ARIOC SOLDIERS PARTICIPATE IN INFORMATION ASSURANCE TRAINING

ARMY RESERVE MAGAZINE, FALL 2004 (VOL. 50, NO. 2)

In future conflicts, winning the battle in cyberspace could become as important as winning the war on land, sea and in the air. Potential enemies know that, if they can disable a military force's networks, they could seriously degrade that force's war fighting capability.

Soldiers in the Army's five regional Information Operations Centers (IOCs), which are staffed entirely by Army Reserve Soldiers and represent "units of action" of the Army Reserve Information Operations Command (ARIOC), are responsible for maintaining an information assurance capability for the entire Army. They work in cooperation with other Army organizations, such as the network of Regional Computer Emergency Response Teams (RCERTs) that span the globe. Their role includes detecting, evaluating and ultimately neutralizing cyber threats that could affect the mission of the Army and its supported agencies, such as the National Security Agency and Joint Reserve Intelligence Program.

In order to be able to counter any developing global threat, it became clear early in 2003 that an ambitious program would have to be developed very quickly to train ARIOC Soldiers in information assurance techniques. With U.S. Senator Rick Santorum's (R-PA) support, $1.5 million in federal funds was secured to establish a partnership between Carnegie Mellon University's Software Engineering Institute (SEI), located in Pittsburgh, Pennsylvania, and the ARIOC to meet the Army's need for a force trained in network security.

The SEI has developed several initiatives to help improve the quality of industrially developed software, as well as to ensure the integrity of information systems. Its program consists of four separate training activities: 1) a Basic Course in network technology; 2) an Advanced Course, which provides a hands-on laboratory in network redesign; 3) a virtual network auditing (VNA) activity to allow the IOCs to use virtual private network encryption technology to conduct remote vulnerability assessments and information security audits of simulated Army production networks; and 4) an information assurance exercise (IAX), in which all of the technologies taught can be tested in as close to a hostile cyber battlefield as can be created.

The SEI has developed several initiatives to help improve the quality of industrially developed software, as well as to ensure the integrity of information systems.

The IAX is implemented as a simulation in which the IOCs build computer networks to support a deployed force and then must defend those networks against a Red Team — a group of ARIOC "aggressors" assigned the task of attempting to penetrate the networked systems.

The first two activities already have taken place. One feature of the training was that it was taught in a "train-the-trainer" context to prepare the participants to present the same training to others back at their home units. The individual IOCs now are engaged in implementing such follow-on course offerings locally using the SEI-trained Soldiers as primary instructors. At the same time, the SEI is developing the VNA and IAX training activities, scheduled for deployment in late 2004.

As the Army moves into the next millennium, cyber terror may figure more prominently in deciding the outcome of the nation's wars. The successful implementation of this cooperative training program will ensure that the Army is equipped to defeat this new kind of enemy.