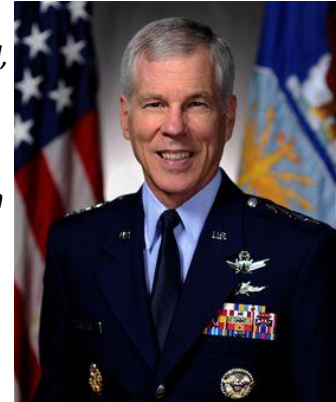




### SENIOR LEADER PERSPECTIVE: GENERAL WILLIAM L. SHELTON, USAF

NSCI's Charles Winstead recently had the opportunity to interview General William L. Shelton. General Shelton is Commander, Air Force Space Command, Peterson Air Force Base, Colo. He is responsible for organizing, equipping, training and maintaining mission-ready space and cyberspace forces and capabilities for North American Aerospace Defense Command, U.S. Strategic Command and other combatant commands around the world. General Shelton oversees Air Force network operations; manages a global network of satellite command and control, communications, missile warning and space launch facilities; and is responsible for space system development and acquisition. He leads more than 46,000 professionals, assigned to 88 locations worldwide and deployed to an additional 35 global locations.



General Shelton entered the Air Force in 1976 as a graduate of the U.S. Air Force Academy. He has served in various assignments, including research and development testing, space operations and staff work. The general has commanded at the squadron, group, wing and numbered air force levels, and served on the staffs at major command headquarters, Air Force headquarters and the Office of the Secretary of Defense. Prior to assuming his current position, General Shelton was the Assistant Vice Chief of Staff and Director, Air Staff, U.S. Air Force, Pentagon, Washington, D.C.

**NSCI:** You recently became the Commander, Air Force Space Command, which now includes responsibility for cyberspace forces. How is the command doing at bringing this new mission online? What areas do you plan to focus on?

**SHELTON:** I believe we've made great strides in just over 2 years. We stood up 24th Air Force, our new cyber numbered AF, with 3 wings and an operations center, and it now has been declared fully operational. We, in partnership with Air Education and Training Command, are well on our way in transforming cyberspace training and education into the standard AF operational training model. We partnered with the AF Headquarters Chief Information Officer and Deputy Chief of Staff for Operations, Plans and Requirements to create officer and enlisted cyber operations career fields. In concert with AF Materiel Command, we are developing a rapid cyber acquisition construct to meet our operational requirements. And finally, we're getting our arms around our programming, budgeting and sustainment responsibilities to bring an enterprise focus to our cyber business. All that said, we still have much to do.

**NSCI:** In November 2009, we loaded "The United States Air Force Blueprint for Cyberspace" to our Cyber Reference Library. It's been downloaded a couple of thousand times and we routinely hear positive comments on it. Are there any plans to update the document?



**SHELTON:** While the Blueprint is 17 months old, it is a 5-year plan to operationalize the AF's cyber enterprise. We really need to let the dust settle a bit from the organizational, training and operational changes we've been through. We'll take a look at the end of the year and decide if we need to publish an update.

**NSCI:** When you were at 14AF/JFCC Space, increasing space situational awareness was beginning to be a high priority. Now we hear a lot about the need for better cyberspace situational awareness. How do you envision the AF contributing to and leveraging that increased SA?

**SHELTON:** As in every domain, it's difficult to provide command and control if you can't "see" and the scale of the arena is enormous. Just within the Air Force we are currently responsible for 21 unique networks with over 800,000 users accessing 1.9 million networked devices over which approximately 168 Terabytes of information flows each week. Each week, AFSPC assures the reliable delivery of information while simultaneously screening for cleverly disguised virtual needles in a haystack of data.

Consequently, we are pushing hard to develop technological solutions and improved operator processes to increase SA of cyberspace for 24 AF as we are transitioning to a single Air Force network. This is a big step which will create the conditions for increased situational awareness and enhanced defensive capabilities. We are partnering with AF Research Laboratories and industry to improve our network monitoring through improvements in network sensors, thereby reducing the time to detect and characterize threats.

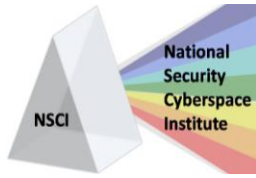
We are also working to better integrate intelligence information on adversary intent, threats to our networks, and indications and warnings of potential attack. This will help us support the joint warfighter by ensuring our AF cyber capabilities stay available when and where needed.

**NSCI:** Within the AF, DoD, and government as a whole, the cyberspace command and control roles, responsibilities, and authorities seem to still be a work in progress. Is that a fair statement? What would you like to see happen to clarify things over the next year or two?

**SHELTON:** Let me speak just to my corner of the world. In the Air Force, we have a clear definition of the cyberspace command and control roles and responsibilities and authorities. And it's clear how we plug into USCYBERCOM via our component, 24<sup>th</sup> AF. Our focus at AFSPC is to continue to develop the necessary standards and processes to operationalize and normalize cyberspace operations.

**NSCI:** What do you see as the major challenges to integrating cyber capabilities with other domains and capabilities?

**SHELTON:** I believe we need to continue to provide realistic training environments where AF cyber capabilities can be integrated with other domains, as well as challenged such that we are forced to operate in a contested domain. It's amazing to see the synergies that are possible when you put the domain experts together and allow them to innovate.



# CyberPro

April 7, 2011

## *Keeping Cyberspace Professionals Informed*

**NSCI:** There have been some fairly recent changes to how Information Operations is being viewed within DoD. How would you explain the current relationship between Cyberspace and Information Operations? Where do you see it going in the future?

**SHELTON:** I am more inclined to disaggregate the mission from the domain. We can conduct Info Ops missions from literally every domain, including cyberspace. Once we think about it in this way, it's clear that cyber capabilities can be used in conjunction with information operations tactics, techniques and procedures to accomplish the information operations objectives of the warfighter.

**NSCI:** How is the AF coordinating with the other services, USCYBERCOM, and/or departments to improve cyber information sharing?

**SHELTON:** When USCYBERCOM declared initial operational capability in May 2010, the 24th Air Force (AFCYBER) along with Air Force Space Command established lines of communication with each of the services' cyber component: Fleet Cyber Command, Army Forces Cyber Command and Marine Forces Cyber Command. All the services collaborate with and through USCYBERCOM's Joint Operations Center to ensure they are sharing information. This communication and teamwork will continue to grow as all the services mature their components.

For AF focus, we established an Air Component Coordination Element (ACCE) to provide on-site support to USCYBERCOM. The ACCE serves as the AFCYBER commander's personal representative to the commander of USCYBERCOM and will provide Air Force cyber expertise through direct liaison and reach back to the 24 AF staff.

**NSCI:** How do you think industry can best help the AF improve its cyberspace capabilities?

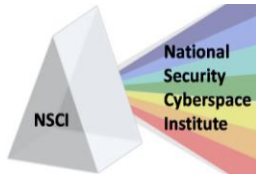
**SHELTON:** Cyberspace is a fast-changing environment, and the AF has to be able to respond quickly to that change. Industry can help us achieve that goal in three ways...interoperability, scalability and embedded security. We face a significant integration challenge when we buy disparate tools from various vendors and then have to spend considerable time, money and resources to create coherent effects. Usually, we end up with overly complex systems that have additional vulnerabilities for an enemy to exploit. Additionally, we need tools that are scalable as a single point threat today could quickly escalate into an enterprise-level issue. We need to be able to address that threat quickly...without having to go through the entire acquisition process to get another tool. Finally, too often we get tools that perform their primary mission well, but then we have to add security tools to protect them or patch vulnerabilities they create. We must have tools that have security embedded from the start.

**NSCI:** If you had "one more dollar" to invest in improving cybersecurity, where would you spend it (e.g., policy, education, training, offense, defense, situational awareness)? Why?

**SHELTON:** Today's answer: I would spend it on training. We need to build the cyber career force as part of my larger goal of normalizing and operationalizing cyber in the AF. Modeled after space professional

---

110 Royal Aberdeen • Smithfield, VA 23430 • ph. (757) 871-3578



# CyberPro

April 7, 2011

## *Keeping Cyberspace Professionals Informed*

development, we are shaping the use of cyber capabilities in exercises, simulations, and war games. Additionally, we are developing higher education courses and including cyber-specific training into the AF weapons school curriculum. Our goal is to create critical mass such that our talented Airmen can help us connect the dots on the future of cyber operations—integrated into joint operations.

We will utilize training opportunities to help drive a culture change throughout our military, civilian and contractor workforce. Every person who touches our network must be imbued with the mindset that a vulnerability introduced by one is a vulnerability accepted by all.

After we establish adequate training opportunities, I would spend the next dollar on developing additional situational awareness capabilities. We operate with the mindset that the adversary is already on our networks, and our challenge is to operate through that potentially hostile presence. But I would prefer to operate with certainty of who is on the networks, and have the capability to deterministically address that threat.

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

**SHELTON:** It's very clear to us that the government does not lead technological development in the cyber domain. Industry is in front of us, with the agility to move quickly in concert with Moore's Law. We plan to continue close partnerships with academia, industry, and government agencies to stay abreast of rapid advances. There are many challenges ahead, but we believe we are now organized and have the appropriate focus in the AF to step up to these challenges.

**NSCI: Thank you very much for taking the time to visit with us.**