



MARCH 4, 2015

# CYBER OPERATIONS: IMPROVING THE MILITARY CYBER SECURITY POSTURE IN AN UNCERTAIN THREAT ENVIRONMENT

U.S. HOUSE COMMITTEE ON ARMED SERVICES

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

---

## HEARING CONTENTS:

### WITNESS STATEMENTS

**Admiral Michael Rogers, USN** [\[view pdf\]](#)  
Commander, U.S. Cyber Command

**Lieutenant General Edward C. Cardon, USA** [\[view pdf\]](#)  
Commander, U.S. Army Cyber Command

**Vice Admiral Jan Tighe, USN** [\[view pdf\]](#)  
Commander, Navy Fleet Cyber Command / 10<sup>th</sup> Fleet (FCC/C10F)

**Major General Daniel J. O'Donohue, USMC** [\[view pdf\]](#)  
Commanding General, MARFORCYBER

**Major General Burke E. Wilson, USAF** [\[view pdf\]](#)  
Commander, 24<sup>th</sup> Air Force

### AVAILABLE WEBCASTS

**3.4.2015 – Cyber Operations: Improving the Military Cyber Security Posture...**  
(via youtube and HTML5 player)  
<https://youtu.be/rdBUPI2tNFI>

### COMPILED FROM:

<http://armedservices.house.gov/index.cfm/2015/3/cyber-operations-improving-the-military-cyber-security-posture-in-an-uncertain-threat-enviornment>

*\* Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

STATEMENT OF  
ADMIRAL MICHAEL S. ROGERS  
COMMANDER  
UNITED STATES CYBER COMMAND  
BEFORE THE  
HOUSE COMMITTEE ON ARMED SERVICES  
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES  
4 MARCH 2015

Chairman Wilson, Representative Langevin, and distinguished members of the Committee, thank you for the opportunity to speak to you today on behalf of the men and women of United States Cyber Command (USCYBERCOM). This is the first time I have had the honor of testifying before this Committee in a posture hearing about our Command's dedicated uniformed and civilian personnel. It gives me not only pride but great pleasure to commend their accomplishments, and I am both grateful for and humbled by the opportunity I have been given to lead them in the important work they are doing in defense of our nation.

USCYBERCOM is a subunified command of U.S. Strategic Command; we are based at Fort Meade, Maryland. Approximately 1,100 people (military, civilians, and contractors) serve at USCYBERCOM, with a Congressionally-appropriated budget for Fiscal Year 2015 of approximately \$509 million for Operations and Maintenance (O&M), Research, Development, Test and Evaluation (RDT&E), and military construction (MILCON). USCYBERCOM also includes its key Service cyber components: Army Cyber Command/Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force. Our collective missions are to direct the operation and defense of the Department of Defense's information networks while denying adversaries (when authorized) the freedom to maneuver against the United States and its allies in and through cyberspace. On a daily basis, we plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of specified Department of Defense information networks and the Department's critical infrastructure; and prepare to and, when directed, conduct full-spectrum military cyberspace

operations in order to enable actions in all domains, ensure U.S. and allied freedom of action in cyberspace and deny the same to our adversaries.

USCYBERCOM operates with several key mission partners. Foremost is the National Security Agency and its affiliated Central Security Service (NSA/CSS). The President's decision to maintain the "dual-hat" arrangement (under which the Commander of USCYBERCOM also serves as the Director of NSA/Chief, CSS) means the partnership of USCYBERCOM and NSA/CSS will continue to benefit our nation. NSA/CSS has unparalleled capabilities for detecting foreign threats, producing intelligence for our warfighters in all domains, analyzing cyber events, and guarding national security information systems. The best, and only, way to meet our nation's needs, to bring the military cyber force to life, to exercise good stewardship of our nation's resources, and to ensure respect for civil liberties and privacy, is to leverage the capabilities (both human and technological) that have been painstakingly built up at Fort Meade. Our nation has neither the time nor the resources to re-learn or re-create the capabilities that we tap now by working with our co-located NSA/CSS partners.

Let me also mention another key mission partner and neighbor at Fort Meade, the Defense Information Systems Agency (DISA). DISA is vital to the communications and the efficiency of the entire Department, and its people (especially those supporting the new Joint Force Headquarters-DoD Information Networks) operate in conjunction with us at USCYBERCOM on a constant basis. We also work with other federal government departments and agencies, particularly the Department of Homeland Security (DHS) and the Department of Justice and Federal Bureau of Investigation (FBI). We interact regularly with private industry and key allied nations as they seek to secure their networks, identify adversarial and criminal

actors and intentions, build resiliency for federal and critical infrastructure systems, and investigate the theft and manipulation of data.

### *Where We Were*

This year we will mark the fifth anniversary of USCYBERCOM's activation. The Department authorized the creation of a Cyber Command in 2009, and accelerated its establishment the following year. This initiative was truly reflective of a broad consensus. The highest levels of our government saw potential adversaries militarizing cyberspace, mounting cyber espionage on a world-wide scale and using cyber capabilities to intimidate their neighbors. We also saw cyber efforts against DoD and realized the need to ensure our ability to defend its networks and command and control our own Department's forces and information systems. We in the U.S. military took the step of creating a new warfighting organization for cyberspace because we recognized that our nation's economy, infrastructure, and allies were incurring grave risks from digital disruption, and that potential adversaries were working aggressively to exploit those vulnerabilities. We saw unfriendly states, organized criminals, and even unaffiliated cyber actors stealing American intellectual property and using cyber means for coercion. USCYBERCOM was established to help stop such activities, or at least to minimize their effects on the United States and its allies.

USCYBERCOM confronted serious challenges from the outset. DoD networks had been planned and initially constructed decades earlier in an environment in which redundancy, resiliency, and defensibility were not always primary design characteristics. Operators in USCYBERCOM, not surprisingly, could not even see all of our networks, let alone monitor all the traffic coming into and out of them from the Internet. Our people were and are professionals,

so that issue was rapidly engaged, but nonetheless the sheer volume of work involved in starting a new, subunified command was substantial.

I have been at USCYBERCOM for approximately a year, and thus have had time to form some impressions of the organization and its progress. I knew when I took command that we had a sound foundation and could build upon it with confidence. The organizations had been well scoped and granted the authorities necessary to do our work. The bad news was that USCYBERCOM was built from the ground up by cutting manning to the bone, initially sacrificing vital support functions and institutional infrastructure to build mission capabilities as fast as possible. I was nonetheless pleased by the quality and dedication of the personnel across USCYBERCOM and our Service cyber components. These are professionals, in every sense of the word, and they are determined to put in place military cyber capabilities that will keep the nation safe in cyberspace. For their sake, and even more so for America's, I intend to make our organizations even stronger—and provide my successors the opportunity to do the same.

### *Where We Are Now*

Over the last five years we have built USCYBERCOM to help defend our networks in DoD and the nation. This has not always been a straightforward process. Our Command is growing and operating at the same time, performing a multitude of tasks across a diverse and complex mission set. Of course, every command changes with events in its mission space, adjusts to evolving policies and direction, and adapts with the development of armaments and tactics. I do not want to foster the impression that we are completely unique. It is true, nonetheless, that we are constructing a new command and force while engaged on a 24-hour a day basis, every day of the year, with smart, energetic actors operating in an environment that is

highly dynamic. Some of those actors, I hasten to add, operate with no discernible legal or ethical restraints. At the same time, we are writing doctrine, training people to execute options, and keeping up with the ever-shifting topography of cyberspace. That complexity presents us—and every nation that seeks a military cyber capability—with a set of challenges that are significant.

In essence, USCYBERCOM has been “normalizing” our operations in cyberspace. We seek to afford an operational outlook and attitude to the running of the Department’s roughly 7 million networked devices and 15,000 network enclaves. Collectively these represent a weapons system analogous to a carrier strike group or an aircraft strike package, through which we deliver effects. Like conventional weapons systems, our networks enable operations in other domains and distant locations, they demand constant upkeep and skillful handling, and they can be a target themselves for our adversaries. They give us the vital command and control (C2), connectivity, and intelligence for a global, 21<sup>st</sup> century military. No other nation enjoys such resources—they impart to us formidable advantages over any conceivable adversary. It is for exactly this reason that potential adversaries very much want to map, understand, exploit, and possibly disrupt our global network architecture.

In keeping with that operational mindset, we seek to impress upon commanders that cyber defense is no longer information technology (IT) it is not a mere support function that they can safely delegate to someone on their staff. Cyber is now a central part of their ability to execute their mission. It is commander’s business. A successful intrusion, or severance of connectivity, can result in a direct and immediate impact to successful mission accomplishment. We have seen this happen in recent years, and though we have not yet experienced a serious,

sustained disruption to the Department's information systems, it may be only a matter of time before we face one, given the inherent vulnerability of our networks.

The fragility of that legacy architecture motivates our emphasis on deploying the Joint Information Enterprise (JIE) across DoD. We have gained significantly more visibility in our networks, but that is only a stopgap measure while the Department migrates its systems to a cloud architecture that promises to increase security and efficiency while facilitating data sharing across the enterprise. That means that the warfighter at the forward edge of battle benefits from the same data pools as our analysts, operators, and senior decisionmakers here in the United States. While the JIE is being implemented, however, our concerns about our legacy architecture collectively have spurred our formation of our new Joint Force Headquarters to defend the Department's information networks (JFHQ-DoDIN). The JFHQ-DoDIN gained then-Secretary of Defense Hagel's authorization late last year and has recently achieved initial operational capability, working at DISA under my operational control at USCYBERCOM. JFHQ-DoDIN's mission is to oversee the day-to-day operation of DoD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses. Placing the just-established JFHQ-DoDIN under USCYBERCOM gives us a direct lever for operating DoD's information systems in ways that make them easier to defend, and tougher for an adversary to affect. It also gets us closer to being able to manage risk on a system-wide basis across DoD, balancing warfighter needs for access to data and capabilities while maintaining the overall security of the enterprise

USCYBERCOM directs the operation and defense of Department of Defense networks, but it does much more as well, hence its formation of a Cyber Mission Force (CMF) to turn strategy and plans into operational outcomes. The Command's last two annual posture

statements have mentioned the CMF's authorization and initial steps, and I am pleased to report that the Force is very much a reality. With continued support from Congress, the Administration, and the Department, USCYBERCOM and its Service cyber components are now about halfway through the force build for the CMF. Indeed, many of its teams are generating capability today. Three years ago we lacked capacity; we had vision and expertise but were very thin on the ground. Today the new teams are actively guarding DoD networks and prepared, when appropriate and authorized, to help Combatant Commands deny freedom of maneuver to our adversaries in cyberspace. Dozens of teams are now operating; and even though many of them are still filling out their rosters and qualifying their personnel, they are proving their value daily as well as confirming the overall need for such a construct.

The work of building the CMF is not done yet. We have a target of about 6,200 personnel in 133 teams, with the majority achieving at least initial operational capability by the end of FY 2016. I have been working with the Services to accelerate the work we are doing to keep on schedule, but I can promise you that will not be easy. We are already hard pressed to find qualified personnel to man our CMF rosters, to get them cleared, and to get them trained and supported across all 133 teams. To address these gaps, I am working with our Service components, Chief, National Guard Bureau, and Reserve Chiefs to ensure we have considered a total force solution. In several areas, such as critical infrastructure, both USCYBERCOM and the Services have recognized that our Reserve Component brings us unique and valuable skills. In addition, we are charting the proper command and control relationships and structures for these teams, seeking to establish proper headquarters support for them, and giving my commanders insight into their activities so we can ensure the best possible synchronization, deconfliction, and unity of effort across the CMF. There are all sorts of good ideas for doing

this; indeed, we hear no shortage of suggestions. What I tell everyone, however, is that we have admired this issue long enough. For instance, it is time to implement and exercise measures like the objective C2 model that we agreed upon as a Department almost two years ago, even if we believe it may not end up as the permanent solution. Let us see how it works, and then change what needs to be fixed later as we gain insights from operations and the shifting threat.

Where we need help from you is with resources required to hire personnel to fill the team seats as well as necessary operational and strategic headquarters operations, intelligence, and planning staffs, facilities where we can train and employ them, and resources to properly equip them. Everyone involved knows this is a priority for the Department as well as for the Administration writ large. We also know that our Department in particular has a broad range of critical priorities, each of which competes with cyberspace for resources. This is a cold, hard reality—as is the fact that weaknesses in cyberspace have the potential to hold back our successes in every other field where the Department is engaged. Similarly, success in securing our networks and denying adversaries freedom of maneuver in cyberspace can and does bolster our DoD successes in all warfighting domains. That should factor into our resource decisions, particularly as we face the renewed possibility of sequestration—and mandatory, across-the-board eight percent budget cuts—when Fiscal Year 2016 begins a few months from now.

Let me emphasize the value of the intangibles in our work and our environment. Collectively we in USCYBERCOM have gained priceless experience in cyberspace operations, and that experience has given us something even more valuable: insight into how force is and can be employed in cyberspace. We have had the equivalent of a close-in fight with an adversary, which taught us how to maneuver and gain the initiative that means the difference between victory and defeat.

Enhancing such insight is increasingly urgent. Every conflict in the world today has a cyber dimension. Actors with modest conventional military capabilities have shown considerable capacity to harass, disrupt, and distract their adversaries through digital means. This is not, however, some on-line version of a Hobbesian state of nature; it is not a war of all against all. What we are seeing are clear patterns to cyber hostilities, and those patterns have four main trends:

- First, it has to be noted that autocratic governments in several regions view today's open Internet as a lethal threat to their regimes. For example—as President Obama noted last December—North Korea recently turned its cyber capabilities on Sony Pictures Entertainment in revenge for a forthcoming movie. The North Koreans employed unlawful cyber activities to steal and destroy data and property, to intimidate and coerce U.S.-based businesses, to threaten American citizens, and to disrupt free speech within the United States. This is unacceptable. Democracies value Internet freedom and a multi-stakeholder system of governance, in which the Internet is officially neutral with regard to free and open political speech—with clear protection for criticism and debate. We make no apologies for the fact that such neutrality is abhorrent to regimes that fear their own citizens; hence their ubiquitous and determined efforts to redefine “cybersecurity” to mean protection from “dangerous” ideas as well as from malicious activity.
- Second are the ongoing campaigns to steal intellectual property. Massive thefts of personal and institutional information and resources, by states and by criminals, have been observed over the last decade or so. Criminals are mining

personal information for use in identity theft schemes, in a sense committing fraud on an industrial scale. States have turned their much greater resources to theft as well. These intrusions and breaches have drawn comments from the highest levels of the U.S. Government. I would only add here the observation that the most worrisome of these campaigns are state-sponsored, persistent, and world-wide in scope. They are aimed at governments, non-profits, and corporations wherever they might be accruing intellectual capital that the attackers believe could be valuable, whether for re-sale or passage to competing firms and industries.

- The third form of cyber tactic we see is disruption. Once again, the actors, techniques, and targets of these incidents are numerous and varied, ranging from denial-of-service attacks, network traffic manipulation, and employment of destructive malware. We see these used all over the world, particularly in most or all of the conflicts pitting two armed adversaries against one another.
- Finally, we see states developing capabilities and attaining accesses for potential hostilities, perhaps with the idea of enhancing deterrence or as a beachhead for future cyber sabotage. Private security researchers over the last year have reported on numerous malware finds in the industrial control systems of energy sector organizations. As I suggested in my appearance before the House Permanent Select Committee on Intelligence last fall, we believe potential adversaries might be leaving cyber fingerprints on our critical infrastructure partly to convey a message that our homeland is at risk if tensions ever escalate toward military conflict.

Despite the spread of cyber attacks and conflicts around the world, we have increasing confidence in our operations-based approach. Though it is still developing and not yet fully implemented, it has nonetheless given us significant advantages in relation to potential adversaries. For instance, I can tell you in some detail how USCYBERCOM and our military partners dealt with the Heartbleed and “Shellshock vulnerabilities that emerged last year. These were unrelated but serious flaws inadvertently left in the software that millions of computers and networks in many nations depend upon; an attacker could exploit those vulnerabilities to steal data or take control of systems. Both of these security holes were discovered by responsible developers who did just what they should have done in response—they kept their findings quiet and worked with trusted colleagues to develop software patches as quickly as possible—allowing systems administrators to gain the jump on bad actors who read the same vulnerability announcements and immediately began devising ways to identify and exploit unpatched computers.

We at USCYBERCOM (and NSA/CSS) learned of Heartbleed and Shellshock at the same time that everyone else did. Our military networks are probed for vulnerabilities thousands of times every hour, so in both cases it was not long before we detected new probes checking our websites and systems for open locks, as it were, at the relevant doors and windows. By this point our mission partners had devised ways to filter such probes before they touched our systems. We were sheltered while we pushed out patches across DoD networks and monitored implementation, directing administrators to start with those systems that were most vulnerable. Very quickly we could determine and report how many systems had been remedied and how many remained at risk. Three years ago, DoD would have required many, many months to

assess the danger and formulate responses to Heartbleed and Shellshock. Thanks to the efforts we have made in recent years, our responses by contrast were comparatively quick, thorough, and effective, and in both cases they helped inform corresponding efforts on the civilian side of the federal government. We also know that other countries, including potential adversaries, struggled to cope with the Heartbleed and Shellshock vulnerabilities. In military affairs it is often relative speed and agility that can make a difference in operations; we demonstrated that in these instances, and in others that we can discuss in another setting.

This operational approach is what we need to be building in many more places. The nation's government and critical infrastructure networks are at risk as well, and we are finding that computer security is really an enterprise-wide project. To cite one example, the U.S. Government is moving toward cloud computing and mobile digital devices across the enterprise, and DoD and the Defense Industrial Base (DIB) are moving with this trend. We are working, moreover, to make our data as secure from insider threats as from external adversaries. This could eventually compel a recapitalization of government systems comparable to the shift toward desktops in the 1980s and local-area networks in the 1990s. In short, a lot of money and many people are involved at all levels. USCYBERCOM is not running this transformation, of course, but we are responsible for defending the DoD systems that will be changed by it.

Neither the U.S. Government, the states, nor the private sector can defend their information systems on their own against the most powerful cyber forces. The public and private sectors need one another's help. We saw in the recent hack of Sony Pictures Entertainment that we have to be prepared to respond to cyber attacks with concerted actions across the whole of government using our nation's unique insights and complete range of capabilities in cooperation with the private sector. This interdependence will only increase in the future. Indeed, the cyber

environment evolves rapidly—making the maturation of our capabilities and their agility in this changing mission space still more imperative for our ability to deter adversaries who might be tempted to test our resolve.

### *Where We Are Headed*

USCYBERCOM has accomplished a great deal, but we still have a long road ahead. Cyberspace is dynamic—it changes constantly with the actions of users and the equipment and software they connect on-line. Compounding that routine volatility are two factors: the rapid evolution of the technology itself, and the changing habits and expectations of users. If current trends hold, then we can expect more nations, and even state-less groups and individuals as well, to develop and employ their own tools and cyber warfare units to cause effects in targeted networks. The cyber strife that we see now in several regions will continue and deepen in sophistication and intensity. In light of our recent experience with the destructive attacks on Sony Pictures Entertainment, we expect state and unaffiliated cyber actors to become bolder and seek more capable means to affect us and our allies. Sadly, we foresee increased tensions in cyberspace.

This is truly a period in history in which we are falling behind if we are merely holding our position in the overall movement to forge new capabilities. We in the U.S. Government and DoD must continue learning and developing new skills and techniques just to tread water, given the rapid pace of change in cyberspace. I liken our historical moment to the situation that confronted the U.S. early in the Cold War, when it became obvious that the Soviet Union and others could build hydrogen bombs and the superpower competition showed worrying signs of instability. We rapidly learned that we needed a nuclear force that was deployed across the three

legs of the triad and underpinned by robust command and control mechanisms, far-reaching intelligence, and policy structures including a declared deterrence posture. Building these nuclear forces and the policy and support structures around them took time and did not cause a nuclear war or make the world less safe. On the contrary, it made deterrence predictable, helped to lower tensions, and ultimately facilitated arms control negotiations. While the analogy to cyberspace is not exact, it seems clear that our nation must continue to commit time, effort, and resources to understanding our historical situation and building cyber military capabilities, along with the “whole-of-nation” structures and partnerships they work among. Just as we fashioned a formidable nuclear capability that served us through the Cold War and beyond, I am confident in our ability to keep pace with adversaries who are determined to control “their” corners of cyberspace, to exfiltrate our intellectual property, and to disrupt the functioning of our institutions. They are every bit as determined, creative, and persistent in these efforts as the Soviet leaders we contained during the Cold War, and unfortunately we see few hints they will act more responsibly in cyberspace. Thus we must commit to the long-term goal of building a truly open, secure cyberspace governed collaboratively by many stakeholders, while we remain prepared for crises and contingencies that can arise along the way—just as we do in every other domain.

I can assure Congress, and the American people, that we are executing and will carry out a well-conceived and systematic plan for doing that. As we train our cyber mission teams, we are inculcating a culture of respect for civil liberties and privacy while learning how to assess their readiness and establishing expectations and an institutional base that will serve to sustain this force, and even to expand it further if that someday becomes necessary. The team members we train today will furnish the leadership of the U.S. military’s cyberspace organizations of the

future; they are digital natives, having come up through the ranks thinking about cyber issues. I have no doubt their perspectives will differ from our own, and that they will see solutions to problems that vex us now. Building the capabilities of USCYBERCOM and the CMF is also providing valuable lessons for the reconfiguration of DoD's networked architecture to make it more defensible. When the JIE is completely implemented a few years from now, we will have a far more secure base from which to operate in cyberspace, and all of our capabilities in the other domains will benefit as well from the massive data support they receive from a cloud architecture.

The sophistication of our defenses and operations must grow, of course, in partnership with our allies and as part of a truly whole of nation approach to the problem. Let me reiterate that there is no Department of Defense solution to our cybersecurity dilemmas. The global movement of threat activity in and through cyberspace blurs the U.S. Government's traditional understandings of how to address domestic and foreign military, criminal, and intelligence activities. This is exacerbated further by the speed with which unforeseen threats can impact U.S. interests and the fact that adversaries frequently use (wittingly or unwittingly) U.S.-based resources due to the nation's robust cyber infrastructure. This creates a circumstance in which unity of effort across the U.S. Government is required. DoD's growing capabilities and capacities need to be considered within this broader context. Any plausible solutions will involve multiple actors and stakeholders from within and across several agencies, governments, and economic sectors. Everything we do in USCYBERCOM we do in partnership with other commands, agencies, departments, industries, and countries. As we saw over the last year in our collective response to the Shellshock and Heartbleed vulnerabilities, we must all work together across the U.S. Government, with the states, industry, and allies on a constant basis to ensure we

are ready to surge for incidents and crises and thus provide the necessary assurance for inter-agency and foreign partners.

What does the future hold for USCYBERCOM specifically? I will strongly recommend to anyone who asks that we remain in the dual hat relationship under which the Commander of USCYBERCOM also serves as the Director, NSA/CSS. This is simply the right thing to do for now, as the White House reiterated in late 2013. It might not be a permanent solution, but it is a good one given where we are in this journey as it allows us to build upon the strengths of both organizations to serve our nation's defense.

### *Conclusion*

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak, and for all the support that you and this Committee have provided USCYBERCOM. I appreciate our continued partnership as we build our nation's defenses. Our progress has been made possible because of support from all stakeholders, in terms of resources, trust, and impetus. Cyberspace is more than a challenging environment; it is now part of virtually everything we in the U.S. military do in all domains of the battlespace and each of our lines of effort. There is hardly any meaningful distinction to be made now between events in cyberspace and events in the physical world, as they are so tightly linked. We in USCYBERCOM have strived to direct the operation and defense of DoD information systems and to protect and further the nation's interests in cyberspace. We have a great deal of work ahead of us, and thus accelerating USCYBERCOM's growth in capability will remain my focus, and be a continuing emphasis for the Department. We can all be proud of what our efforts, with your help, have accomplished in building USCYBERCOM and positioning its men and women for continued success.

RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL EDWARD C. CARDON  
COMMANDING GENERAL  
U.S. ARMY CYBER COMMAND AND SECOND ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OPERATIONALIZING CYBERSPACE FOR THE SERVICES

FIRST SESSION 114TH CONGRESS

MARCH 4, 2015

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

## **Introduction**

Chairman Wilson, Ranking Member Langevin, and Members of the Subcommittee, thank you for your support of our Soldiers and Civilians, our Army, and our efforts to operationalize cyberspace. It is an honor to address this subcommittee on behalf of the dedicated Soldiers and Army Civilians of U.S. Army Cyber Command (ARCYBER) and Second Army who work every day supporting Joint and Army commanders defending the Nation in cyberspace.

Army Cyber Command and Second Army have gained tremendous momentum building the Army's cyberspace capabilities and capacity. While making significant strides over the past two years, continued progress requires persistent congressional support in three core areas: people, operations, and technology. Put differently, we require resources, appropriate authorities, organizations, and capabilities, which can be synchronized in time and space with singular purpose to accomplish directed missions. This testimony focuses on the actions and activities the Army has underway, or is planning, to support our Title 10 responsibilities to organize, man, train, and equip Army cyber forces for cyberspace.

## **Mission and Organization**

Army Cyber Command and Second Army directs and conducts cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries. To accomplish this mission, the Secretary of the Army and the Army Chief of Staff streamlined the Army's cyberspace command and control structures by placing operational control of all Army operational cyber forces under one commander. The ARCYBER commanding general is responsible for Army and joint cyberspace operations; and is also designated as the Second Army commanding general responsible for all Army network operations (to meet United States Code Titles 40 and 44 requirements as defined by Headquarters, Department of the Army); and is also designated as the Joint Force Headquarters-Cyber (JFHQ-Cyber) commander responsible for cyberspace operations supporting select geographic combatant commands as directed by U.S. Cyber Command (USCYBERCOM). This construct works to enable unity of effort for cyberspace operations. The Secretary of Defense's recent decision to establish Joint Force

Headquarters- Department of Defense Information Networks (DoDIN) better aligned DoDIN operations, and by extension, Army networks, in a joint construct. This decision is essential to realizing the Department's goal of establishing one joint global network that connects Service networks as required for operational missions.

To achieve greater synergy and efficiencies within the Army, we have already established the initial elements of JFHQ-Cyber at Fort Gordon, Georgia, and will collocate the ARCYBER headquarters alongside National Security Agency-Georgia at Fort Gordon by 2020. Army Cyber Command is grateful that the FY16 President's Budget included \$90 Million to build a state-of-the-art headquarters and operations facility at Fort Gordon.

Other recent Army decisions include the formation of the Army Cyber Institute at the U.S. Military Academy, West Point, the establishment of the Cyber Center of Excellence (Cyber CoE) at Fort Gordon, Georgia and the transition of the proponent for cyberspace operations from ARCYBER to the Army's Training and Doctrine Command at the Cyber CoE. The Cyber CoE is now the center of gravity for institutionalizing cyberspace, to include the necessary doctrinal, organizational, training, and materiel activities and policies, but it needs more dedicated resources to reach its full potential. The Cyber CoE will also integrate the electronic warfare and cyberspace operations proponents. As a partial solution and in accordance with the Total Army policy with reference to cyberspace, the Cyber CoE is initiating a partnership with the Army National Guard Professional Education Center in Little Rock, Arkansas to increase Cyber training throughput. These decisions have garnered operational and institutional momentum for cyberspace operations across the Army.

### **Bounding the Impact of Cyberspace on Military Operations**

The Army's doctrine, Unified Land Operations, and recently published Army Operating Concept, establish a set of assumptions about conditions of the network and cyber-electromagnetic environment in which our forces are expected to operate. Services and combatant commanders base their plans on the expected Army capabilities, derived from this doctrine. As the current force downsizes, the Army must incorporate additional capability sets to amplify our units' means to operate more effectively in and through cyberspace.

For cyberspace, commanders at all levels will synchronize cyberspace operations into traditional land, sea, air and space activities in time and space and they will simultaneously maneuver with and through networked assets, the electromagnetic spectrum, and kinetic forces in mutually supporting operational constructs to achieve a disproportionate advantage. Achieving operational success also hinges on having the requisite command and control, alignment of authorities with missions, and other key enabling capabilities such as intelligence, information technology and communication activities. Tactical and enterprise networks are converging and future networks and the data they carry will be more contested and challenged — especially in the event of more intense forms of conflict.

The network is a critical enabler and operational capability for cyberspace operations. Congress, recognizing the importance of efficient and effective Information Technology (IT) and Information Assurance (IA) practices, legislated policy standards for both issues in Titles 40 and 44. Information Assurance, now known as Cybersecurity, has evolved into an operational imperative. Army Cyber Command is charged to plan and direct cyberspace operations in support of both Army and USCYBERCOM, and these missions require unity of effort and unity of command.

Now that cybersecurity has to be considered an element of cyberspace operations, where does cybersecurity fit, within the DoD's full-spectrum of cyberspace operations? In other words, where does statutory responsibility for cybersecurity nest with the operational commanders' responsibility to conduct full-spectrum cyberspace operations?

In response to congressional direction, DoD has recently created a new policy position within the Office of the Secretary of Defense, called the Principal Cyber Advisor, to bring an operational focus to all DoD activities affecting cyberspace. In the process, DoD clarified the policy role of the Chief Information Officer (CIO) function within DoD. The policy role of a CIO and the operational focus of a cyberspace operations commander must be mutually supportive to achieve statutory IT and cybersecurity (formerly Information Assurance) mandates. At the same time, operational commanders must assure the effectiveness of DoD networks as warfighting platforms and enablers of DoD operations.

Army leaders and cyber organizations must be capable of ensuring both freedom of maneuver in cyberspace, and integrating interactions between cyberspace operations and our traditional military activities, that are increasingly reliant on networks and network-dependent enablers. This requires an agile and adaptive network that does not exist in the Army today. The Army recognizes it must collapse its vast array of disparate networks, enclaves, and nodes at both tactical and enterprise levels to improve security, effectiveness and efficiency through network modernization. In his recent testimony, the Army's Chief Information Officer, LTG Robert Ferrell, described how the Army will address this issue.

### **Recruiting, Retaining and Maintaining Cyberspace Operations Personnel**

The Army's first priority is to grow the Cyber Mission Force (CMF). We have grown its capacity exponentially since September 2013 with 25 of 41 teams at initial operating capability. We are on track to have all 41 CMF teams established and operating by the end of FY 16. However, they will not all be fully operationally capable until FY17.

Nothing is more important and vital to the growth of cyber capabilities than our ability to attract and retain the best people. As such, the Army views people as the centerpiece to cyberspace characterized by high degrees of competence and character. After a detailed study, the Army determined it needs 3,806 military and civilian personnel with core cyber skills. The Secretary of the Army established a cyber branch on September 1, 2014, and discussions are ongoing to determine how to better manage civilians supporting cyberspace operations. In addition, the Army has also created an "E4" additional skill identifier to better track personnel who have served in cyber and cyber related assignments as we build the branch and the force.

The Army has enjoyed success with in-Service recruiting into the growing cyber force, and is actively working to expand access to high-quality recruits. We have increased recruiting aptitude scores, visibly expanded our marketing efforts, and started work on a Cyber CoE-led initiative to encourage Science Technology Engineering and Mathematics cadets from both United States Military Academy (USMA) and the Reserve Officers' Training Corps (ROTC). We will commission the first 30 Cyber branch officers from both USMA and ROTC programs this summer. Once assessed

into the cyber branch, officers are managed by the U.S. Army Human Resources Command's Cyber Management Branch.

The Cyber CoE, in collaboration with ARCYBER and other stakeholders is working to implement a cyber Career Management Field for enlisted personnel that will encompass accessions, career management, and retention this fiscal year. The Army recently approved Special Duty Assignment Pay, Assignment Incentive Pay, and bonuses for Soldiers serving in operational cyber assignments. We have also expanded cyber educational programs, including training with industry, fellowships, civilian graduate education, and utilization of inter-service education programs (e.g., Air Force Institute of Technology and the Naval Postgraduate School). We are confident these will serve as additional incentives to retain the best personnel for this highly technical field.

Additionally, as part of our Total Force efforts, we have worked with the Reserve Components on key retention initiatives, including bonuses for critical skill Service members transitioning from active duty service into the Reserve Components; and accession bonuses for commissioned and warrant officers upon award of their duty qualifying military occupational specialties. Appropriate Special Duty and Assignment Incentive Pays should be considered for each of the Reserve Components' cyber Soldiers.

Recruiting and retaining Army Civilian cyber talent is challenging given internal federal employment constraints regarding compensation and a comparatively slow hiring process. Current efforts to attract and retain top civilian talent include extensive marketing efforts, and leveraging existing programs and initiatives run by the National Security Agency, Office of Personnel Management, and National Science Foundation.

The targeted and enhanced use of recruiting, relocation and retention bonuses, and repayment of student loans will improve efforts to attract, develop and retain an effective cyber civilian workforce. These authorities exist but require consistent and predictable long-term funding. Retaining highly skilled cyber professionals will continue to be a significant challenge that needs to be addressed.

## **Training**

Training is critical to building and retaining our cyberspace force. Individual and collective cyber training has four components: training the CMF; integration of cyber into

unified land operations at echelon; training other cyber forces and enablers; and training to achieve basic cybersecurity awareness across the Total Army.

The Department of Defense provided resources to fund joint training requirements through USCYBERCOM for the CMF build for all the Services through FY16. This training allotment was only for Active Component Soldiers and Civilians. Training and sustainment resourcing after FY16 will become a Service responsibility, which the Army must fund beginning in 2017. The Army Cyber CoE recently conducted a Joint Cyber Training Forum in conjunction with USCYBERCOM and representatives from other Services and agencies to determine the way ahead for the transition to Service responsibility. The forum established that the Services are best positioned to develop the common core individual training and will re-evaluate the feeder school training model with regards to specific CMF operator work roles.

Both ARCYBER and the Cyber CoE are developing robust collective training methods that include both simulated, virtual, and real-world operational events on ranges and production networks that stress individual and team capabilities. We now require dedicated training facilities, support infrastructure and cyberspace live fire facilities consistent with joint range requirements at the Service and joint levels. These persistent training environments with dedicated facilities and resources will enable training innovations and further growth in capability and capacity available to combatant and Army commanders.

Army Cyber Command works closely with Army Training and Doctrine Command to ensure the continuum of cyberspace leader development, education, and training remains current and relevant despite the high rates of technological change. The Cyber CoE is explicitly charged with incorporating joint standards into existing programs of instruction in Military Occupational Specialty schools and the Combined Arms Center is incorporating cyber operations planning into their training scenarios. The Army must place equal attention toward the training of our cyber network defense service providers, our computer emergency response teams, and our information technology professionals. Finally, we must continue to improve the effectiveness of training on user practices for the Total Army. This also requires a culture change.

To ensure synergy between Army and joint training, the Army fully participates in the design and conduct of USCYBERCOM-sponsored and executed training and

exercise events. Army Cyber Command has also incorporated cyberspace operations into multiple operational plans and major exercises — building a cadre of cyberspace planners now supporting the joint force and Army commanders. The Army recognizes that cyber capabilities should also extend and be executed at the tactical edge to provide our forces a winning advantage across warfighting functions; therefore, the Army is working hard to define cyber requirements, including training requirements, for cyber support to our Corps and below formations with pilot programs planned for this year. We continue to expand our professional cyberspace opposing force, to more effectively train organizations and individuals on how to better protect and defend themselves against cyber attacks and how to operate in a degraded cyberspace environment during operational training events, such as major exercises and training center rotations.

### **Reserve Components Integration**

Army Cyber Command is a total multi-component force of Active and Reserve Components which are fully integrated into the cyberspace force mix. Building the U.S. Army Reserve (USAR) and Army National Guard (ARNG) cyber forces is a high priority for the Army and ARCYBER. Our Reserve Components integration strategy was reflected in the Army's response to Section 933 of the FY14 National Defense Authorization Act, titled "Cyber Mission Analysis for Cyber Operations of the Department of Defense," which requested an analysis of the Reserve Components' role in cyberspace operations and is focused along several lines of effort, including: building an operational reserve in the USAR and ARNG for cyberspace crisis response; seeking opportunities to provide dual-use capability in support of Military and Homeland Defense and Defense Support of Civil Authorities missions; organizing cyber units to match CMF structure; aligning ARNG and USAR cyber forces under ARCYBER training and readiness authority; leveraging industry connected skills and using the Reserve Components' retention advantages for the Total Force.

The Army and ARCYBER will create a Total multi-component Army cyber force that includes 21 Reserve Component Cyber Protection Teams trained to the same standards as the Active Component cyber force. The civilian acquired skills and experience of Reserve Component Soldiers should be leveraged to provide equivalency for cyber training, enabling faster integration of the Reserve Components' capability into

the cyberspace force mix. In October 2014, in coordination with the Director of the Army National Guard, the Army activated one Army National Guard Cyber Protection Team in a Title 10 status supporting ARCYBER and Second Army.

Army Guard and Reserve forces routinely augment our headquarters now for cyberspace operations even as we work to build additional capability and capacity in the Guard and Reserve. Our Reserve Components' contributions include supporting Operation ENDURING FREEDOM, current operations in Southwest Asia, the Defense Information Systems Agency, USCYBERCOM, the standup of JFHQ-Cyber, and the defense of Army networks. As we move forward with the ARNG and USAR to build the Total Army cyber force, we will continue to train and integrate 429 ARNG and 469 USAR Soldiers into the Army's cyberspace operations.

Authorities are a complex problem. While the 933 report was an excellent start for defining the critical role our Reserve Components must play in cyberspace operations, authorities remain a challenge. While Title 10 authorities are clear, Title 32 and State active duty require the application of varied State constitutional, legislative, and executive authorities and coordination with state agencies and officials. While every State is different, there is merit in developing a common approach for authorities and capabilities to facilitate rapid and effective response in cyberspace.

### **Equipping the Army's Cyberspace Operations Force**

As cyberspace grows more complex, and increasingly contested with sophisticated threats able to exploit known and unknown vulnerabilities, cyberspace operations and cybersecurity are exceptionally critical to national security. Sophisticated software is readily available that almost anyone can operate to achieve altruistic or nefarious ends. Aided by the proliferation of dual-use technologies, cyber actors of all types continue to exercise distinct advantages in cyberspace, especially when acting as an aggressor, as illustrated by the recent attacks on Sony Pictures Entertainment and Anthem health insurance. Electronic devices are increasingly embedded in everything from vehicles to guided missiles, and are often integrated into systems which are difficult and costly to update or upgrade as new threats or vulnerabilities are identified with increasing speed and widely ranging tempo. These factors represent malefactors impacting our warfighting systems.

In conjunction with our joint partners, the Army is aggressively improving its defensive posture beginning with architecture modernization efforts that reduce attack surface area, improve bandwidth and reliability, and fortify our long-standing but ever-critical perimeter defense capability. Notably, the Joint Regional Security Stack (JRSS) initiative, a component of the Joint Information Environment (JIE), will consolidate and improve the security of currently disparate networks, and provide foundational elements for enhanced situational awareness. Recent intrusions plainly underscore the extent to which DoD lacks sufficient situational awareness, putting operations and sensitive data at grave risk. With the proliferation of cyberspace capabilities globally, situational awareness also depends upon analysis of unprecedented quantities of data across friendly, enemy, and neutral space. Essential data elements are created throughout all phases of cyber attacks, which potentially originate deep within adversary space, and span our entire defense in depth. All of these separate data sources must be captured, aggregated, and correlated in near real-time to discover ever-evolving and diverse threats, including insider threats. Accordingly, we are aggressively pursuing foundational big data analytic capabilities required to deliver complete cyber situational awareness across all cyberspace operations. We have to modernize and get to the JIE as quickly as possible for improved mission effectiveness, enhanced security, and to increase efficiency — an imperative to protecting the DoDIN. Coupled with architecture modernization, these efforts align directly with JIE standards and its Single Security Architecture construct. In parallel, we are pursuing several advanced technologies to include network mapping, cloud and virtualization, and cyber infrastructure, platforms and tools, all of which are also fully integrated with USCYBERCOM's Unified Platform initiative. Additionally, we are also an active partner with Defense Advanced Research Projects Agency on its PLAN X cyberwarfare program that is developing foundational platforms for the planning and execution of cyber operations.

Given the pace of technological change, we must address distinct requirements, resourcing and acquisition processes. Together, they influence the entire spectrum of research, development, testing, evaluation, fielding, and sustainment. Dynamic and agile institutional processes are crucial to building and maintaining our decisive technological advantage. Recent updates to policy instructions for the Joint Capabilities Integration and Development System and the Defense Acquisition System provide a

foundation for requirements and acquisition governance and management rooted in agility, flexibility, and accountability with the objective to rapidly deliver cyberspace capabilities. The Army is also establishing the requisite fiscal structures and governance construct for investments and appropriations against urgent requirements. We must capitalize on the cumulative innovative power of industry, academia, and our National Laboratories to develop, test, and pilot promising technology and concepts. This requires a willingness to engage in iterative development and operations, for which success is measured by rapidly validating assumptions, failing cheaply, early, and often to ensure resources are liberated from non-performing programs and applied to those demonstrating promise, as well as delivering new or enhanced cyberspace capabilities in weeks or months instead of months or years.

In recognition of the unique demands of cyberspace, the Army has designated a cyber focal point at the office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology, and designated initial cyber materiel development roles across our Program Executive Offices. The Army is deeply focused on improving the security posture and resilience of its critical weapons and business platforms, ensuring cyber threats and vulnerabilities are considered both in the design phase and throughout production and sustainment. Remaining focused on DoD and USCYBERCOM guidance and directives we will ensure Army capabilities are presented in alignment with joint requirements and are interoperable within the joint community so that we optimize our collective investments across DoD. As we work to ensure current processes evolve to capitalize on innovative technologies, ultimately, new programming and acquisition authorities can provide greater flexibility to developing and fielding the infrastructure, platforms, and tools needed by our operational cyber forces.

## **Conclusion**

Despite cyberspace operations' central role in current defense strategy, funding for core requirements remains uncertain. Cyber professionals – resourced with the right infrastructure, platforms and tools – are the key to dominance in cyberspace. Army Cyber Command, Second Army, and JFHQ-Cyber have made tremendous progress operationalizing cyberspace for the Army. Army networks are better defended and our cyber forces are better manned, trained and equipped. Recent institutional changes are helping recruit, retain, and continuously develop competent and disciplined cyber

professionals. This is a journey and congressional support is essential to ensure the Army has the required resources and authorities, and the right people, processes, and technologies to provide our combatant commanders and national decision makers with a ready, capable, and superior operational cyber force.

With your support, we can provide national leaders and military commanders with an expanded set of options in support of national security objectives. We will deliver.

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

STATEMENT  
OF  
VICE ADMIRAL JAN E. TIGHE  
COMMANDER, U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET  
BEFORE THE  
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES  
OF THE  
HOUSE ARMED SERVICES COMMITTEE  
ON  
CYBER OPERATIONS: IMPROVING THE MILITARY CYBER SECURITY POSTURE IN  
AN UNCERTAIN THREAT ENVIRONMENT  
March 4, 2015

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

Chairman Wilson, Ranking Member Langevin and distinguished members of the Subcommittee, thank you for your support to our military and the opportunity to appear before you today along with my military service component counterparts and partners.

Mr. Chairman, I have been in command of U.S. Fleet Cyber Command and U.S. TENTH Fleet for just under one year. U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for Navy Networks, Cryptology, Signals Intelligence, Information Operations, Electronic Warfare, Cyber, and Space. As such, U.S. Fleet Cyber Command serves as the Navy Component Command to U.S. Strategic Command and U.S. Cyber Command, and the Navy's Service Cryptologic Component Commander under the National Security Agency/Central Security Service, exercising operational control of U.S. Fleet Cyber Command operational forces through TENTH Fleet. Specifically, we conduct cyberspace operations to ensure Navy and Joint or Combined forces' freedom of action while denying the same to our adversaries.

The commissioning of U.S. Fleet Cyber Command and reestablishment of U.S. TENTH Fleet on January 29, 2010 closely followed the Navy's 2009 acknowledgement of information's centrality to maritime warfighting, known as Information Dominance. Information Dominance is defined as the operational advantage gained from fully integrating the Navy's information functions, capabilities, and resources to optimize decision making and maximize warfighting effects. The three pillars of Information Dominance are assured command and control (C2), battlespace awareness, and integrated fires. U.S. Fleet Cyber Command is a key warfighting element in delivering on missions across those three pillars.

Since my U.S. Fleet Cyber Command predecessor ADM Michael S. Rogers last testified before this Subcommittee in July 2012, the Department of Defense (DoD), U.S. Cyber Command, and the Service Components have significantly matured cyber operations and enhanced cyber operational capabilities. I appreciate the opportunity to outline the Navy's progress over the past two years, where we are headed to address an ever increasing threat, and how budgetary uncertainty is likely to impact our operations.

## **Cyber Operations, Posture, and Future Investments**

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks within the Department of Defense Information Networks (DoDIN). We operate the Navy Networking Environment as a warfighting platform, which must be aggressively defended from intrusion, exploitation and attack. The Navy Networking Environment consists of more than 500,000 end user devices; an estimated 75,000 network devices (servers, domain controllers); and approximately 45,000 applications and systems across three security enclaves.

Operations during the past two years led to a fundamental shift in how we operate and defend in cyberspace. Specifically, late summer 2013 we fought through an adversary intrusion into the Navy's unclassified network. Under a named operation, known as OPERATION ROLLING TIDE, U.S. Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy leaders, U.S. Cyber Command, National Security Agency, Defense Information Systems Agency (DISA), and our fellow service cyber components. Although any intrusion upon our networks is troubling, this operation also served as a learning opportunity that has both matured the way we operate and defend our networks in cyberspace, and simultaneously highlighted gaps in both our cybersecurity posture and defensive operational capabilities. As a result of this operation and other cybersecurity initiatives, the Navy has already made or proposed (through FY20) a nearly 1 billion dollar investment that reduce the risk of successful cyberspace operations against the Navy Networking Environment. Of course these investments are built on the premise that our future year budgets will not be drastically reduced by sequestration. Specifically, if budget uncertainty continues, we will have an increasingly difficult time addressing this very real and present danger to our national security and maritime warfighting capability.

The Navy's future cybersecurity investments are being informed by the Navy's Task Force Cyber Awakening, which was chartered by the Chief of Naval Operations and the Assistant Secretary of the Navy for Research, Development and Acquisition to gain a holistic view of cybersecurity risk across the Navy, and beyond just our corporate navy networks to include

combat and industrial control systems. The FY16 Proposed Budget (PB16) includes Task Force Cyber Awakening -recommended investments amounting to \$248M for FY16 and \$721M across the Future Years Defense Plan (FYDP). Task Force Cyber Awakening will make additional recommendations on how to organize and resource capabilities to mitigate that risk.

Concomitant with the Task Force Cyber Awakening outcomes is the migration to a single defensible Cyber architecture, which is vital to the continued success of Navy's worldwide operations. The Navy recognizes that the Joint Information Environment (JIE) is an operational imperative and endorses that vision, including the implementation of a single security architecture (SSA). The Department of the Navy intends for the Navy and Marine Corps Intranet (NMCI) to serve as the primary onramps into JIE, incorporating JIE technical standards through our network technical refreshment processes as those standards are defined. Through delivery of these enterprise environments, the Navy will achieve the tenets of JIE's framework of standards and architecture consistency.

For our part, U.S. Fleet Cyber Command is operationally focused on continuously improving the Navy's cyber security posture by reducing the network intrusion attack surface, implementing and operating layered defense in depth capabilities, and expanding the Navy's cyberspace situational awareness as outlined below.

### ***Reducing the network intrusion attack surface***

Opportunities for malicious actors to gain access to our networks come from a variety of sources such as known and zero day cyber security vulnerabilities, poor user behaviors, and supply chain anomalies with counterfeit devices from untrusted sources. Operationally, we think of these opportunities in terms of the network intrusion attack surface presented to malicious cyber actors. The greater the attack surface, the greater the risk to the Navy mission. The attack surface grows larger when security patches to known vulnerabilities are not rapidly deployed across our networks, systems, and applications. The attack surface also grows larger when network users, unaware of the ramifications of their on-line behavior exercise poor cyber hygiene and unwittingly succumb to spear phishing emails that link and download malicious

software, or use peer-to-peer file sharing software that introduces malware to our networks, or simply plug their personal electronic device into a computer to recharge it.

The Navy is taking positive steps in each of these areas to reduce the network intrusion attack surface including enhanced cyber awareness training for all hands. Furthermore, we are bolstering our ability to manage cyber security risks in our networks through our certification and accreditation process, and through cyber security inspections across the Navy. Additionally, the Navy is reducing the attack surface with significant investments and consolidation of our ashore and afloat networks with modernization upgrades to the Next Generation Enterprise Network (NGEN) and the Consolidated Afloat Networks and Enterprise Services (CANES), respectively. Finally, the Navy is executing a Data Consolidation Center (DCC) strategy, which will reduce the number and variance of information systems at the same time allow for a centralized approach towards managing the confidentiality, integrity and availability of our data.

For long term success in cyber security, the Navy is working on improved acquisition and system sustainment processes. Specifically, we will design in resiliency by generating a common set of standards and protocols for programs to use as guiding principles during procurement, implementation, and the configuration of solutions, which will improve our cyber posture by driving down variance.

The Navy recognizes that all hands (users, operators, program managers, systems commands...) have an impact (for better or worse) on the magnitude of the Navy's attack surface and the mission risk associated with it. U.S. Fleet Cyber Command must defend this attack surface, regardless of size, using defense in depth capabilities described below.

### ***Defense in Depth***

The Navy is working closely with U.S. Cyber Command, NSA/CSS, our Cyber Service Partners, DISA, Interagency partners, and commercial cyber security providers to enhance our cyber defensive capabilities through layered sensors and countermeasures from the interface with the public internet down to the individual computers that make up the Navy Networking Environment. We configure these defenses by leveraging all source intelligence and industry

cyber security products combined with knowledge gained from analysis of our own network sensor data.

We are also piloting and deploying new sensor capabilities to improve our ability to detect adversary activity as early as possible. This includes increasing the diversity of sensors on our networks, moving beyond strictly signature-based capabilities (to include reputation-based and heuristic capabilities), and improving our ability to detect new and unknown malware.

JIE Joint Regional Security Stacks are also integral to our future defense in depth capabilities. As described above, the Navy has already consolidated our networks behind defensive sensors and countermeasures. We expect that JIE Joint Regional Security Stacks (JRSS) v2.0 will be the first increment to bring equal or greater capability to Navy Defense in Depth. Accordingly, the Department of Navy is planning to consolidate under JRSS 2.0 as part of the technical refresh cycle for NMCI when JRSS meets or exceeds existing Navy capabilities.

### ***Cyber Situational Awareness***

Success in cyberspace requires vigilance: it requires that we constantly monitor and analyze Navy Networking Environment. We must understand both its availability and vulnerabilities. Furthermore we must be able to detect, analyze, report, and mitigate any suspicious or malicious activity in our Networks. The Navy is planning to expand our current capabilities to include a more robust, globally populated and mission-tailorable cyber common operating picture (COP). Additionally, with improved network sensor information across the DoD, however, comes the need for a single dedicated data strategy and big data analytics for all DoD network operations and defense data. This will allow for better overall situational awareness and improved speed of response to the most dangerous malicious activity by leveraging the power of big data analytics to harness existing knowledge rapidly.

### **U.S. Fleet Cyber Command Operational Forces**

U.S. Fleet Cyber Command's operational force comprises nearly 15,000 Active and Reserve sailors and civilians organized into 22 active commands and 32 reserve commands around the

globe. The commands are operationally organized into a TENTH Fleet-subordinate task force structure for execution of operational mission. Approximately 35 percent of U.S. Fleet Cyber Command's operational forces are aligned with the cyber mission.

### ***Status of the Cyber Mission Force***

As you may recall, during a hearing before the Senate Committee on Armed Services on March 12, 2013, General Keith Alexander briefed the Cyber Mission Force model, which DoD endorsed in December 2012. The Cyber Mission Force is designed to accomplish three primary missions: National Mission Teams will defend the nation against national level threats, Combat Mission Teams to support combatant commander priorities and missions, and Cyber Protection Teams to defend Department of Defense information networks and improve network security.

Navy and other cyber service components are building these teams for U.S. Cyber Command by manning, training, and certifying them to the U.S. Cyber Command standards. Navy teams are organized into existing U.S. Fleet Cyber Command operational commands at cryptologic centers, fleet concentration areas, and Fort Meade, depending upon their specific mission. Navy is responsible for sourcing four National Mission Teams, eight Combat Mission Teams, and 20 Cyber Protection Teams as well as their supporting teams consisting of three National Support Teams and five Combat Support Teams.

The Navy is currently on track to have personnel assigned for all 40 Navy-sourced Cyber Mission Force Teams in 2016 with full operational capability in the following year. As of 1 March 2015, we had 22 teams at initial operating capability (IOC) and 2 teams at full operational capability (FOC). We are in the process of manning, training, and equipping our FY15 teams to meet IOC standards by the end of FY15. Additionally, between now and 2018, 298 cyber reserve billets will also augment the Cyber Force manning plan as described below.

U.S. Fleet Cyber Command has also been designated as the Joint Force Headquarters-Cyber by U.S. Cyber Command to support U.S. Pacific Command and U.S. Southern Command in the development, oversight, planning and command and control of full spectrum cyberspace operations that are executed through attached Combat Mission and Support Teams. In 2014,

Navy's Joint Force Headquarters-Cyber was certified and declared to have achieved Full Operational Capability. This capability was attained without additional U.S. Fleet Cyber Command resources. As the Cyber Mission and Support Teams continue to grow and mature, additional resources to operationally control and manage these teams in support of Combatant Command Priorities will be required.

### ***Reserve Cyber Mission Forces***

Through ongoing mission analysis of the Navy Total Force Integration Strategy, we developed a Reserve Cyber Mission Force Integration Strategy that leverages our Reserve Sailors' skill sets and expertise to maximize the Reserve Component's support to the full spectrum of cyber mission areas. Within this strategy, the 298 Reserve billets, which are phasing into service from FY15 through FY18, will be individually aligned to Active Duty Cyber Mission Force teams and the Joint Force Headquarters-Cyber. Accordingly, the Joint Force Headquarters-Cyber and each Navy-sourced team will maximize its assigned Reserve Sailors' particular expertise and skill sets to augment each team's mission capabilities. As our Reserve Cyber Mission billets come online and are manned over the next few years, we will continue to assess our Reserve Cyber Mission Force Integration Strategy and adapt as necessary to develop and maintain an indispensably viable and sustainable Navy Reserve Force contribution to the Cyber Mission Force.

### ***Future Cyber Workforce Needs***

The Navy's operational need for a well-trained and motivated cyber workforce (active, reserve and civilian) will continue to grow in the coming years as we build out the balance of Cyber Mission Force and as we refine our needs to holistically address the challenges being informed by Task Force Cyber Awakening. We will depend upon commands across the Navy to recruit, train, educate, retain and maintain this workforce including the Chief of Naval Personnel, Navy Recruiting Command, Naval Education and Training Command and Navy's Institutions of Higher Education (United States Naval Academy, Naval Postgraduate School, and Naval War College.) Additionally, the establishment of Navy Information Dominance Force (NAVIDFOR) in 2014 as a Type Commander will go a long way in generating readiness for cyber mission requirements. NAVIDFOR will work closely with the Man, Train, and Equip organizations

across the Navy to ensure that U.S. Fleet Cyber Command and other Information Dominance operational commands achieve proper readiness to meet mission requirements.

### ***Recruit and Retain***

There are many young Americans with the skill sets we need who want to serve their country. I am very encouraged by the dedication and commitment I see entering our ranks. I am awed by their dedication and growing expertise every day. We must consistently recruit and retain this technically proficient group of diverse professionals for the cyber mission to sustain this momentum.

In FY2014, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession goals in FY2015. Currently authorized special and incentive pays, such as the Enlistment Bonus, should provide adequate stimulus to continue achieving enlisted accession mission, but the Navy will continue to evaluate their effectiveness as the cyber mission grows.

Today, Navy Cyber Mission Force (CMF) enlisted ratings (CTI, CTN, CTR, IS, IT) are meeting retention goals. Sailors in the most critical skill sets within each of these ratings are eligible for Selective Reenlistment Bonus (SRB). SRB contributes significantly to retaining our most talented Sailors, but we must closely monitor its effectiveness as the civilian job market continues to improve and the demand for cyber professionals increases.

Cyber-related officer communities are also meeting retention goals. While both Information Warfare (IW) and Information Professional (IP) communities experienced growth associated with increased cyber missions, we are retaining officers in these communities at 93 percent overall. Both IW and IP are effectively-managing growth through direct accessions, and through the lateral transfer process, thereby ensuring cyber-talented officers enter, and continue to serve.

With respect to the civilian workforce, we are aggressively hiring to our civilian authorizations consistent with our operational needs and fully supported by the Navy's priority to ensure health of the cyber workforce. We have also initiated a pilot internship program with a local university

to recruit skilled civilian and military cyber workforce professionals. Navy will measure the success of this approach as a potential model to harness the nation's emerging cyber talent.

As the economy continues to improve, we expect to see more challenges in recruiting and retaining our cyber workforce.

### ***Educate, Train, Maintain***

To develop officers to succeed in the increasingly complex cyberspace environment, the U.S. Naval Academy offers introductory cyber courses for all freshman and juniors to baseline knowledge. Additionally, USNA began a Cyber Operations major in the Fall of 2013. Furthermore, the Center for Cyber Security Studies harmonizes cyber efforts across the Naval Academy.

Our Naval Reserve Officer Training Corps' (NROTC) program maintains affiliations at 51 of the 180 National Security Agency (NSA) Centers of Academic Excellence (CAE) at colleges around the country. Qualified and selected graduates can commission as Information Warfare Officers, Information Professional Officers, or Intelligence Officers within the Information Dominance Corps.

For graduate-level education, the Naval Postgraduate School offers several outstanding graduate degree programs that directly underpin cyberspace operations and greatly contribute to the development of officers and select enlisted personnel who have already earned a Bachelor's Degree. These degree programs include Electrical and Computer Engineering, Computer Science, Cyber Systems Operations, Applied Mathematics, Operations Analysis, and Defense Analysis. Naval War College is incorporating cyber into its strategic and operational level war courses, at both intermediate and senior graduate-course levels. The College also integrates strategic cyber research into focused Information Operations (IO) /Cybersecurity courses, hosts a Center for Cyber Conflict Studies (C3S) to support wider cyber integration across the College, and has placed special emphasis on Cyber in its war gaming role, including a whole-of-government Cyber war game under active consideration for this coming Summer or Fall.

With respect to training of the Cyber Mission Force, U.S. Cyber Command mandates Joint Cyberspace Training & Certification Standards, which encompass procedures, guidelines, and

qualifications for individual and collective training. U.S. Cyber Command with the Service Cyber Components has identified the advanced training required to fulfill specialized work-roles in the Cyber Mission Force. Most of the training today is delivered by U.S. Cyber Command and the National Security Agency in a federated but integrated approach that utilizes existing schoolhouses and sharing of resources. The Navy is unified in efforts with the other Services to build Joint Cyber training capability, leveraging Joint training opportunities, and driving towards a common standard.

### **Declining Budgets**

While the overall Navy budget has been impacted by financial constraints and sequestration, the Navy has done a good job in terms of minimizing the budgetary impact on U.S. Fleet Cyber Command and the capabilities it employs to conduct its operations. Should this circumstance change and future budgets decline, however, there will be an impact to the capability and capacity to conduct operations in cyberspace. The scope and magnitude of such impacts would be driven by the scope and magnitude of a budget decline.

It is, however, possible to speak in broad terms regarding the potential areas of impact.

Operations in cyberspace are highly dependent on people - to a certain extent our people are part of the warfighting platform in cyberspace. Budgetary declines impacting our ability to attract and retain the numbers of people with the requisite skills and experience would negatively impact the Navy's ability to conduct operations in cyberspace. Additionally, declining budgets affecting the ability of the Navy to implement initiatives described above that reduce the network intrusion attack surface, enhance defense in depth and cyber situational awareness, or modernize/migrate to the Joint Information Environment greatly jeopardizes the Navy's ability to accomplish all missions, since all Navy mission accomplishment depends on having an available and secure network.

### **Summary**

Our success in the maritime domain and joint operational environment depends on our ability to maintain freedom of maneuver and deliver effects within cyberspace. To ensure operational success in the maritime and other warfighting domains, defense of Navy and DoD networks and information is essential and cannot be separated from the overall maritime operational level of war.

In order to continue to progress in cyberspace operations, we must have sufficient resources to ensure we close any identified cybersecurity gaps and provide our workforce with the right capabilities to maintain our warfighting advantage. We must be prepared – both technologically and with skilled operators, civilian and uniformed - and remain innovative. The threat in cyberspace will only continue to grow despite our budgetary challenges. U.S. Navy freedom of action in cyberspace is necessary for all missions that our nation expects us to be capable of carrying out including winning wars, deterring aggression and maintaining freedom of the seas.

I thank you for this opportunity to share U.S. Navy and U.S. Fleet Cyber Command operations and initiatives in cyberspace.

MARFORCYBER RECORD VERSION

STATEMENT BY

MAJOR GENERAL DANIEL J. O'DONOHUE  
COMMANDING GENERAL  
MARINE FORCES CYBERSPACE COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OPERATIONALIZING CYBERSPACE FOR THE SERVICES

FIRST SESSION 114TH CONGRESS

MARCH 4, 2015

NOT FOR PUBLICATION

UNTIL RELEASED BY

THE HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

## Introduction

Chairman Wilson, Ranking Member Langevin, and distinguished members of this subcommittee, it is an honor to appear before you today. On behalf of all Marines, our civilian workforce, and their families, I thank you for your continued support. I appreciate the opportunity to discuss the Marine Corps' cyberspace operations posture.

The Marine Corps is the nation's expeditionary force-in-readiness. We are forward deployed, forward engaged, and prepared for crisis response. For generations, your Marines have been victorious against our nation's foes by remaining agile and adaptable to dynamic environments and evolving threats. As the force that is 'the most ready when the nation is least ready,' we are prepared to defend against adversaries who operate across multiple domains to include cyberspace.

Our current operating environment is volatile, complex, and distinguished by increasingly sophisticated threats that seek asymmetric advantage through cyberspace. Our cyberspace posture guards against these threats while simultaneously exploiting our competitive advantage in employing combined arms to include closely integrated cyberspace operations.

Our joint cyberspace mission builds on the Marine Corps institutional focus as a global crisis response force with strong naval, inter-agency, COCOM, SOF, cross-service and coalition partnerships. 2015 is a key transitional year as we deploy rapidly maturing cyber capabilities and make them central to Marine Air Ground Task Force, COCOM and coalition training, planning and operations. Activities in cyberspace increasingly influence all our warfighting functions.

Marine Forces Cyberspace Command (MARFORCYBER) is engaging in ongoing cyberspace operations, making strong progress with the force build, achieving operational outcomes, and building capacity for tomorrow's opportunities and challenges. Our priorities are to operate and defend our networks, support designated COCOMs with full spectrum cyber operations, organize for the fight, train and equip the cyber workforce, develop workforce

lifecycle management, and to ensure mission readiness through joint and service capabilities integration.

### **Mission and Organization**

As the service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum Cyberspace Operations to ensure freedom of action in and through cyberspace, and deny the same to our adversaries. The operations include operating and defending the Marine Corps Enterprise Network (MCEN), conducting Defensive Cyberspace Operations (DCO) within the MCEN and Department of Defense Information Networks (DODIN), and - when directed - conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces. MARFORCYBER is also designated at the Joint Force Headquarters – Cyber (JFHQ – CYBER) as directed by USCYBERCOM.

### **Operationalizing Cyber**

MARFORCYBER is in its sixth year of operation. Our focus remains developing ready cyberspace capability for the naval, joint and coalition force. Consistent with our Commandant's guidance, we are developing tactical cyber capacity as an organic aspect of how we fight.

Further, in conjunction with joint and interagency partners, we intend to pursue the development of an integrated and unified platform for cyberspace operations that will enable centralized command and control, real time situational awareness, and decision support. We are accomplishing this through close coordination with industry partners, and aligned with DoD and USCYBERCOM priorities in support of the Joint Information Environment.

### **Train and Equip**

In this presumably automated and system driven arena, our most valuable resource is our people. Just as the Marine Corps remains dedicated to the notion that there is no more

dangerous weapon than a Marine and his rifle, we believe the solutions to our shared problems in cyberspace revolve around our people, and not systems. However, we must provide our workforce the training, tools, and resources they need to defend our nation. Our ability to acquire tools and technology more rapidly than our adversaries is paramount to mission success.

MARFORCYBER's approach to training and developing the cyber work force has a singular vision—to train as we fight. Specifically, MARFORCYBER will adapt a persistent training environment to support training and exercises of cyber units that are assigned to conduct military cyber operations. This training environment will be designed to enhance military occupational skills (MOS) proficiency, test and development of next generation solutions, host remote training and education of Marine Corps Operating Forces, and refine tactics, techniques, and procedures (TTPs) to increase effectiveness of cyberspace operations. Additionally, we are developing a web based training environment hosted by Carnegie Mellon University Software Engineering Institute (CMU-SEI), a Federally Funded Research and Development Center (FFRDC). This environment combines extensive research and innovative technology to offer a new solution to cyberspace operations workforce development. The focus of this collaboration is to help practitioners and their teams build knowledge, skills, and experience in a continuous cycle of professional development. The combined effect of this approach is for cyberspace operations workforce to train individually and collectively. This initiative will support the future development and certification of Cyber National Mission Forces (CNMF) training requirements.

The training pipeline to build these teams is extensive and often depends on joint schoolhouses that serve all the cyber service components. There are simply not enough school seats to meet the demand from the joint force. Compounding this problem are slowdowns in the clearance process, as technically qualified personnel from our communications or data job fields still require high level security clearances. Often these personnel come from distant and austere duty stations that lack investigators who can complete their clearances prior to arrival at MARFORCYBER. These personnel often wait months at the command prior to starting work due to long wait times for clearance adjudication.

We have dramatically increased cyber integration into the training cycle by leading, supporting, or participating in over 31 combined, joint, and Marine Corps exercises in the past year. Commanders across our Marine Corps are asking for cyber capabilities both in real world operations and in training to ensure their Marines are ready to face the challenges presented by a shifting complex landscape.

### **Workforce Life-Cycle Management**

We have seen substantial increases in capacity and capability. Such achievements are significant but they have not been easy, and MARFORCYBER's success grows from the hard work of its people. Marines and Civilians have shown a sharp interest in pursuing a cyber career.

Since MARFORCYBER last appeared before this committee in 2012, we have dramatically increased our workforce—with an authorized strength of almost 1000 Marines and civil servants today. By the end of fiscal year 2016, MARFORCYBER's authorized strength will increase to over 1300 personnel, which is in line with previous projections. The majority of these new personnel are allocated to support the cyber mission force as directed by the Secretary of Defense.

In order to attract and retain the best people, the Marine Corps has followed multiple lines of effort. To improve continuity and reap greater return-on-investment in the lowest density highest demand military occupational specialties (MOS), we have coordinated with our Service to extend standard assignments to four years. Additionally, the number of feeder MOS available to lateral move into critical cyber related specialties has been increased in order to obtain a larger talent pool of qualified and experienced Marines. We are currently accessing sixteen feeder occupational specialties from the communications, signals intelligence, electronic warfare, data, and aviation specialty fields to meet the personnel demands of cyber occupational field. The largest reenlistment or lateral move bonus offered in the past year of \$60,750 dollars was offered to Sergeants who move into the Cyber Security Technician specialty. To drive home the point of how seriously the Marine Corps takes its cyber talent

management, this bonus consumed 16% of the retention bonus budget for the last fiscal year. Furthermore, to ensure we have the right metrics, we are leveraging academia and industry to understand how to better attract and retain talent. In the future, our focus will broaden to include generating a sustainable force generation model that retains a unique, skilled expertise within the larger contexts of cyber ready MAGTFs.

## **Readiness**

MARFORCYBER is leading the effort to take cyberspace operations mainstream across the Marine Corps so as not to be outpaced in an evolving and complex battlespace. Initial teams are being operationally employed as they achieve IOC. As we support the DoD and USCYBERCOM efforts to implement a unified cyberspace architecture of the JIE, we continue to improve the operational readiness of our existing enterprise network (MCEN). We have assumed full control of the MCEN, which was previously contractor-managed, and have decreased our legacy network footprint.

In conjunction with joint, interagency, and private partners, we intend to improve our operational readiness and our ability to measure it. In this context, our staff is working and collaborating with our partners to develop rapid acquisition of tools, training environment, and development of procedures that will allow us to train as we fight.

Last June, USCYBERCOM certified our first Cyber Mission Team (CMT) as fully operational (FOC) and simultaneously, our first national Cyber Protection Team (CPT) and the second Cyber Mission Team (CMT) reached initial operational capability (IOC). MARFORCYBER is on track to have over 75% of its CMT, CPT, and CST teams resourced by the end of fiscal year 2015.

In order to fulfill the requirements of USCYBERCOM, we have been actively engaged in building and sourcing our national and combat mission, protection, and support teams (CMT, CPT, CST). With one CMT currently certified, the plan going forward is to have MARFORCYBER's second CMT certified early in calendar year 2015. We have one operational CPT working from the MCNOSC, which is our service wide network operations and security center. Our second

CPT, which will be in support of national missions, is in the process of certification now. In addition, we stood up our Joint Forces Headquarters-Cyber (JFHQ-C), now at Full Operational Capability (FOC), which directs and coordinates the actions of cyber forces in support of directed missions. The current glide slope for team build-out is to have two (2) CMTs, three (3) CPTs, and one (1) CST at either IOC or FOC by the end of fiscal year 2015. No later than the end of FY17 all teams will be FOC, meaning the Marine Corps will furnish one (1) NMT, three (3) CMTs with one (1) CST in support, and eight (8) CPTs. Three of those CPTs will be dedicated to Marine Corps' specific needs. All other teams will function in support of joint requirements from unified and sub-unified combatant commands.

## **Conclusion**

Over the past six years, MARFORCYBER experienced both the increased risk and opportunity presented by a world that grows more connected. These experiences reinforced the need to remain focused on our priorities of developing our organization and cyber work force, refining our service support to MAGTF operations and joint cyber forces, and securing our networks to yield results for commanders worldwide. Although I am pleased to report that our growth is increasing our capacity, capability, and integration with warfighters, I must reiterate the opportunities and challenges that lie ahead are great. While global technology advances rapidly, the Marine Corps faces challenges in adapting its acquisitions to operate at the speed required of cyberspace. Critically, in this domain characterized by human activity, people remain our center of gravity. Resourcing and sustaining this most valuable asset also remains a difficult task. These are difficult challenges, but through your continued support and leadership, we can count such difficulties among the many that Marines have overcome in the defense of this great nation.

Thank you for this opportunity to appear before you today. Thank you for your continued support of our Marines and Civilians and I look forward to answering your questions.

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

PRESENTATION TO THE  
HOUSE ARMED SERVICES COMMITTEE  
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES  
UNITED STATES HOUSE OF REPRESENTATIVES

SUBJECT: Cyber Operations: Improving the Military Cyber Security Posture in Uncertain  
Threat Environment

STATEMENT OF: Major General Burke E. Wilson  
Commander, Air Forces Cyber and  
Commander, 24th Air Force

March 4, 2015

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

## *Introduction*

Chairman Wilson, Ranking Member Langevin, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today, with my counterparts from the other military Services, to discuss Air Forces Cyber's contributions to joint operations in cyberspace. We have made significant strides towards normalizing the Air Force's cyber operations since Major General Vautrinot had the privilege of speaking to the committee in August 2012. Air Forces Cyber (24<sup>th</sup> Air Force) is one of four Service Cyber Components established to support U.S. Cyber Command; our headquarters is at Joint Base San Antonio-Lackland, Texas and we have ongoing cyber operations around the world. The outstanding men and women of Air Forces Cyber have been diligently working to increase our capacity and capability to build, operate, defend and engage across the full spectrum of cyberspace capabilities in, through and from cyberspace in support of joint warfighters. I'm extremely proud of the work they do each and every day in support of military operations around the world, while at the same time, innovating and mastering new and emerging technologies within cyberspace to project global military power.

Cyberspace is an inherently global domain that impacts nearly every function of our Joint Force, which is increasingly dependent upon cyber capabilities to conduct modern military operations. To that end, today's capabilities enable streamlined command, control and execution of joint operations through the rapid collection, fusion and transmission of information at unprecedented speed, capacity and precision.

However, the pace of threats continues to grow in scope, intensity and sophistication. Recent attacks such as the Sony Pictures Entertainment incident that resulted in physical damage demonstrate that no industry or sector is immune to this growing threat. State-sponsored actors, non-state-sponsored actors, criminals, and terrorists operating in the cyberspace domain will continue their attempts to penetrate Department of Defense networks and mission systems. We must remain vigilant and not falter in our commitment to properly prioritize our support to cyber missions, even with the strain of diminishing resources across the Department.

In response to these growing threats, Air Forces Cyber remains committed to delivering innovative and cost-effective solutions for the joint warfighter with unwavering focus on delivering mission success. Air Forces Cyber's priorities are as follows: employ cyber capabilities in support of Combatant and Air Force Commanders; develop and empower our Airmen and take care of their families; lead through teamwork, partnerships and a strong warfighting narrative; and equip the force through rapid, innovative fielding of cyber capabilities. In this dynamic environment, resource stability will be critical to our ability to protect our networks, provide the needed cyber forces, protect critical information, and provide full spectrum cyber capabilities in support of Combatant and Air Component Commanders around the world.

### ***Employing Cyber Capabilities***

Air Forces Cyber has placed significant emphasis on normalizing cyber operations. We continue to transform our organization to an operational Component Number Air Force providing ready cyber forces and capabilities to Combatant and Air Force Commanders. Our operational level command and control center has made incredible gains towards our ability to effectively integrate the full spectrum of cyber operations and capabilities in support of joint and air component operations.

We cannot stand still in this environment and must continue to build our capability and capacity. Working closely with Air Force Space Command, 25th Air Force (formerly Air Force Intelligence, Surveillance and Reconnaissance Agency), and the Air Staff we have established cyber forces in support of the DoD's approved strategy. In full coordination with our Total Force partners in the Air National Guard and Air Force Reserves, these new cyber teams are providing U.S. Cyber Command with capabilities to defend the nation, support Combatant Commanders, and defend the DoD Information Network. We have reorganized our units to meet the training and equipment requirements to build a ready force of approximately 1,700 mission-ready personnel. In concert with the Air Force's basing process, we have identified Joint Base San Antonio-Lackland, Texas, as well as Scott Air Force Base, Illinois, as primary locations for our Cyber Protection Teams. The remaining cyber forces will operate at the National Security

Agency's regional operating centers. Today, Air Forces Cyber has seventeen operational cyber mission teams -- two fully operational teams and an additional fifteen teams that have achieved initial operational status. Our Joint-Forces Headquarters-Cyber also declared initial operational status in October 2013 and continues to work toward achieving full operational status.

In 2014, the Air Force designated seven cyberspace systems as weapons systems directly supporting our lines of effort. This designation has been critical to our ability to operationalize and integrate cyber capabilities through a normalized budget, sustainment and support process. Since we last briefed this subcommittee, the Air Force has completed the migration of its portion of the DoD Information Network (e.g. the Air Force Information Network or "AFIN") into a single, centrally-managed and defended architecture. Transitioning over 644,000 users across more than 250 geographic locations to a single network has enabled Air Forces Cyber (24<sup>th</sup> Air Force) to operate, maintain and defend a standardized network using centralized control and decentralized execution with more optimally employed resources. Additionally, we've worked tirelessly to collapse over 100 internet access points into a more streamlined and manageable 16 gateways for the Air Force. The end result has been critical to achieving a more effective, efficient and defensible network.

Finally, our operations center is leveraging a combat-proven joint planning and execution process to command and control our cyber forces. Air Forces Cyber is employing small defensive cyber maneuver forces to complement our enterprise defensive capabilities to identify, assess and mitigate vulnerabilities and adversary actions within our networks. This new approach has proven truly effective in a number of operations over the past year and we continue to make strides in the planning, command, control and execution of cyberspace operations.

### ***Develop and Empower Our Airmen and Take Care of Their Families***

Our innovative Airmen are the centerpiece to our Air Forces Cyber capabilities. Therefore, we continue to be wholly committed to recruiting, training, developing and retaining the right cyber talent. Whether a military or civilian candidate, the Air Force begins by recruiting highly-qualified individuals with demonstrated competency and character.

To meet the growing requirements of the Department of Defense's Cyber Mission Force, the Air Force has restructured and expanded its initial training and force development programs. These changes are yielding significant results and put us on pace to nearly quadruple the rate at which cyberspace operators will be qualified to join Air Force cyber teams in support of the Cyber Mission Force since we last briefed the subcommittee in 2012.

Realizing the need to operationalize our training, we have also mirrored our cyber operations training based on lessons from our counterparts in air and space operations. Specifically, we have leveraged the mission qualifications process to ensure our cyber operators meet mission-ready status. Additionally, our cyber operators now participate in U.S. Cyber Command and Air Force Warfare Center events such as CYBER FLAG and RED FLAG to better hone their skills through real-world force-on-force exercises that provide the ability to integrate cyber capabilities with other domains in a live training environment. Air Forces Cyber's participation in simulated live-fire environments is accelerating the development and fielding of new tactics, techniques and procedures. These cyber warrior's experiences are further magnified when participants bring hard won lessons back to their home units.

Air Forces Cyber's participation in a wide array of Combatant Command, Joint and Service exercises also complements our efforts to integrate cyber effects with both kinetic and non-kinetic operations across multiple warfighting domains. While demanding in terms of time and resources, these exercises have become integral to effectively developing our Airmen into a ready cyber force capable of operating in joint and coalition environments.

To better develop our forces, the Air Force has also instituted a new cyberspace officer career field specific to Cyberspace Warfare Operations to develop Airmen with the requisite skills and expertise to meet our nation's emerging needs. In addition, a Cyber Intermediate Leadership program has been developed to ensure cyber operators and appropriate intelligence officers are provided the right professional growth opportunities in key command and operational positions. The first Air Force board recently convened to review and competitively select officers for these unique leadership positions. In an effort to retain our highly skilled

enlisted force, the Air Force offers a selective reenlistment bonus that provides additional incentive to continue to serve our nation in this emerging mission.

### ***Lead Through Teamwork, Partnerships and a Strong Warfighting Narrative***

Conducting successful operations in cyberspace requires seamless integration with a host of mission partners. In many ways, cyber is a “team sport” and Air Forces Cyber (24<sup>th</sup> Air Force) is wholly committed to strengthening our relationships with other Air Force partners, our sister Services and interagency counterparts, Combatant Commanders, coalition allies, as well as civilian and industry partners. Given the proximity of our headquarters and close mission alignment, 25th Air Force continues to be a critical strategic partner across all of our missions. The 25th Air Force Commander, Major General Jack Shanahan, has been a steadfast supporter throughout the standup of the Cyber Mission Forces.

U.S. Cyber Command serves as the focal point for all Department of Defense cyber operations. As one of the four Service Cyber Components, we provide an array of cyber forces and capabilities in order to defend DoD Information Networks (DoDIN), support Combatant Commanders, and strengthen our nation’s ability to withstand and respond to cyber events. The recent stand-up of the Joint Force Headquarters DoDIN under the leadership of Lieutenant General Hawkins and the Defense Information Systems Agency (DISA) was a major milestone in normalizing the command and control of network defensive operations.

As already highlighted, we partner closely with the Air Reserve Component in day-to-day cyber operations. Through a compliment of Traditional Reservists, Air Reserve Technicians and Air National Guardsmen, our Air Force’s cyber units are a striking example of Total Force Integration in action. These total force professionals bring a unique blend of experience and expertise to the full spectrum of cyber missions. Many work in prominent civilian positions within the Information Technology industry, which bolsters our mission effectiveness through their willingness to serve the nation. Likewise, we are often able to retain unique skillsets gained by investment in our Airmen by supporting their continued service in the Air Force Reserves or

Air National Guard. These partnerships will be vital to our future operations as the Air Reserve Component continues to provide integrated support of the DoD's Cyber Mission Force.

Air Forces Cyber also understands the cyberspace domain is primarily provisioned by private industry and our ability to collaborate with our industry partners benefits the nation's cybersecurity posture. We have developed Cooperative Research and Development Agreements with industry leaders such as Symantec, AT&T, USAA, Northrop Grumman and 21 other partners to share and collaborate on innovative technologies and concepts. These collaborative efforts allow us to advance science and technology in support of cyberspace operations, as well as share best practices with industry partners. We continue to leverage this program and are currently in the process of enhancing our partnerships with academia.

We also enjoy strong relationships with other DoD Components. As an example, the Air Force recently aligned with the Army and the Defense Information Systems Agency (DISA) to support the development and fielding of a key technology in the transition to a Joint Information Environment (JIE). Together we are implementing Joint Regional Security Stacks (JRSS) and making enhancements to our networks with Multi-Protocol Label Switching (MPLS) as part of the single security architecture. Through this teamwork, the first JRSS "security stack" was fielded at Joint Base San Antonio-Lackland, Texas, in line with one of the sixteen Air Force Gateways. Additional "security stacks" are being installed at other AF and DoD sites as part of the JIE. These efforts [JRSS, MPLS] benefit the entire DoD by reducing attack surface of our networks and threat vectors – allowing for more standardized security of our networks and by providing increased network capacity to support defense missions.

We are also fortunate to have a long-standing, close relationship with San Antonio, Texas, also referred to as "Cyber City USA." The local community has committed significant resources to support the growth of cybersecurity both locally and nationally. Our leadership team participates in a variety of civic leader engagements to share lessons related to cybersecurity. The community leadership also understands that encouraging our younger generation to gain the needed cyber skills will be essential to our nation's success in this arena. By partnering together, Air Forces Cyber (24<sup>th</sup> Air Force) supports a broad array of programs

designed to touch young students. A good example is the Air Force Association's "CyberPatriot" STEM initiative in which our Airmen mentor cyber teams as part of a nationwide competition involving over 9,000 high school and middle school students. Another example is our "Troops for Teens" program at a local high school focused on reaching over a hundred at-risk students through exposure to military values, heritage and way of life.

### ***Equip the Force Through Rapid, Innovative Fielding of Cyber Capabilities***

We are also making gains in improving our acquisitions process to support the ever changing technology of cyberspace. The Air Force Life Cycle Management Center has worked diligently to streamline our ability to provide solutions to support our cyber missions through "Rapid Cyber Acquisition" and "Real Time Operations and Innovation" initiatives. These efforts have resulted in the fielding of capabilities that have thwarted the exploit of user authentication certificates, the unauthorized release of personally identifiable information, and the blocking of sophisticated intrusion attempts by advance persistent threat actors. These technical solutions were developed and fielded in weeks to months.

Similarly, Air Forces Cyber (24<sup>th</sup> Air Force) is working closely with 25<sup>th</sup> Air Force to improve our development, fielding and employment of multi-domain capabilities that leverage the Air Force's unique strengths in cyber, electronic warfare and intelligence, surveillance and reconnaissance. The collaboration is enabling Airmen to drive innovative solutions to many of our most challenging operational challenges. It also harnesses the subject matter expertise in other Air Force organizations such as the Air Force Research Laboratory, Air Force Institute of Technology, National Air and Space Intelligence Center, Air University, Air Force Academy, as well as academia and industry to meet growing joint warfighter needs.

### ***Conclusion***

We are proud of the tremendous strides made by Air Forces Cyber (24<sup>th</sup> Air Force) to operationalize cyber capabilities in support of joint warfighters and defense of the nation. Despite the challenge of growing and operating across a diverse mission set, it is clear Air Force

networks are better defended, Combatant Commanders are receiving more of the critical cyber effects they require, and our nation's critical infrastructure is more secure due to our cyber warriors' tireless efforts. They truly are professionals in every sense of the word.

Congressional support has been essential to the progress made and will only increase in importance as we move forward. Without question, resource stability in the years ahead will best enable our continued success in developing Airmen and maturing our capabilities to operate in, through and from the cyberspace domain. Finally, resource stability will foster the innovation and creativity required to face the emerging threats ahead while maintaining a capable cyber force ready to act if our nation calls upon it.