



Over the last several months, I've addressed the information operations evolution and how it will impact this Agency's future.

I've focused on both the historical role and current prominence and significance of the Gain and Exploit pieces of our information operations.

This month I will highlight a third piece of information operations that is vital to our information superiority core competency—information

defend. A key Air Force goal in mastering information warfare is to "render AF information and its functions, including weapon systems, secure in war and peace."

Related to this goal is the recognition that "we cannot hope to dominate warfare without possessing trustworthy information functions." The exponential growth of our C4 requirements has led us to depend on commercial providers and maintainers, facilitating global reach but hindering global protection. The threat to our information security is real, but AIA is at the forefront of making "information defend" a cornerstone of military operations.

Historically, this Agency has had a significant role in raising the awareness of field commanders to communications security issues.

Over the last 30 years, our Electronic Systems Security Assessment professionals have done a tremendous job, providing commanders a snapshot of unit communications security by conducting telephone and radio monitoring. Modern AF communications technology has resulted in the need to expand monitoring services to include faxes, E-mails, pagers and cellular phones.

To meet this challenge in an era of declining budgets, we are consolidating ESSA operations into three regional locations—Europe, the Pacific, and CONUS—while embedding ESSA personnel into the information operations detachments at the Numbered Air Forces.

As a result, we are providing efficient, yet tailored support through more centralized monitoring, analysis, and reporting. Air Force commanders have come to depend on ESSA services. In fact, Air Force Special Operations Command leadership considers this program a "must have" to effectively accomplish the vital AFSOC mission.

Today, most Air Force day-to-day missions depend on computers and the vast amount of information computers process. While a large portion of our work is accomplished on secure computer networks, the majority of Air Force systems—to include operational and logistical—are unclassified and not protected by encryption techniques and secure facilities.

This "window of vulnerability" is being aggressively addressed by the Air Force Information Warfare Center. The AFIWC manages the Air Force's Computer Security Assistance Program which focuses on ensuring AF C4 systems are protected and available for optimum use by operational forces. AFIWC operations conducted by the AF Computer Emergency Response Team have yielded superb results. Their efforts to raise the awareness of Air Force Commands on anti-

virus measures played a key role in a reduction of man-hours lost due to computer downtime from 7,950 in 1996 to 1,100 in 1997.

AFCERT uses on-line surveys to verify implementation of countermeasures for common vulnerabilities and continues to pinpoint weaknesses in Air Force systems.

With 113 Automated Security Incident Measurements systems (ASIMs) to monitor base unclassified networks for suspicious or unauthorized activities in 1997, the AFCERT was able to detect and validate 84 such incidents—events that could potentially cause a serious impact to AF operations.

The AFIWC success in meeting computer security challenges has not gone unnoticed in the Department of Defense. Recognizing the AFIWC as the corporate knowledge base for information assurance operations, several other Air Force and Department of Defense organizations are joining the fight. PACAF is leading the way, having established the first AF Regional Information Protect Center.

This center, modeled after and developed with AFCERT expertise, gives the Pacific Commander a localized capability to detect and take preventative measures against intrusions into his information infrastructure.

All AF MAJCOMS are directly working with the AFCERT to build similar information protect centers. The combination of localized protection centers with AFCERT operations will ensure we can detect and respond to intrusions across a broad spectrum of activities, from actions by curious hackers to full-scale structured attacks by adversaries as part of a military campaign.

With the assistance of AFCERT personnel, STRATCOM successfully established the first joint information protection center. The AFIWC is working in concert with the Defense Information System Agency to proliferate AFCERT procedures and tools at the joint level.

Given the fact that we will fight under joint commands, we must work hard to integrate our successful capabilities into joint information protection programs. This includes challenging their protection capabilities during exercises by executing adversary attack capabilities, or Red Teaming.

Both AFIWC and the Joint Command and Control Warfare Center red team efforts raise vulnerability awareness in a wartime planning and execution environment, and are playing a key role in the development of a Department of Defense red team concept of operations. Defensive information warfare efforts are one of our biggest challenges in our pursuit of information superiority.

Historically, we have been effectively engaged. Our embrace of the revolution in information technologies has placed our agency at the forefront of the Defend piece of information operations. Our IO programs are comprehensive and will play an increasingly vital role in ensuring we maintain the AF core competency of information superiority.

I salute the challenging work our AIA personnel are doing in the diverse information defend arena and encourage you to take a look at a recent video we produced: *Information Operations: A New Dimension in Warfare For The 21st Century*. The video describes all four pieces of information operations—gain, exploit, defend and attack. ■

*James E. Mills*