to accomplish their cyberspace operations mission?

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Please describe the doctrine, guidance, policies, and/or requirements the services are developing individually and in coordination with one another?

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Given current budget and personnel constraints (i.e. shrinking end strength and heightened operational demands), describe steps you are taking to meet your requirements to fund and staff your cyberspace operations?

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. What efforts have the services made to define the emerging role of the cyber warrior for both service-specific and joint cyberspace operations mission areas (including the development of mission specialties, job qualification and training opportunities)?

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

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

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. How are you integrating cyber capabilities into Service-level, joint, international or interagency exercises?

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

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

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

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

Admiral MCCULLOUGH. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Can you please explain your understanding of command and control responsibilities, relationships and authorities between U.S. Cyber Command and the military services?

General FLYNN. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Have DOD and U.S. Cyber Command provided the services with clear doctrine, guidance, policies, and/or requirements to accomplish their cyberspace operations mission?

General FLYNN. [The information referred to was not available at the time of printing].

Ms. SANCHEZ. What additional doctrine, guidance, policies, and/or requirements do the services need from DOD and U.S. Cyber Command to accomplish their cyberspace operations mission?

General FLYNN. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Please describe the doctrine, guidance, policies, and/or requirements the services are developing individually and in coordination with one another?

General FLYNN. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Given current budget and personnel constraints (i.e. shrinking end strength and heightened operational demands), describe steps you are taking to meet your requirements to fund and staff your cyberspace operations?

General FLYNN. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. What efforts have the services made to define the emerging role of the cyber warrior for both service-specific and joint cyberspace operations mission areas (including the development of mission specialties, job qualification and training opportunities)?

General FLYNN. [The information referred to was not available at the time of printing.]

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

General FLYNN. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. How are you integrating cyber capabilities into Service-level, joint, international or interagency exercises?

General FLYNN. [The information referred to was not available at the time of printing.]

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

General FLYNN. [The information referred to was not available at the time of printing.]

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

General FLYNN. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Can you please explain your understanding of command and control responsibilities, relationships and authorities between U.S. Cyber Command and the military services?

General HERNANDEZ. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Have DOD and U.S. Cyber Command provided the services with clear doctrine, guidance, policies, and/or requirements to accomplish their cyberspace operations mission?

General HERNANDEZ. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. What additional doctrine, guidance, policies, and/or requirements do the services need from DOD and U.S. Cyber Command to accomplish their cyberspace operations mission?

General HERNANDEZ. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Please describe the doctrine, guidance, policies, and/or requirements the services are developing individually and in coordination with one another?

General HERNANDEZ. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Given current budget and personnel constraints (i.e. shrinking end strength and heightened operational demands), describe steps you are taking to meet your requirements to fund and staff your cyberspace operations?

General HERNANDEZ. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. What efforts have the services made to define the emerging role of the cyber warrior for both service-specific and joint cyberspace operations mission areas (including the development of mission specialties, job qualification and training opportunities)?

General HERNANDEZ. [The information referred to was not available at the time of printing.]

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

General HERNANDEZ. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. How are you integrating cyber capabilities into Service-level, joint, international or interagency exercises?

General HERNANDEZ. [The information referred to was not available at the time of printing.]

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

General HERNANDEZ. [The information referred to was not available at the time of printing.]

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

General HERNANDEZ. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Can you please explain your understanding of command and control responsibilities, relationships and authorities between U.S. Cyber Command and the military services?

General WEBBER. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Have DOD and U.S. Cyber Command provided the services with clear doctrine, guidance, policies, and/or requirements to accomplish their cyberspace operations mission?

General WEBBER. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. What additional doctrine, guidance, policies, and/or requirements do the services need from DOD and U.S. Cyber Command to accomplish their cyberspace operations mission?

General WEBBER. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Please describe the doctrine, guidance, policies, and/or requirements the services are developing individually and in coordination with one another?

General WEBBER. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. Given current budget and personnel constraints (i.e. shrinking end strength and heightened operational demands), describe steps you are taking to meet your requirements to fund and staff your cyberspace operations?

General WEBBER. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. What efforts have the services made to define the emerging role of the cyber warrior for both service-specific and joint cyberspace operations mission areas (including the development of mission specialties, job qualification and training opportunities)?

General WEBBER. [The information referred to was not available at the time of printing.]

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

General WEBBER. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. How are you integrating cyber capabilities into Service-level, joint, international or interagency exercises?

General WEBBER. [The information referred to was not available at the time of printing.]

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

General WEBBER. [The information referred to was not available at the time of printing.]

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

General WEBBER. [The information referred to was not available at the time of printing.]

Ms. SANCHEZ. The committee is aware that there is an Application Software Assurance Center of Excellence (ASACOE) at Gunter Annex, Alabama that has been recognized by the DOD for its software vulnerability analysis tools and methodologies. What role does the ASACOE in 24th Air Force efforts to secure AF networks? Is the ASACOE a program of record with funding across the FYDP to support additional software vulnerability analysis work from the AF, or with other services, defense agencies or Federal partners?

General WEBBER. [The information referred to was not available at the time of printing.]

○