



SENIOR LEADER PERSPECTIVE:

GENERAL ROGER A. BRADY

NSCI's Lindsay Trimble recently interviewed General Roger A. Brady, commander, U.S. Air Forces in Europe; commander, Air Component Command, Ramstein Air Base, Germany; and director, Joint Air Power Competency Center, Ramstein AB. He has responsibility for Air Force activities in a theater spanning three continents, covering more than 20 million square miles, 92 countries and territories, and possessing one-fourth of the world's population and about one-third of the world's Gross Domestic Product.



NSCI: What is USAFE's relationship to other Department of Defense organizations supporting cyberspace operations?

GEN. ROGER BRADY: The cyberspace domain dictates that a myriad of organizations integrate laterally and vertically to meet the common goal of protecting our cyberspace domain. Within this paradigm, USAFE is responsible for ensuring the security and integrity of our portion of the Net.

NSCI: You became USAFE commander at the beginning of last year. Have there been any specific cyber successes since then that you'd like to highlight?

BRADY: Yes, since I became the USAFE commander, we have had several key cyber successes in the MAJCOM. One significant cyber success has been our deployment of the Host Based Security System (HBSS). The HBSS is a suite of integrated applications providing intrusion prevention, intrusion detection and firewall capabilities. The HBSS suite may be installed on any network client, with configuration and management of the HBSS suite occurring at a centralized location. Our particular HBSS implementation encompassed the entire USAFE NIPRNet, with more than 30,000 workstations and servers receiving the HBSS suite. This initiative dramatically improved the security of our networks, establishing a new level of situational awareness and threat mitigation.

Another recent cyber success that I am proud of was our USAFE Information Assurance (IA) campaign. This IA campaign was an aggressive 14-week focused effort on raising the awareness of network users and preparing them to better defend cyberspace. The campaign included Armed Forces Network commercials and radio spots, base newspaper articles and structured exercises such as phishing scenarios. The effectiveness of the campaign was illustrated by the requests from other agencies during the May 09 Security Solutions Conference for our IA products.

NSCI: From a USAFE perspective, can you discuss a few of the key challenges regarding cyberspace operations?



Keeping Cyberspace Professionals Informed

BRADY: Since the cyber domain is a very dynamic environment, we need to ensure that we are postured correctly to defend this domain much like other operational domains such as air and space. The right people with the right skills, tools and leadership need to be aligned logically to respond to cyber threats quickly and decisively. With the inception of our newest Numbered Air Force, this concept has become a reality, and we have a critical part of that mission in USAFE. It is critical for all MAJCOMs, not just USAFE, to work side by side to ensure that the mission of the new Cyber NAF, 24th Air Force, is accomplished every day.

NSCI: You are also the commander of the NATO Allied Air Component Command. Does this include any cyber collaboration with NATO similar to the Air Force mission (e.g. air, space and cyberspace)? If not, who is responsible for coordinating cyber issues with NATO?

BRADY: The Cooperative Cyber Defense Center of Excellence (CCD CoE) was formally established May 14, 2008, in order to enhance NATO's cyber defense capability. Located in Tallinn, Estonia, the Center is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic and Spain as sponsoring nations. The United States has already stated our intent to join this organization and we are in the process of coordinating this effort. We fully support the cyber collaborative effort by providing insight, subject matter expertise and assistance to NATO on various aspects of cyber defense.

NSCI: Does the Joint Air Power Competence Centre include any cyber roles / responsibilities?

BRADY: The Joint Air Power Competence Centre's (JAPCC) current role, in the cyber world, is working with the national and NATO authorities on the cyber implications to air and space. JAPCC's efforts occur at the operations and strategic level as it relates to our program of work. Its role is to look further into the future to frame the challenges and prepare how we might address them as an alliance.

NSCI: Are you planning any cyber-related organizational changes within USAFE as a result of the recent decisions to stand-up a cyber NAF within the Air Force and a Sub-Unified Command for cyber under USSTRATCOM?

BRADY: There are no organizational changes within USAFE that are the direct result of the Cyber NAF; however, we were already looking at streamlining processes and using more reachback support to meet Program Budget Decision (PBD) 720 requirements. Units that will provide that reachback capability will be aligned under the new Cyber NAF, 24th AF. Our current framework is in-line with the aforementioned organizational changes.

NSCI: Since you took command, have there been any USAFE exercises that focused on cyberspace capabilities or were adjusted to include that aspect? Can you discuss any upcoming exercises or training activities that USAFE has planned in 2009 that aim to improve cyberspace capabilities?

BRADY: There have been no specific USAFE exercises that focused on cyber, but it has become an integral part of our exercises. Austere Challenge 2009 was a EUCOM exercise to certify its components as a Joint Task Force. During this exercise, there was heavy cyber involvement. Each component under EUCOM created a cyber playbook that furthered our efforts to standardize theater tactics, techniques



and procedures (TTP) related to Cyber Network Defense, ultimately improving command and control relationships and ensuring and maintaining cyber network readiness.

The Cyber Playbook is a three-tiered approach to providing Cyber Network Defense.

- Tier 1 (top tier) requires TTPs at the enterprise level that are aimed at synchronizing information flow and actions from external organizations through the COCOM and out to the components
- Tier 2 (middle tier) is focused on specific actions required on the networks to prevent cyber events and react to indications and warnings of cyber events that occur
- Tier 3 (bottom tier) focuses on how division, sections and individuals will work in a diminished cyber environment

NSCI: What kinds of opportunities do you see for interaction with industry partners in training for cyber defense and offense? Are these partnerships influenced or changed by USAFE's position in the European and African theaters?

BRADY: USAFE's current focus is on our internal training via the DoD 8570 initiative. The DoD 8570 initiative is designed to train our U.S. Armed Forces in specific cyber operation core competencies. With respect to USAFE, the DoD 8570 effort has incorporated industry partners to provide instructor-led classes and hands-on training to our cyber forces. This training has led USAFE to meet its goals of certifying personnel in A+, Security+ and CISSP. Once USAFE has met our internal DoD 8570 goals, we will look at future training opportunities and exercises with industry partners.

NSCI: What have cyber operations in support of USAFRICOM looked like so far? What do you think they will entail in the future?

BRADY: Presently, both the cyber operations supporting USAFRICOM air component forces and the cyber operations supporting USAFE forces have been very similar. This similarity is primarily due to the U.S. Air Force's effort to centrally manage all network users and resources (AFNetOps) by consolidating many U.S. Air Force network systems and services. This initiative has allowed USAFE to standardize or "template" our cyber operations, giving both our end-users and cyber operators the same cyber environment, regardless of their physical or geographic location. Hence, all aspects of cyber operations, including offense, defense and support, can be managed in the same fashion.

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

BRADY: Cyberspace is absolutely critical to our operations. We do not operate without it and every individual must be aware of the responsibility to ensure we can operate in this critical domain.