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 (24th 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 (24th 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 (24th 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$^{th}$ 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 (24th Air Force) is working closely with 25th 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 (24th 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.