

Science fiction approaches reality

First warrant officer cyber defense experts complete training program

By CW5 Todd M. Boudreau

The Army has taken a bold step toward protecting an expansive and continually threatened frontier by graduating its first class of cyber defense experts.

The gap between science fiction and current cyber space operations has become much smaller. For example, the Star Trek communicator is realized in today's mobile smart phones; flip-top and all. The Star Trek universal translator has also been realized in the U.S. Army's TRANSTAC (Spoken Language Communication and Translation System for Tactical Use); though it only focuses on common Iraqi Arabic - English translation.

The Star Trek electronic clipboards used by LT Uhura are closely proximate in such devices as the iPad. Even the Star Trek holodeck, a simulated reality room used to recreate objects and people, is becoming a reality in agencies such as the Joint Training Counter-IED Operations Integration Center where researchers are working on virtual reality rooms.

However, reality does not follow the script where all of the high tech devices assure the good-guys succeed. In real life, adversarial attacks remain unpredictable and unwilling to ensure we maintain the upper hand in cyberspace. Our adversaries continuously demonstrate that they intend to degrade, disrupt, deny and destroy the advantages our Armed Forces have through the use of high technology systems. In real life, cyber attacks result in any one or more of a variety of threats to include: (1) denial of service attacks, (2) communications networks penetration, (3) manipulation to communications networks routing, (4) information exploitation, and, maybe the most dangerous, (5) information manipulation.

As the Department of Defense continues to adjust its policies and procedures to shape the future cyberspace environment and combat these threats, the Army continues to adjust its doctrine, organizations, and personnel to meet its capability requirements.

On 29 October 2010 the U.S. Army Signal Center of Excellence and Fort Gordon graduated the first class of warrant officer cyber defense experts. Each graduate was reclassified to Military Occupational Specialty 255S to ensure the Army's ability to: (1) track these highly trained experts, (2) prevent the loss of their highly perishable skills, (3) provide an enduring cradle-to-grave career path, and (4) meet doctrinal/organizational positional requirements.

This first class of cyber experts is unique in that several will remain at Fort Gordon and continue working

toward the requirements to be SANS Institute instructor qualified. The SIGCoE considers this necessary to allow the Army to conduct its own training, yet leverage the educational and training power of SANS Institute, a leading organization in computer security training.

Other graduates will go on to work in support of U. S. Cyber Command, Army Cyber Command, Forces Command, Army Theater Network Operations Centers, and Theater Computer Emergency Response Teams. Misinformation has caused some to believe that MOS 255S will address Information Assurance compliancy issues.

This is totally inaccurate. MOS 255S will create the first focused capability to hunt for plausible threat vectors and evidence of adversarial activity in our networks. These Soldiers will coordinate with the Intelligence Community to gain the most up-to-date classified adversarial tactics, techniques, and procedures and to coordinate for appropriate level Computer Network Defense Response Actions. The Army has invested quite a lot in the 255S training, and thus will endeavor to ensure they are situated and focused on that which will get us the greatest return.

MOS 255S applicants must have demonstrated cyberspace operations proficiency as a senior W2 from the Signal Regiment's two other warrant officer MOSs; meaning the nominal applicant has 10-12 years enlisted experience and another 5-7 years experience as a warrant officer. Due to the classification of much of the instruction, applicants must also hold a valid Top Secret security clearance. The applicant must also have a demonstrated aptitude for the training by successfully passing the Certified Information Systems Security Professional certification exam (an industry led global standard demonstrating an understanding of security domains) and the Global Information Assurance Certification Security Essentials Certification exam (a SANS Institute hands-on training/certification that is more practically oriented) prior to selection.

Two classes are scheduled for 2011 and a third class in calendar year 2012. These classes are pilot courses and will train up to a total of 20 warrant officers each consisting of Active Army, National Guard, and Army Reserve students. Formal classes begin on or about 1 October 2012. It is currently estimated that all three components (USA, ARNG, USAR) will grow over 100 255S each. As it will take time to grow to these numbers, the Signal Regiment is developing a strategy to assign these cyber defense specialists to the right units at the right time.

CW5 Todd M. Boudreau is the U.S. Army Signal Regimental Chief Warrant Officer. 