CyberPro

June 2, 2011

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Steven J. Spano, Brigadier General, USAF

NSCI's Charles Winstead recently had the opportunity to interview Brigadier General Steven J. Spano. Brig. Gen. Spano is the Director of Communications, Headquarters Air Combat Command, Langley Air Force Base, Va. He is the functional leader for 15,000 communications professionals, providing information technology services to 101,500 active-duty military and civilian members at 30 major installations in the United States and overseas. General Spano directs the activities of 40 Reserve communications units upon their activation. He is responsible for policy guidance, program management and resource allocation supporting the command's mission to provide nuclear forces for U.S. Strategic Command, theater air forces for the U.S. Northern Command, U.S. Central Command, U.S. Southern Command, U.S. European Command and U.S. Pacific Command, as well as air defense forces for the North American Aerospace Defense Command.

General Spano was born in Albany, N.Y. He was commissioned in 1983 through the ROTC program at Norwich University, Northfield, Vt. The general has commanded at the detachment, squadron and group levels. In addition, he served in key joint assignments at the National Security Agency, the Joint Staff, and U.S. Forces Korea. Prior to his current assignment, he was Deputy Chief of Staff Communications and Information Systems, Multi-National Force-Iraq, Baghdad, Iraq.

NSCI: You've been ACC/A6 a little over 2 years now. A lot has happened during that time, including the stand-up of USCYBERCOM and the AF alignment of cyberspace under AFSPC. How have these changes affected ACC and the AF as a whole?

Spano: We have been rebalancing our emphasis from the legacy role of acquisition, ops and sustainment, and assurance of traditional core services toward enabling MAJCOM-specific mission systems and their integration. This doesn't mean the ACC/A6 is out of the communications planning area, but it does mean that we're transforming to the end state of AFSPC/USCYBERCOM assuming more and more of the core services roles. By refocusing the limited remaining resources, we'll ensure that infrastructure and systems planning are sufficient to meet the current and future needs of the Warfighter while we focus on enabling Combat Air Force (CAF) and ACC command and control operations.

As part of this refocus, we are empowering the staff to adopt an approach where they become even more tightly integrated with the functional communities and as trusted partners to the Warfighter.

Solving the tough cyber-related problems has and will be a core function, but we are becoming more heavily invested in the functional application and integration of command and control, intelligence, and logistics capabilities rather than primarily the underlying infrastructure and network dial tone of the past. While the skill sets are different and retooling of the work force is required, I'm confident the staff will respond to these new challenges.

NSCI: What would you like to see ACC/A6 focus on for 2011?

Spano: I'd like to highlight two major focus areas; one is enabling true, collaborative knowledge operations across the command (and AF); and two, focus efforts on Ops and Intel related systems.

Knowledge operations, or KO, has been a focus area for the AF, and a personal passion, for the last 10+ years. We have come a long way towards improving decision superiority utilizing KO tools and new processes but continuous improvements will drive KO into 2020 and beyond… through both tools and policies/procedures. We authored an AF enabling concept of operations for KO and began driving toward its implementation as we work through the staffing process. For instance, we are working vigorously toward an enterprise content and records management solution, enterprise task management workflow, business workflow development, "YouTube-like" video distribution for training and commander's messages, and a comprehensive mobility strategy. This shifts the work force from the traditional static email in-box into a customized, collaborative, role-based mobile work environment. We also continue to lead the Air Force efforts in delivering an innovative, unified communications strategy to enable seamless, ubiquitous connectivity for our Airmen while reducing dependence on costly legacy infrastructure. Underpinning these efforts is policy/procedures, which we are documenting in the CAF's Information Strategy. This capstone strategy will support continued growth, standardization, and accessibility supporting mission requirements for secure, reliable information sharing.

The second focus is operations/intel , where we continue to make progress in such areas as communications support to aerial network integration, command and control systems, and information assurance of mission systems. First, we're embedded deeply in the ACC staff's roadmap efforts for building the next generation aerial networking capabilities and their linkages with air platforms. This is a great example of taking our core networking skills and bringing it to another level with air platforms and tactical data links. Another example is our work to build mission-related information strategies to codify the missions, systems, and personnel interactions, enabled by IT, to document how functional C2 programs must interact. By detailing these information exchange strategies, we've made great strides in improving how we achieve decision superiority. And finally, the Cyber Surety professionals, the men and women documenting, correcting, and guiding the integration to ensure our systems meet regulatory and, most importantly, mission assurance requirements.

The staff successes this year have been evident in base networks to functional systems… and we must continue these efforts as the threat continues to evolve and we focus on mission systems integration.

NSCI: When most people talk cyber, they are generally referring to the Internet. It seems for ACC, and the Combat Air Forces as a whole, data links would also be included. Can you tell us what is being done to secure military data links and prevent possible compromises such as the one reported in December 2009[1]?

Spano: The military data links are absolutely critical to CAF and Air Force operations and we've continued to make significant strides in these areas. Our tactical data links are secure and deliver operational advantages every day from open to denied air space.

Additionally, our Communications Support Squadron continues to lead in the joint interoperability test arena. Last year, our superb tech team successfully tested and modified over 100 data link variants ensuring warfighting standards and requirements, to include security, were met. The data link business is definitely booming, growing at literally exponential rates, and our folks are front and center to bring them to the fight.

Finally, we are tightly integrated with the AF Command and Control Integration Center (C2IC) in building the next generation aerial roadmap along with the respective analysis of alternatives, integration strategies, cyber surety, and management. So, we are not only rooted in the present, but we are also focused on integrating and securing tactical data links for the future.

NSCI: In light of Army Private Bradley Manning's alleged leaking of sensitive and classified information recently to WikiLeaks, what steps has the Air Force taken to reduce the "Insider Threat"? Is this threat best addressed by hardware, software, process, or some combination?

Spano: The AF has addressed the WikiLeaks with a combination of education, process, and technology improvements.

First, we have stepped up education starting with AF-wide guidance explaining the problem/threat and individual responsibilities. We also re-emphasized our on-line training resources for network users and base/organization security program managers. ACC continues to stress recurring education – for example, Information Assurance Awareness; Force Protection; Information Protection.

Second, administrative processes were improved by implementing security controls for copying classified information from secure systems and networks. The AF has also instituted a formal removable media waiver process that requires the AF DAA to formerly grant waivers for organizations to transfer data from the DoD SIPRNet to removable media. This approach is necessary to ensure users protect classified information on the SIPRNet in compliance with Air Force instructions.

And finally, we've focused on how technology can help through investments like the AFNet Migration, Data at Rest efforts, and Integrated Identity management. The AFNet Migration is critical as it will bring

[1] "Insurgents Hack U.S. Drones"; Gorman, Siobhan; The Wall Street Journal; December 17, 2009; available at http://online.wsj.com/article/SB126102247889095011.html

all the MAJCOMs under a single management domain which will allow us to better focus and standardize security controls and management across the enterprise… a huge step forward that's being led by AFSPC. And while at the early stages, the Air Force is also moving out on implementing Data at Rest beginning this year and with DISA on an integrated DoD identity management solution. By better managing/securing our network and then applying additional IT-based security controls closer to the user, we'll continue to move in the right direction.

The Air Force has taken these and many other additional, reasonable measures to reduce the risk of reoccurrence. However, there is no one solution that will fully eliminate the insider risk and allow government to function effectively. The threat is being addressed from all security facets - personnel; physical; information; industrial; computer and cyber security disciplines.

Just as insiders can be a threat, they are our largest asset. Thus, our security framework has a distinct challenge in ensuring that it empowers Airmen while also protecting critical information.

NSCI: In addition to the CONUS, you've had assignments in both the Pacific and European theaters. How would you describe theater differences and similarities regarding cyber-related challenges such as situational awareness and information sharing given varying environments and threats?

Spano: While my time is dated in both theaters, the main issue still remains – secure interoperability. In Korea, information exchange, situational awareness, C2 integration, etc had to be achieved in dual language collaborative environments. GCSS-K and counter-fire systems were front and center in this challenge. In Europe, C2 interoperability was also a central theme with NATO. The growing disparity of investment in IT from the various NATO nations is making the challenge even more complex. Some nations are generations behind in technology, which make interoperability challenges more glaring and difficult to solve.

There is also the challenge of releasibility of information. That is a policy issue more than it is a technology issue. At the end of the day, the end state was the same, shared situational awareness to the extent allowable under the classification rules and guidance. However, the rule set often brought information exchange down to the lowest common denominator which affected the total picture. In the end, we tried to address these challenges by closing the gap between technology and policy in ways that fostered operational effectiveness.

NSCI: There continues to be a lot of talk regarding the need for increasing the quantity and quality of "cyber warriors." What advice would you give a new recruit or young airman in preparation for a military career in cyberspace?

Spano: Increasing the quality of cyber professionals has, and always will be, a continuous effort. However, increasing the quantity is not likely to happen in this environment given the past and pending force shaping initiatives as well as the quest to achieve efficiencies through consolidation and centralization. We have to be careful to balance natural evolution of centralized services with the continued need to maintain the spirit of innovation that made our AF great. I see a shift in many

functional areas from a centralized control and decentralized execution model to a centralized control and centralized execution model. While it may achieve some efficiency in the short run, if we are not measured in our approach, it will cost dearly over the long run in effectiveness… and relevance.

Innovation and training always occurs best at the edges, not in large central organizational structures. If we over-centralize in areas we view as strategic necessities to achieve savings, over time we will stifle innovation. Stifle innovation and you lose the heart and soul of any institution – innovation! Our young Airmen bring the type of innovative thought we need. They grew up in the digital age and think differently than us analog thinkers. They are collaborative by nature and assimilate technology while we merely accommodate it. They are less tolerant of bureaucracy and rules, are more agile, adaptive and want work to be fun. We are rigid, structured and don't mix work and play. As such, there are opposing forces at play that have significant consequences for long term relevance.

The best advice I have is for them to challenge the status quo and show the way with innovative operational uses of smartphones, tablets, wireless connectivity, mobile and social network concepts. The key to their success will be driving through the bureaucracy and solidifying the cyber constructs to make the concepts real. If they fail, we all fail as the institution cannot endure if it cannot attract and retain the best talent. They are ready and eager, and I have full trust and confidence the next young airman will continue to drive innovative thought in cyberspace.

NSCI: What improvements would you like to see regarding military and industry cyber-related partnerships?

Spano: First let me say that the relationship between the Air Force and industry is stronger than ever as we fight similar battles on the cyber front. Our industry partners continue to innovate with new capabilities that reach far beyond what was possible 10 years ago. Cloud, innovative wireless approaches, cutting edge security appliances, transformational knowledge ops tools, and web services are truly enabling AF mission operations.

With that said, we can always do better with industry in cyber security. The key lies within the often debated and frustrating topic of acquisition. Acquisition should be based on overall value, not least cost technically acceptable…analog thinking. I believe there are numerous opportunities to work through the many challenges we all recognize. A couple of examples include:

Crowdsourcing in contracting to improve transparency and increase partnerships with industry shows great promise. GSA has started this effort on a couple fronts. Typically, we release an RFI to industry for comments and then we proceed to an RFP. This generates a serial approach rather than a highly interactive approach to sharing information and ensuring the requirements are adequately documented. In a recent press release, GSA stated that this open innovation with the public would "shorten innovation cycles, involve our customers, introduce out-of-the-box thinking (or challenge the 'dominant logic'), increase customer loyalty, and get access to exclusive knowledge and creativity." More needs to be done to mature this concept, but it shows that technology and process can bridge wide gaps between industry and the government for the mutual benefit.

Another area is acquisition speed. The AF is working hard internally to address the speed at which contracting can take action for Cyber capabilities and we look to industry for support, ensuring we get it right. Such concepts as ESC's Cyber Safari reflect the lessons learned on the airborne platform side of the AF with Big Safari. The intent is to begin addressing the speed of IT acquisition in the Cyber era. We need to balance best value determinations with lowest cost, technically acceptable acquisitions to drive IT superiority. We expect best value in combat aircraft acquisitions and should expect the same for Cyber.

NSCI: The AF has done a lot of work to re-organize cyber-related jobs and provide an improved career path for "cyber warriors." Have you identified any metrics or other measures that can show whether the changes are achieving the desired results?

Spano: There is no doubt that our career field is in a distinct period in its history. The pressure of constrained resources is driving new operational constructs. Thus, there are both tactical and strategic efforts to address these challenges.

On the tactical front, we have proposed metrics/measures to achieve the desired effects at the base level but they are still under review. For example, in ACC we are gathering information on how the Client Systems Technicians consolidation is transpiring at each of our bases to identify efficiencies and address any challenges our bases are facing. The consolidation of these functions has seen its challenges but this data collection will assist in building a stronger way-ahead for that functional area. Additional key metrics worth pointing out are internal and external cyber readiness indicators such as Time Compliance Network Orders (TCNO), Mission Assurance Training through 8570, and Federal Statistics such as FISMA. Operationally, we are assessing overall network management as it relates to the right level of manning and overall expertise. Indicators such as backlog of authorized service interruptions, training and ability to keep pace with IOS updates on the infrastructure, etc are all indicators of how well we are balancing resources and skill level with adequate network performance. On a weekly basis we're tracking these key tactical metrics to ensure we understand our cyber surety levels, we've got the right education and training for our personnel through certification courses, and that our program management office systems are meeting the DoD and Federal guidelines for security.

To support these endeavors on the strategic front, we launched the "Comm Squadron of the Future" analysis which broke down the challenges and opportunities that our Base Communications squadrons are facing. In essence, our previous construct in building a Cyber Warrior was primarily via a Comm Squadron development path. Tomorrow, we have to think differently about how we develop those Cyber Warriors. A couple of constructs stick out that we're beginning to pursue in more depth: operational integration and cyber surety. For the first, we believe we need to embed more cyber professionals in the various functional areas (Ops, Intel, Logistics), to improve our focus on command and control, logistics, and other mission areas. We talked to this in the beginning of this interview. Second, we need to increase our skills in mission integration along the Cyber Surety front at the MAJCOM level. Cyber Security is so critical to every system, and by focusing communications/ cyber professionals in these areas, they'll gain the additional skills and more importantly, work with the

functionals to integrate security from the ground up. These two areas aren't the panacea but they are foundational elements to improving our cyber warrior development path.

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

Spano: First, let me thank you for the opportunity to provide our views on these very important topics. Only through communicating in forums like this can we collectively make progress in developing a comprehensive cyber strategy and professional work force.

I'd like to leave you with a final thought on security. For the last few years, our focus has been on building up boundaries, both at the edge of the network and on clients. Centuries ago, security was focused on tall, thick walls to protect critical information and resources. But, our enemies didn't stop innovating and that model of security went away, migrating to a model where each person is authenticated and their credentials open many new doors. Today's security model is fundamentally changing with the promulgation of billions of end devices. As such, it is time to relook and rework that model. Security is occurring at the transaction level. We must follow that trend as we move toward cloud services…rather than continuing to build bigger walls and boundaries that create unmanageable complexity. Cloud is about how to do computing, not where. It is about agility more than it is about efficiency. Consolidation is not cloud as cloud is built on interfaces, integration, and rapid provisioning of services through automated tools. Security and innovation are not opposing values. They can and must co-exist if we want to remain relevant in the digital age. Industry has proven it already. We have to do a gut check on whether security and privacy are really a smoke screen for trust and control. An honest answer to that will help lead us down the road to developing a comprehensive strategy for the cloud.

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