CyberPro

December 2010

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: MAJ. GEN. RICHARD WEBBER

NSCI's Lindsay Trimble recently had the opportunity to interview Major General Richard Webber, commander of 24th Air Force and Air Force Network Operations, at Lackland Air Force Base, Texas. Webber is responsible for the Air Force's newest numbered air force, providing combatant commanders with trained and ready cyber forces which plan and conduct cyberspace operations. 24th Air Force personnel extend, maintain and defend the Air Force portion of the Department of Defense global network. Since his commissioning in 1975, Webber has commanded a missile squadron, support group, missile operations group and missile wing equivalent and two space wings. He is a command space and missile operator with qualifications in the Minuteman II, Minuteman III, Global Positioning Satellite and Counter Communications System weapon systems.

NSCI: What is the 24th Air Force's relationship to other Department of Defense organizations supporting cyberspace operations?

WEBBER: The 24th Air Force is the Air Force's component to U.S. Cyber Command, a sub-unified command subordinate to U.S. Strategic Command. Each of the services has a respective cyber component: Fleet Cyber Command, Army Forces Cyber Command and Marine Forces Cyber Command. When USCYBERCOM declared initial operational capability in May, the 24th Air Force along with Air Force Space Command established lines of communication with each of these elements to synchronize efforts. This communication and teamwork will continue as all the services grow beyond their initial declaration of full operational capability and into the foreseeable future.

We established an Air Component Coordination Element which is assigned to USCYBERCOM at Fort Meade. The ACCE serves as my personal representative to the commander of USCYBERCOM and will provide Air Force cyber expertise through direct liaison and reach-back to the USCYBERCOM staff.

NSCI: How do 24th Air Force operations integrate with the various Component Numbered Air Forces (C-NAF) supporting other Combatant Commands?

WEBBER: Each Component Numbered Air Force (C-NAF) establishes and maintains relationships with their assigned Combatant Commands in order to provide required operations forces and recommendations when appropriate. 24th Air Force partners with other C-NAFs to integrate cyber expertise in operational planning. The primary means of partnering is the Cyber Operations Liaison Elements (COLE) supporting each of the C-NAFs. The COLE will inject cyber expertise at the point of synchronization with the combatant commander.

Another key part is the establishment of C-NAF defended asset lists within the context of the C-NAF commander's intent. 24th Air Force works with the partner C-NAFs to build situational awareness of their cyber vulnerabilities, determine what systems are necessary for mission assurance and then works with those C-NAFs to secure their systems through multiple layers of dynamic defense.

NSCI: As the Air Force Cyber Component, how is the 24th Air Force fulfilling its mission to train and equip Air Force cyberspace operations? Are there any specific successes you'd like to highlight from the organization's first year?

WEBBER: Headquarters Air Force and Air Force Space Command, in conjunction with 24th Air Force, have built a rigorous program to ensure that Air Force cyber operators have the knowledge and tools to be able to operate in the cyber domain in a secure and deliberate way. Partnering with Air Education and Training Command, we have developed Undergraduate Cyber Training to mirror other operational training pipelines. Headquarters Air Force Space Command is leading the charge to identify requirements for and develop suitable initial qualification and mission qualification training programs to provide system-specific training to our cyber operators with the goal of delivering a fully capable operator to our cyber operational units. We are now providing professional development courses to our cyber operators; Cyber 200 provides professional development during the first half of an operator's career and Cyber 300 provides professional development in greater depth in the latter half of an operator's career. All of this is modeled after what has been done for many years in training the air and space operators, creating a "Culture of Cyber" on par with the other operational domains.

This build-up of training rigor is a large part of the effort to establish throughout the Air Force a mindset change on how cyber operations are conducted. Mission assurance is the No. 1 goal in current cyber ops, versus the old paradigm of network assurance. Prior to operationalizing cyber, the Air Force would default to shutting down a system that was under imminent threat, which would save the information under attack, but would also halt the required Air Force missions being done through the threatened system. Mission assurance provides capabilities to work through a highly contested environment, allowing the Air Force missions to continue unhindered while protecting the most essential information and systems.

Additionally, Air Force Space Command declared 24th Air Force to be at Full Operational Capability Oct. 1, which is a great achievement with less than 14 months of existence.

With the creation of 24th Air Force, more than 12,000 Air National Guard and Air Force Reserve cyber experts now have a single organization to partner with in the execution of cyber missions. Training of cyber professionals is being looked at across the total force spectrum of active, reserve and civilian positions, ensuring our cyber warriors are fully trained for the challenging missions they face.

NSCI: A hot topic in the news is the lack of enough cyberspace professionals to fill all of the available positions in the military, government and industry. What is your team doing to develop enough highly-skilled cyber experts?

WEBBER: Part of creating the “Culture of Cyber” and operationalizing the cyber domain is continuing education for our cyber professionals. These professionals include more than the 17D and 1B specialties. To ensure the development of all the critical skills and specialties needed to establish, control and leverage the cyberspace domain, we have built a rigorous architecture of training and development for all those working in cyberspace operations.

The undergraduate cyber training is now run by AETC at Keesler Air Force Base, Miss. Initial and mission qualification training are done at the unit level, but with very methodical and documented requirements for training certification. These are used to ensure personnel sitting in critical positions have all the requirements necessary for a Combat Mission Ready designation. This designation creates rigor and structure in cyber operations, and delineates operators from sustainers. We are ensuring focused cyber career professional development, such as the Cyber 200 and 300 courses mentioned earlier. These courses will contribute to the deliberate development of cyberspace professionals. They will leverage students’ experiences and training to enhance their abilities to integrate and apply cyberspace capabilities at the operational and strategic levels of Department of Defense operations.

Also, the Air National Guard and Air Force Reserve capture critical skill sets from the corporate world and employ these resources through established unit programs and Individual Mobilization Augmentees. Citizen Airmen carry the skills they learned while on active duty and compliment them through civilian workplace education and training to provide the Air Force with a cost effective resource that provides continuity and surge support to the cyber domain.

NSCI: How vulnerable is the Air Force to a cyber attack? What has the 24th AF done to prepare for the increase in large-scale cyber attacks and the significant impacts cyber attacks may have on our nation?

WEBBER: We teach Airmen to have a weapons system mindset about the network. Every Airman needs to know that when they sit down in front of a terminal and log on to our network, they are our strongest and our weakest link at the very same time. On Oct. 4, we started our Basic Military Training cyber awareness course, instructing new Airmen on the potential impact their interaction with the cyberspace warfighting domain can have. Placing cyber training in the basic training curriculum emphasizes the importance of operating securely in the cyber arena – the BMT cyber curriculum allows us to imbed cyber security principles at the earliest point in the Airman’s career. Cyber education is also included in professional military education venues for officers and enlisted members throughout their careers to reinforce the discipline and rigor required on the Air Force network.

NSCI: What are some of the key challenges facing the Air Force regarding cyberspace operations?

WEBBER: Threats to security in this domain are just as real and significant as physical threats. The frequency and sophistication of malicious activity is increasing exponentially and new methods are being developed every day.

Another big challenge is due to the highly dynamic nature of cyberspace. It is absolutely critical that we create automated situational awareness of our cyber networks. The warfighter requires insight and situational awareness in any system connected to the Air Force network, including non-Air Force systems with which we have trusted connections (e.g., Defense Information Systems Agency, National Security Agency, National Reconnaissance Office, sister services, contractor networks, etc). It's not enough to simply understand the configuration of the network. 24th Air Force must be able to map the essential mission activities to the segments of the network supporting these activities, and then employ defensive capabilities to protect those segments as needed. This is foundational to mission assurance. Furthermore, human analytical capability is required for higher level threats.

We are also in the process of building a network defense in depth, concentrating on dynamically protecting our most important assets to ensure mission assurance. What we need is a new paradigm for defense – one that is designed into the networks from the beginning, rather than simply adding on protective measures afterwards. We are focusing our defensive efforts on our “crown jewels” – those systems and capabilities vital to Air Force mission accomplishment – instead of trying to defend the entire network.

Air Force Space Command has the responsibility to organize, train and equip the Air Force network, and 24th Air Force has responsibility to define the strategy for defending it. To be effective in the future, the architecture must be based on a solid strategy. This imperative guides the development of a strategy-based architecture for the Air Force network. Conceptually, the strategy-based architecture acknowledges the requirement to support the operational scheme of the warfighters and inculcate the newest technologies in support of operational objectives. Our challenge is to lay the groundwork for the integration of an operational scheme of maneuver in cyberspace with the technologies that will best support our objectives.

NSCI: How does your team keep up with the rapid changes in technology and threats? How does innovation from organizations such as the Air Force Research Laboratory and industry help?

WEBBER: Industry is the primary driver behind innovation within the cyber domain. Our traditional acquisition system was built to support systems such as tanks and aircraft that have a different technology cycle. The Air Force has recognized this shortfall and Air Force Space Command is working with the Electronic Systems Center to streamline cyber acquisition, in an effort to deliver systems at the “speed of need.”

Our current acquisition pyramid consists of three layers. The top layer is for real-time operations. When we need a tool in hours or days, we have the 688th Information Operations Wing to develop or acquire and test tools in a very expeditious way. The middle layer is for urgent operational and joint urgent operational needs. When we need a tool in months to a few years, these acquisition processes provide us with quick reaction capability delivery, or modifications to existing capabilities. The bottom layer is the traditional acquisition process, when we can wait several years to acquire the capability. All together these different types of acquisition give us more flexibility to get the right tools at the right times. In addition, the Air Force works closely with our industry partners to keep abreast of the newest technologies, especially those associated with defending our networks.

AFRL and the National Laboratories also play a key part in keeping the Air Force on the leading edge of cyber technology, and these organizations play a role in the Air Force's strategy for cyber innovation. The Air Force recently stood up a "Cyber Safari," modeled after the Big Safari program. This is part of the middle layer of the acquisitions pyramid described above and can help us transition capabilities from AFRL to our operational units.

NSCI: What opportunities do you see for industry, academia and international partners to collaborate with the Air Force?

WEBBER: Partnering with academia, industry and other government agencies is the key to staying current with the rapid advances in cyber technology. From what I've seen so far, the local academic institutions and elected officials are moving ahead in that respect.

We currently participate in a number of working groups with local San Antonio universities and numerous defense contractors, and we supported several local events in 2010, with the intent to continue such support in the future. Our work with the Cyber Innovation and Research Consortium, the Defense Technology Cluster, Texas Lyceum and the Armed Forces Communications and Electronics Association help to further cyber organizational cooperation. We support events such as the National Collegiate Cyber Defense Competition – an effort encouraging higher learning in the cyber career fields. We are constantly looking to create new organizational relationships that will encourage growth in cyber awareness and innovation.

NSCI: Is there anything else you'd like to add?

WEBBER: 24th Air Force has made significant progress in our short 15 months of existence, due to the hard work of our talented personnel. But there is much left to do in this new domain. Operationalizing the cyber domain, ensuring our operators have world-class training and capabilities and protecting and defending our Air Force networks will require dedication, cutting-edge technology and access to a new generation of cyber warriors. We are a few steps into a thousand-mile journey whose purpose is to deliver world-class cyber capabilities and personnel to our combatant commanders at the speed of need.