NOT FOR PUBLICATION UNTIL RELEASED BY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

DEPARTMENT OF THE AIR FORCE

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

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

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

September 23, 2010

NOT FOR PUBLICATION UNTIL RELEASED BY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

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

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

Air Force Cyber Forces

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

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

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

Fourth, we have streamlined our acquisition processes to give our Airmen the cyberspace tools they need, when they need them. Our acquisition professionals will have the processes and authorities needed to rapidly deliver Cyber capabilities for operations in an increasingly dynamic

and contested environment. Everything we do begins and ends with the needs of the Joint Force Commanders and our measure of merit is how well we contribute to the Joint team.

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

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

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

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

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

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

Mission Assurance

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

Under the mission assurance paradigm, we are no longer communicators; we are "Cyberspace Operators." We have centered the focus on conducting the mission, not just providing a service. We are also conducting deliberate planning with the Component Numbered Air Force (C-NAF) commanders, which are the leaders of the Air Force warfighting units presenting forces to the Combatant Commanders. We are working with them to identify the

assets these warfighters must have in order to execute their Joint mission. We then prioritize those critical assets and map their dependencies to capabilities and infrastructure in cyberspace. Once we know where those dependencies lie, we perform analysis to determine what vulnerabilities and failure points in cyberspace threaten those critical assets. These threats can be malicious or simply accidental. Regardless, we take responsibility for identifying, proactively preventing, or in the worst case, rapidly recovering from an incident to avoid mission failure.

Operate Through an Attack

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

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

Instead, we are pursuing a defense-in-depth strategy that segregates internal assets based on their prioritization as determined during deliberate planning. We build defended asset lists, map our Cyber dependencies, and provide higher levels of security for more valuable, mission-critical resources. Attackers must therefore overcome increasingly greater protections to gain

unauthorized access to higher value resources. Moreover, with our situational awareness tools focused on critical assets we can detect important unauthorized access or activities much faster.

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

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

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

Cyberspace Situational Awareness

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

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

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

We are working to build a single, integrated cyberspace situational awareness picture for the Air Force enterprise. Initially, we're working to bring together a number of existing feeds

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

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

Joint Integration

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

Conclusion

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