NOT FOR PUBLICATION UNTIL RELEASED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

DEPARTMENT OF THE AIR FORCE

PRESENTATION TO THE SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

HOUSE ARMED SERVICES COMMITTEE

U.S. HOUSE OF REPRESENTATIVES

SUBJECT: IMPROVING MILITARY CAPABILITIES FOR CYBER OPERATIONS

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

NOT FOR PUBLICATION UNTIL RELEASED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

July 25, 2012

Introduction

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

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

A strategic discussion on cyber is no longer simply a DoD activity; it is a national imperative. We did not arrive at this point overnight. For many decades, leaders in engineering, cryptology, computer science, information technology, and many other contributing disciplines expanded and then integrated these technologies. Yet although the technical disciplines were varied, the application of cyber now follows a path similar to ground, sea, air, and space in their early inceptions. Akin to the Wright Flyer's relationship to the F-22, mainframes and eventually personal computers were the harbingers of our cyber capabilities. Continued platform development led to aircraft being used as a ground forces and intelligence enabler during Army Air Corps operations. Similarly, integrated networks enabled the rapid dissemination of information for defense and intelligence operations…but now we recognize that these capabilities are foundational to mission success. Code-breaking and cryptology applied to secure communications foreshadowed today's cyber information assurance and exploitation capabilities. The application of cyber capability to enable or enhance ground, sea, air, and space operations continues to accelerate; but as with airpower, we should similarly expect cyber to emerge as a strategic alternative.

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

Deliver a Robust, Defensible, Trusted Network

As you have discussed and are working to address through legislation; cyberspace is not simply the internet; rather, it is a network of interdependent information technologies, including the internet, telecommunications networks, computer systems, and embedded processors. Its use has become ubiquitous and every public, industrial, academic, and military organization expects reliable access. The Nation and our Air Force, working in collaboration with all Services, have increased weapon system performance, extended operational capabilities, and enhanced command and control by leveraging cyberspace. At the same time, we are fully cognizant that our adversaries will continue to use this common ground to steal, compromise, degrade or destroy information, disrupt networks or communications, or deny service. The dynamic nature of cyberspace means that as technology advances and expands, so does our adversaries' ability to exploit and attack. Hacktivists, terrorists, cyber criminals and state-sponsored hackers are active in cyberspace networks across the globe; our military networks are no exception. DoD networks are probed millions of times per day: beyond the defensive contribution of the DoD gateway actions, the Air Force blocks roughly two billion potential threats and denies two million spam e-mails each week; however, as General Alexander has previously articulated, passive defenses are necessary, but not sufficient. Armed with an understanding of the growing threat to and our dependency on the network, Air Force leaders directed a Service-wide movement to increase defensibility by creating the AFNet Migration and applying a "defense-in-depth" alignment.

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

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

There are many advantages to be gained by the AFNet Migration, with the most important being the opportunity to now increase sensoring and automation and introduce situational awareness. In the U.S. Central Command's Combined Air Operations Center, walls are filled with screens depicting operational status and providing battlefield video feeds for real-time analysis and decision-making. The corresponding cyber information depicting network operational status and enabling real-time analysis does not currently exist, nor was it possible prior to the re-architecting of the AFNet. Operators in the 24th AF's command and control unit manually perform the task of data synthesis after distant-end units enter status information into the system. There is no common operating picture of activity across our networks, making it more difficult to assess and respond to the threat environment. Yet there are innovators; cyber professionals from many career fields who apply capabilities and leverage new tactics, techniques, and procedures daily to successfully provide mission assurance, threat detection and response, and network operations and defense. The capabilities for sensoring, status monitoring, and automation of operational activities will continue to expand, and so must the capacity elements necessary to reach and execute full spectrum cyber operations globally. Migration to a single architecture provides the opportunity for Air Force-wide network situational awareness -- an awareness that enables robust, defensible and trusted air, space, and cyber operations.

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

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

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

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

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

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

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

Operationally Leverage Cyberspace Capabilities

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

We have come a long way in changing our priority from network assurance to mission assurance. A great example of our efforts in this area is our support to Remotely Piloted Aircraft (RPA) missions. In order to provide mission assurance, we had to conduct extensive front-end mapping to understand the various links from the U.S. to the overseas flight. We found the system was designed with roughly 180 touch points, many of which are not military-controlled, across several different networks making it critical to establish relationships with commercial organizations. The forward commander of Joint air assets prioritizes the most critical RPA missions, and then our Operations Center identifies links and takes proactive steps to ensure the availability of key nodes and reinforce failure points along the network infrastructure. We focus our resources on the highest priority of RPA missions to deliver the greatest downrange advantage. This provides a stark contrast to previous net-focused priorities that resulted in equal defense across the network.

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

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

The complexity of the tasks Air Forces Cyber encounters are typically not a limiting factor to engagement, but recognizing and leveraging the necessary authorities to accomplish the mission continues to be a challenge. Recently, we acted upon these authorities after notification by the Federal Bureau of Investigation, through work conducted at the Air Force Office of Special Investigations and the Navy Cyber Defense Operations Command, that multiple Air Force ROTC computers on a single campus had been compromised. Collaborative efforts between Air Forces Cyber and AFISRA units performing incident and attribution analysis led to the identification of the malware and leveraging that information to defend the Air Force Global Information Grid. Further collaborative investigation identified potential architectural weaknesses through which compromised accounts could be used to access Air Force networks. This broader understanding will allow our cyber engineering and acquisition communities to modify our architecture to mitigate similar types of risks. Additionally, the analytic capabilities of the Rhode Island Air National Guard's 102nd Information Warfare Squadron will be leveraged in the continuing investigation of this incident. These relationships allow the Air Force to engage along non-warfighting avenues and build, scale and deliver capabilities for USCYBERCOM and in defense of the Nation.

Build and Deliver Combat Power

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

A successful STEM program requires collaborations and partnerships with local and national academia and civic leaders. At the high school level, CyberPatriot was initiated by the Air Force Association, through extensive partnerships with the Center for Infrastructure Assurance and Security at the University of Texas in San Antonio, creator of the National Collegiate Cyber Defense Competition, along with Northrop Grumman and other defense and private industry leaders. It has become a premier national cyber defense competition which inspires students toward careers in cyber security and other STEM disciplines. Last year's competition grew to over 1600 teams from schools in all 50 states and 2 U.S. Department of Defense Dependent Schools overseas, and this year's event hopes to redouble that participation. The students gain specialized instruction, industry and government internships and the benefit of realistic application of their newfound expertise in a competitive environment. Major John Picklesimer of our 92nd Information Operations Squadron was an instructor and mentor to the San Antonio-area CyberPatriot team, and we could not have been prouder when that same team placed first at the national competition on defensive principles and campaign planning. At the collegiate level, students compete at the National Collegiate Cyber Defense Competition and future cyber defenders test their acumen in the National Security Agency's Cyber Defense Exercise. In a separate program, selected ROTC cadets like distinguished graduate and 24 AF's own Captain Mike Stamat, attend the Air Force Research Laboratories' Advanced Course in Engineering summer program that provides aspiring cyber professionals hands-on internships and cyber officer development. In every one of these program, global excellence starts with local commitment and nationwide government, industry and academic collaboration.

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

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

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

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

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

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

We continue to require foundational acquisition programs to develop and field large-scale capabilities. However, a factor that hinders the rapid development of cyber capability is the outmoded acquisition practices, policies, and rules that guide cyber acquisition from the top down. The current acquisition system was constructed and optimized to support the acquisition of large weapon and training systems. These programs are built from requirements that are defined years in advance and remain relatively static throughout the programming process. The end result is the acquisition of outdated equipment and inflexibility that prevents us from adapting leading edge technology while it is still leading edge.

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

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

The Air Force culture of innovation continues in Air Forces Cyber. We continue to leverage a new "tech refresh" methodology that focuses on implementing new capabilities rather than incremental system upgrades. Instead of maintaining an aging "wired" infrastructure, Air Force Space Command and 24th Air Force are pursuing the potential of commercial wireless technology to lower base infrastructure costs and increase situational awareness on critical infrastructure. Entire nations have skipped "wires" and leapfrogged generations of IT, and the Air Force is exploring how to incorporate this rapidly emerging technology to increase our return on network infrastructure investment.

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

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

Conclusion

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