CyberPro

March 9, 2009

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: BRIG. GEN. (S) DASH JAMIESON

NSCI's Lindsay Trimble recently interviewed Brigadier General (select) Dash Jamieson, director, ISR Strategy, Integration and Doctrine (HAF/A2D), Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance, Headquarters U.S. Air Force, Pentagon, Washington, D.C. A2D is responsible for developing and promulgating AF ISR strategy and plans, guiding Air Force mid- and long-range ISR capability and requirements, leading end-to-end ISR capability portfolio management, formulating Air Force ISR doctrine and managing policy guidance concerning readiness, education, training and career field development for Total Force ISR personnel.

NSCI: Advancements in cyberspace technology have improved the ability of ISR assets to provide actionable intelligence to commanders and fielded forces. How have those advances in cyberspace increased the vulnerabilities of ISR operations, and what is being done to ensure continued network and information assurance as related to ISR operations?

BRIG. GEN. (S) DASH JAMIESON: We are at the tip of exploding cyberspace capability. As such, they will increase our strengths to shorten the kill chain and provide decision superiority to the warfighter. Our Air Force Network Operations Center does a phenomenal job defending our networks every day to ensure we have continued access to conduct ISR operations.

NSCI: The armed forces have made significant advances in shortening the "kill chain" from finding a target to taking action against it. How has cyberspace impacted the tightening of the kill-chain, specifically find, fix, track and assess?

JAMIESON: Although the kill chain is shortened once we find a target, it takes a lot of time, effort and manpower to find targets through ISR operations. Cyberspace is simply another domain where we can operate, find and track targets. When you are able to conduct ISR operations across multiple domains – such as Air, Space and Cyberspace – you receive the benefit of having multiple avenues to find and/or assess targets which can reduce time in the kill chain.

NSCI: Can you tell us about any efforts underway to improve the targeting process and/or tools to address cyberspace challenges such as interagency coordination and collaboration and time constraints?

JAMIESON: We continue to look at ways to improve our processes – especially if it will save us time or money or if it will provide better capabilities to our warfighters. For example, Air Combat Command, at the request of Lt. Gen. David Deptula, the AF deputy chief of staff for ISR, has created an Air Force Targeting Center building upon the Combat Targeting and Intelligence Group. This center will update processes and tools for kinetic targeting to fully integrate non-kinetic options to include cyber. This development will enhance target planning within the Air Operation Centers by providing fully-integrated and deconflicted targeting options to achieve the Joint Force Commander's desired effect.

NSCI: In the past, databases such as MIDB have supported the targeting portion of the kill-chain with order of battle information. Are there any efforts underway to define and capture cyberspace enemy/friendly order of battle information (e.g. electronic warfare, computer networks)?

JAMIESON: The Air Force operates across Air, Space and Cyberspace and as such, addressing what our adversaries can bring to bear against us in those domains is critical to understanding the operating environment. There is currently an effort underway to develop such a database as part of MIDB. It is still in early development, but the goal is to provide data to support traditional kinetic and non-kinetic planning and targeting.

NSCI: Title 50 and Title 10 obviously provide key authorities. Can you tell us how you view these as enabling or inhibiting cyberspace operations?

JAMIESON: Title 50 is an important enabler for cyberspace operations, and – by its very nature – also inhibits operations in order to protect the rights of US citizens through infrastructure and procedures that provide oversight, deconfliction and decision-making authority to non-military and military leaders.

Title 10 is how our nation authorizes and organizes for warfighting operations. Title 50 authorities allow us to provide decision superiority to our Title 10 warfighters, while protecting the rights of our own citizens. The future for cyber will require a review of these titles and may lead to a blending of the two when operating in cyberspace.

NSCI: There are cyberspace challenges that seem to have significant similarity with ISR, such as "ownership" of the assets and associate personnel, acquisition authorities and command and control of the capabilities. Do you have any thoughts on how these challenges could or should be addressed as they relate to cyberspace operations?

JAMIESON: One team, one fight. We need to remember that cyberspace is a domain and is not about "ownership." It is about "partnership" to accomplish the mission. Integration of capabilities, especially ISR capabilities, from, to and through all domains will help create desired effects. We must always look for seams where we can integrate operations, not only in the Air Force, but with the other Services as well. At the same time, it is necessary to have clear chains of command so we can present our forces to the combatant commander when called upon to execute missions.

NSCI: This past October, the AF Chief of Staff announced that instead of an Air Force Cyber Command, cyberspace warfighting operations would be managed by a new numbered AF, 24th Air Force. What is the role of your organization in assisting the Services with improving their ISR-related organize, train and equip capabilities in support of cyberspace operations?

JAMIESON: A2D is focused on AF ISR future organization and capabilities. We ensure that our Air Force ISR doctrine reflects best practices to guide our ISR Strategy. We then use this strategy as our guide for resourcing future capabilities through our ISR Flight Plan which seeks to match the Combatant Commander's needs and short falls to potential solutions. A2D also handles ISR force management issues, so we also work to ensure our forces are properly trained and developed to deliver effects for our commanders.

NSCI: Industry currently offers various courses and certifications related to ethical hacking and computer forensics. Does the ISR community leverage this kind of industry-provided cyberspace training? Are there other areas where you believe industry can help the ISR community address cyberspace challenges?

JAMIESON: Partnering with industry for training gives us great diversity and affords us a different perspective. I believe that if industry can help us deliver effects in the cyberspace domain, whether through training more accomplished operators or through technical solutions that can provide more capability to the warfighter, they are on the right track.

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

JAMIESON: Thank you for the opportunity to provide my insights to your readers.