Training With Industry

Continuing Education for cyberspace professionals

By CW4 Scott Broten

This article focuses on some of the efforts that U. S. Air Force educators and trainers are taking to develop their cyber force and how Army personnel, can benefit from their education programs.

Leaders throughout the Department of Defense have made the development of a dominant cyberspace workforce a top priority.

Across all branches of the U.S. Armed Forces a competent cyber savvy force is critical in defending our nation against cyber attacks and exploitation from state and non-state actors who seek to do harm against our defense and financial networks, as well as our infrastructure.

Background

The USAF has developed two Cyberspace focused courses to aid in the development and education of their Cyberspace workforce. The courses, the Cyber 200 and Cyber 300, are run by the USAF Center for Cyber Research which is part of the Air Force Institute of Technology located at Wright-Patterson Air Force Base in Dayton, Ohio. The development of these courses covered a period of several years prior meeting Initial Operational Capability in 2010. To further add to the benefit of these two courses, AFIT pursued joint certification and the Army formally recognized the certification in 2011.

The best definition or summary for both of these courses comes from AFIT's Cyberspace Professional Continuing Education Catalog: "Cyberspace 200 Professional Continuing Education course is presented at the classified level for the deliberate development of cyberspace professionals at the six to eight year point of their careers."

This course is covered in two phases. Phase one is Advanced Distributed Learning and Phase Two is a three-week resident phase. The students of Cyber 200 are educated in subjects to include cyber system acquisition, capabilities, limitations and vulnerabilities to help them plan, direct and execute defensive and offensive cyberspace operations. Completion of the Cyber 200 awards 2.0 points towards joint qualified officers.

"Cyberspace 300 Professional Continuing Education course is presented at the classified level for the deliberate development of Cyberspace professionals in the second half of their careers."

(Continued on page 36)

LTC John Bommer, instructs students in the Cyber 300 course at the Air Force Institute of Technology.

(Continued from page 35)

This course is also conducted in two phases. Phase one is ADL and Phase Two is a two-week resident phase. The students of Cyber 300 are educated in subjects to develop strategic focus for the integration and application of cyberspace capabilities in a joint environment. Completion of the Cyber 300 awards 1.5 points towards JFOs.

The graphic at right (See Figure 1) is the current USAF cyberspace professional development approach that depicts where the Cyber 200 and 300 courses fit.

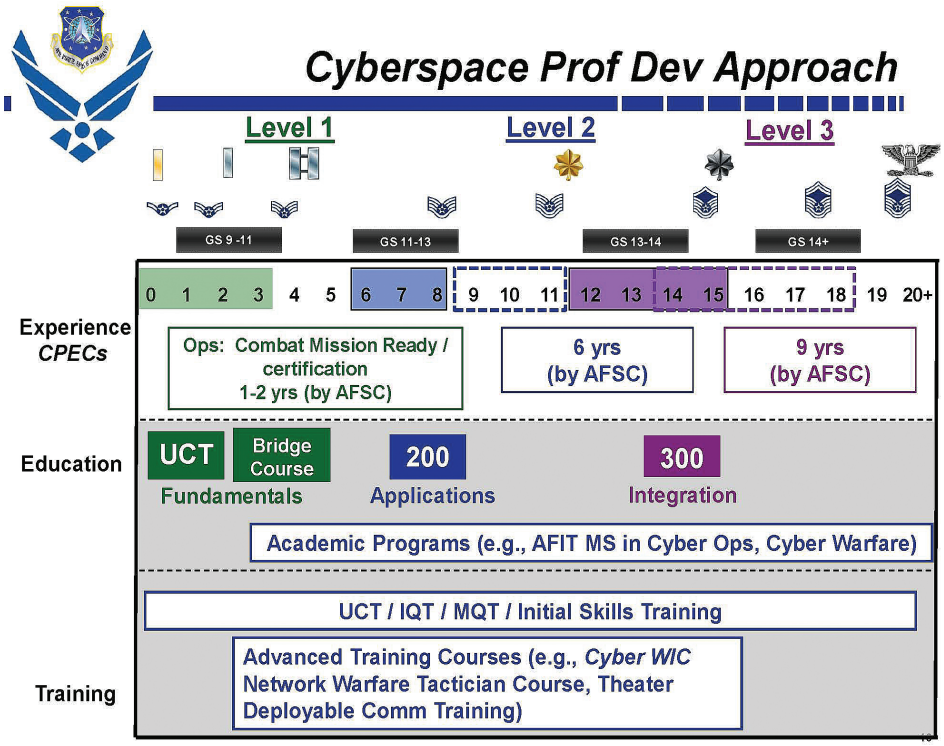

Figure 1: U.S. Air Force Cyberspace Professional Development Approach and Model

Prerequisites

Army officers and NCOs are eligible to attend the Cyber 200 and 300. The basic prerequisites must first be met and then those interested officers and NCOs can contact the Office, Chief of Signal at the Signal Center of Excellence and Fort Gordon to request attendance. OCOS coordinated directly with the cadre at AFIT for possible reservations. The primary point of contact at OCOS is Mr. James Busler (e-mail: james-.n.busler.civ@mail.mil).

The qualifying prerequisites to attend either course follows:

Cyber 200 Prerequisites

- U. S. Citizen
- Secret Security Clearance
- O3, W2 with 6-8 years of service, E5/E6 with 9-11 years of service, and GS-11 through GS-13 in cyberspace operations and Acquisition positions
- Minimum of 24 months of cyber experience (includes our Signal experience)

Cyber 300 Prerequisites

- U. S. citizen
- Top Secret/SCI Security Clearance
- O4/O5, W3/W4 with 12-15 years of service, E7/E8 with 9-11 years of service, and GS-13/GS-14 in cyberspace operations and acquisition positions
- Minimum of 72 months of cyber experience (includes our Signal experience)

My Experience at Cyber 300

I recently had the privilege to attend the Cyber 300 course. Phase one (the ADL phase) began in January and spanned a period of several weeks. The ADL served as mental preparation to attend the resident phase, which I attended from 4-15 March 2013. The ADL requirements are ideal and in no way interfered with the demanding day to day functions we normally have at home station. Requirements consisted of student introductions, a myriad of cyber related readings, topic selection for an information/research paper, and submission of the paper abstract and outline. For those that enjoy reading, the ADL documents ranged from USAF cyberspace operations to joint, interagency, intergovernmental, and multinational subjects.

First impressions are critical and from the first day of the course it was evident that the Cy-

ber 300 is professional continuing education at its best. Led by Dr. Harold J. Arata III and LTC John Bommer, the cadre at AFIT consists of USAF cyber professionals that come from a wide range of backgrounds. Those backgrounds provide relevant, real world experiences and perspectives on cyberspace operations in the DoD. I also found the inprocessing and subsequent administrative activities smooth and easy thanks to AFIT's Ms Jane White.

Over the course of two weeks, students are provided unclassified and classified (up to top secret/SCI classes and briefings. Under the current curriculum, some topics of note were "why cyber," network operations as it pertains to cyberspace operations, supervisory control and data acquisition, cyber intelligence, surveillance and reconnaissance, and cyberspace doctrine. The course also provides a great opportunity for briefings from guest speakers from agencies such as the National Security Agency. My course was able to have an interactive brief with MG Earl Matthews, director of Cyber Operations from the Chief Information Officer, A6 of the Air Force Staff.

The Cyber 300 offers a great deal of interaction between student and instructor/briefer. The interaction, along with the course content provides an outstanding "big picture" view on cyberspace operations that most of us do not have. To enhance the exchanging of information, opinions and ideas students, the Cyber 300 requires students to complete a research paper on a selected topic and then provide a brief to the class on their position. I personally found the interaction throughout the course to be enlightening and I no longer view cyberspace the way I viewed it prior to attending.

The education being provided at AFIT is a tremendous asset to the DoD. The content is relevant to the Army and if able to attend, the student will find that the course is joint focused yet a feel for the Air Force perspective on cyberspace operations is also provided. Cyberspace operations is joint in nature and our nation will only be completely secure by working together and sharing best practices for educating all our forces.

Our Army and Signaleers can greatly benefit from attending and leaders of the Signal Center of Excellence obviously understand and support this. Efforts are under way to assign a chief warrant officer four, 255S Information Protection technician to AFIT to be an instructor for the Cyber 200 and 300 courses.

In the end, this joint effort will enable the Army to send more personnel to these courses to improve our education and understanding as well as bring a bit of an Army perspective to the USAF Cyberspace Professional Continuing Education.

If you have an opportunity to attend either course, go!

CW4 Scott Broten *is the Signal warrant officer personnel developer at the U.S. Army Signal Center of Excellence and Fort Gordon. CW4 Broten enlisted in the Army in 1992 and served with the 7th and 11th Signal Brigades before becoming a warrant officer in 1998. His warrant officer assignments include the Southern European Task Force, 35th Signal Brigade (Airborne), 52nd Signal Battalion, 1st Cavalry Division, and 1st Corps. CW4 Broten has served in four combat deployments, two in support of Operation Iraqi Freedom and two in support of Operation Enduring Freedom. CW4 Broten has completed all levels of warrant officer Professional Military Education and holds a Bachelor's Degree in Information Technology.*

Acronym QuickScan

ADL - Advanced Distance Learning
AFIT - Air Force Institute of Technology
DoD - Department of Defense
JFO - Joint Qualified Officer
JIIM - Joint Interagency Intergovernmental Multinational
NCO - Non-Commissioned Officer
NSA - National Security Agency
OCOS - Office Chief of Signal
SCADA - Supervisory Control and Data Acquisition
USAF - United States Air Force