CyberPro

December 15, 2008

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE

NSCI: What are the current organizational arrangements regarding Army cyber forces, USSTRATCOM, and the Regional Combatant Commanders?

CIO / G-6: The Army defines cyberspace as the global domain consisting of information networks and technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Overall authority for the protection of DoD networks lies with U.S. Strategic Command; however, the Army's Global Network Operations and Security Center (A-GNOSC) in coordination with the respective TNOSCs execute continuous network defense operations of the Army network.

As the Army's global eyes and ears in cyberspace, the A-GNOSC, in coordination with Army Computer Emergency Response Teams, actively monitors and defends Army networks on a 24 hour a day each calendar day. The Army also provides each combatant command cyber-related support down to the tactical level as part of the overall DoD cyber operations structure.

NSCI: Can you give us an overview of any Joint initiatives the Army is working with USSTRATCOM and/or RCCs?

CIO / G-6: The Army is working with USSTRATCOM to develop a trained joint force capable of accomplishing the cyberspace missions outlined in Unified Command Plan (UCP) 2006. As such, USSTRATCOM, together with the DoD and other agencies, has identified a core of 19 cyber skill sets. The next step is to identify the proper manning mix and related training requirements.

NSCI: How does the Army address training and equipping cyber forces?

CIO / G-6: The Army is actively enhancing its network defense capabilities, upgrading technology, such as intrusion detection systems, improving information assurance and adding training for the Soldiers and civilians who use the network. To keep the Army on the cutting edge, the CIO/G-6, the Army Combined Arms Center and the Army Capabilities Integration Center are co-chairing an Integrated Capabilities Development Team to develop new concepts, requirements and solutions for cyberspace operations.

NSCI: What do you see as the most pressing cyber-related threats to Army operations in the next few years?

CIO / G-6: Cyber intrusions and attacks are a real and continuous threat to national security. The United States' adversaries actively target both our information systems and our information infrastructure, hoping to exploit, disrupt or destroy networks. The Army specifically faces a dangerous combination of known and unknown vulnerabilities complicated by limited cyberspace situational awareness.

NSCI: What are your primary cyber-related goals for 2009?

CIO / G-6: The Army CIO/G6 Cyber Directorate Goals for 2009 are:

- Enhance the Army's Information Assurance posture through extensive knowledge sharing, collaboration, compliance standardization and situational awareness
- Establish a CIO/G6 Cyber directorate capable of providing oversight to all CIO/G6 Cyber initiatives
- Facilitate the capability to develop and track the Army's Cyber Warriors by close collaboration with TRADOC, FORSCOM, SIGCEN and HRC
- Facilitate the development of Cyber Operations across the Army by actively participating in the QDR/QRM process and by enhanced integration and collaboration with DA Staff, Joint Staff, OSD, other services, and agencies
- Facilitate standardized IT products and processes across HQDA

NSCI: What are some of your priorities in the area of cyber-warfare and computer network defense?

CIO / G-6: The Army is committed to providing the Warfighter with a secure information environment resistant to known and emerging cyber threats. As such, the CIO/G6 is dedicated to defending LandWarNet, the Army's portion of the global information grid, in order to enable effects-based operations to support the Warfighter and enable decision dominance.