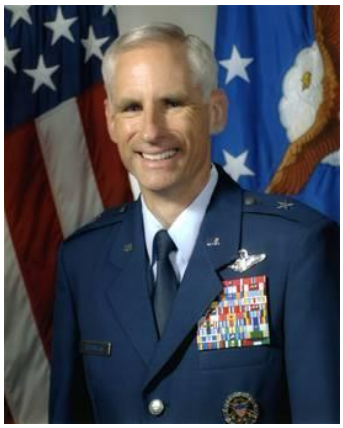
CyberPro

December 8, 2008

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE



Brig. Gen. Mark O. Schissler is the Director for Cyber Operations, Deputy Chief of Staff for Operations, Plans and Requirements, Headquarters U.S. Air Force, Washington, D.C. He is responsible for establishing and advocating policy, guidance and resources for cyber and information operations. In addition, his responsibilities include developing programs and plans for overall Air Force IO and cyber, to include electronic warfare operations, network warfare operations and influence operations. Additionally, he is responsible for the creation and development of the Air Force Cyber Career Force. He interfaces with congressional, Office of the Secretary of Defense, combatant commander, joint and major command staffs to ensure warfighting requirements are met.

NSCI: There have been a lot of opinions in the press regarding the AF's intent as it first sought to stand-up an AF Cyber Command and now is standing up a cyber Numbered Air Force under AFSPC. Can you clarify the real intent of the AF with its various cyber activities?

AF/A3O-C: Our intent has never been in doubt. The United States Air Force mission is to Fly, Fight, and Win in Air, Space and Cyberspace. Our intent has always been to organize, train, and equip our cyber forces in order to provide Combatant Commanders with capabilities to defend and operate in cyberspace and achieve our national objectives. In fact, given the digital nature of our space mission, a numbered air force assigned to Air Force Space Command is a natural fit.

It seems there has been a lot of confusion out there. Thank you for clearing that up. If I can, I'd like to follow up a few aspects of this.

NSCI: Given the relative infancy of cyberspace operations, how would you compare it to the path the AF traveled when the air domain came into being as a part of our nation's defense?

AF/A3O-C: While cyberspace operations may be a new frontier, our nation was quick to recognize the cyber domain as an equal amongst land, sea, air, and space. The US government has taken bold steps to build forces and policy to defend our national interests in this domain. The Air Force is committed to building a joint capability that dovetails with what our sister services and agency partners have so ably accomplished.

NSCI: From an operational perspective, how do you see the AF supporting organizations such as USSTRATCOM's JTF-GNO and JFCC-NW, and/or the theater Combatant Commanders?

AF/A3O-C: The Air Force will continue to build capability in both forces and equipment and be an able force provider to our Combatant Commanders. We will work with their requirements in mind seeking innovative solutions to cyber issues facing these commanders and fully integrate planning and operational support into their warfighting operations.

NSCI: Can you tell us about any initiatives the AF is currently working with the COCOMs, other Services, or agency partners?

AF/A3O-C: We have partnered with service, agency and COCOM representatives to develop a joint/interagency organizational construct for cyber operations. Recently, the Secretary of Defense signed a letter, based on this work, aligning JTF-GNO under JFCC-NW as an initial step toward a broader joint/interagency command and control solution.

NSCI: In a recent interview with Defense Systems, Maj Gen Maluda mentioned co-chairing a General Officer's Steering Group to look at cyber issues. Have there been any discussions about a similar group being established at the Joint level that would include all the Services and/or key Combatant Commander's representatives?

AF/A3O-C: This is an opportunity that needs further exploration. We have been a member of many working groups addressing specific issues of joint organization and force development. Most of the senior leader stewardship has taken place in "Tank" sessions at the Pentagon as issues arise needing senior-level decisions or guidance.

NSCI: Maj Gen Maluda also commented that his organization is working with the AF Doctrine Center to develop doctrine for cyberspace operations. Given the recent reports of defense networks being under attack, are there any AF activities working tactical level issues such as cyberspace TTPs and/or Lessons Learned?

AF/A3O-C: Our 33 NWS (AFCERT), part of our AF Network Operations Center (AFNOC,) defends AF networks everyday and has built much expertise in this area. We also participate in Net Defense exercises, such as BULWARK DEFENDER to hone tactical Net Defense skills. Also our 23 IOS has the mission of capturing / developing / refining Network Warfare TTPs. The 39 IOS, the Air Force's IO Schoolhouse, has created the Undergraduate Network Warfare Training (UNWT) course providing initial qualification training (IQT) for NW Ops specialists. UNWT incorporates lessons learned into the development of our Air Force network warfare operators.

NSCI: Many have observed that cyberspace solutions at all levels (strategic, operational, and tactical) will benefit greatly from a partnership between government, industry, and academia. Can you tell us about any efforts within the AF to foster this type of collaboration?

AF/A3O-C: The Air Force has sought the expertise and experience of a number of partners. Former Air Force CSAF, Gen Welch, and the Institute for Defense Analyses has been instrumental in shaping the ways we think about cyberspace. On the tactical side, the Air Force Lab at Rome NY is building new cyber operators through their Cyber Boot Camp program bringing in the brightest of our ROTC cadets to learn advanced network operations and cyberspace operations techniques. We have also partnered with industry associations like AFCEA to promote industry solutions to emerging cyberspace requirements.

NSCI: Are there any efforts to include international partners?

AF/A3O-C: I just attended a luncheon at the Estonian Embassy here in Washington DC where we agreed that cooperation with our allies and international partners will be critical to securing our network infrastructures and protecting our commercial as well as national defense interests.

NSCI: Command and control of cyberspace is obviously a critical piece. Can you give us your perspective on what, if anything, makes command and control of cyberspace a little different than the other domains?

AF/A3O-C: The general principles of C2 that guide military ops will continue to guide military ops in cyberspace. However, we do have to address the rapid timescale and range of effects from local/tactical to global/strategic that cyberspace forces can provide.

NSCI: What is the AF doing to ensure it is prepared for uniqueness of cyberspace command and control, while also ensuring cyber operations are integrated with other operations?

AF/A3O-C: The Air Force participates in DOD-wide decision-making to determine appropriate authority levels for approving different types of network warfare and cyberspace operations activities. For example, Net Defense actions that have no effect outside the effected network may be delegated to lower-level commanders, where as other actions may require approval from higher levels commanders. To a large extent, those that try to treat cyberspace as different, special or otherwise stovepipe cyberspace C2 just hinder our ability to integrate with operations in other domains.

NSCI: At one time, there was an AF Command and Control Center focused on C2 requirements, integration, and advocacy. Is there any specific organization working these aspects of cyberspace C2 at this time?

AF/A3O-C: The 505th Command and Control Wing at Hurlburt Field, FL is the AF focal point for integration of all Air Force command and control processes. At the Air Staff level A3/5 is investing more

time/resources in larger C2 issues with the C2 Battle Management Operations Division (AF/A3O-AY). Specifically for cyberspace C2, there is no one organization working it; it's a team effort.

NSCI: It seems there is a lot of work left to do in defining cyberspace C2 arrangements, identifying capability gaps, and building relationships and trust with the various organizations that will be involved. Can you tell us about any efforts within the AF to experiment with and/or exercise cyberspace operations to flesh some of this out?

AF/A3O-C: Well, since our defenders are engaged on a daily basis they are training in a real-world, real-time environment. Lessons learned are gathered from these actions. But we also conduct NetD exercises. An example we've had a lot of success with is BLACK DEMON. It started out as an AF only, tactical NetD exercise, but has grown into the USSTRATCOM sponsored BULWARK DEFENDER today. We've also begun putting Network Warfare play into exercises at our Warfare Center, like RED FLAG at Nellis AFB, NV

The Air Force encourages combatant commanders to include or expand the participation of network warfare and cyberspace operations in their exercises. It is essential that our warfighters have practical experience integrating all aspects of military force, including cyberspace operations, and combined exercises is one of the best ways of practicing joint operations that integrate cyberspace operations with operations in the other domains.

NSCI: Is there anything else you would like to add?

AF/A3O-C: Thank you for the opportunity to inform your readers of our services dedication to our nation's cyber defense.