By Lt. Gen. Harry D. Raduege Jr., USAF (Ret.)

Future Defense Department Cybersecurity Builds on the Past

Cybersecurity is becoming a critical issue for both government and industry—and for good reason. A dangerous combination of cyber-related activity is growing daily around us. This includes dependence on technology, skyrocketing cyber crime and terrorism, and vulnerabilities hidden by the complexities of an interconnected, global network. In government, industry and our personal lives, we have growing cyber dependence because that is how we are able to better perform missions, conduct business operations and lead our daily lives.

But there is a flip side. Cyber criminals are profiting by compromising personal identities and financial information and selling this information to the underground market. Cyber terrorism also is a concern because the same technologies used in industry can be leveraged easily for disruptive purposes, including vandalism, fraud and espionage. With increasing demands for sharing information and rapid collaboration any time anywhere, we are becoming more vulnerable to cyberattacks from a variety of bad actors.

In the past, U.S. Defense Department information networks were strictly controlled. We remember the outstanding security found throughout defense networks such as the Automatic Digital Network (AUTODIN), the Automatic Voice Network (AUTOVON) and the Automatic Secure Voice Network (AUTOSEVOCOM). Those were the days of closed networks in which daily security concerns were oriented more toward physical security rather than cyberspace.

However, over the past 20 years, significant changes have emerged in networks and capabilities. These changes have postured the Defense Department for success in this new world of threats and interdependence.

With establishment of the U.S. Space Command (SPACECOM) in 1985, Gen. Robert Herres, USAF, prophetically recognized that "space is electrons." These profound words marked some of the earliest understanding of the linkages among electrons, information technology (IT), global information networks, space operations, information management (IM) and cyberspace. Another significant recognition came with the Information Technology Management Reform Act of 1996. This landmark legislation, also known as the Clinger-Cohen Act, enacted legislation describing the importance of IT, IM and the requirement to appoint chief information officers (CIOs) responsible for information-related activity throughout the federal government.

The importance of IT, information networks and CIOs as critical infrastructure elements within the Defense Department was recognized in the late 1990s after several events highlighted the vulnerabilities of defense networks. In 1998, then Secretary of Defense William Cohen and his deputy, Dr. John Hamre, asked which commander in chief was responsible for securing department networks. Following many senior-level meetings, in December 1998 a SPACECOM Joint Task Force (JTF) for Computer Network Defense (CND) with assigned commander and minimal forces was co-located with the Defense Information Systems Agency (DISA) in Arlington, Virginia. With added missions in April 2001, the JTF-CND became the JTF for Computer Network Operations (JTF-CNO) and, in October 2002, with the disestablishment of SPACECOM, the JTF-CNO was realigned under the U.S. Strategic Command (STRATCOM).

These activities laid the groundwork for what came next—and not a moment too soon. In February 2003, cybersecurity gained national attention when the White House published the National Strategy to Secure Cyberspace. At the same time, it also became evident that both operating and defending Defense Department networks needed to be tightly coupled with someone clearly in charge. Following numerous Pentagon "tank" sessions, on July 18, 2004, then Secretary of Defense Donald Rumsfeld appointed a commander, Joint Task Force–Global Network Operations (JTF-GNO), with clear responsibility and authority for ensuring the end-to-end availability and security of defense information networks.

For the first time in network operations and cybersecurity history, command lines were established from the secretary of defense to the STRATCOM commander, to the JTF-GNO commander, to each of the appointed component commanders within the military services and representatives within the combatant commands and defense agencies. This framework provides an important governance model for optimally operating and defending Defense Department networks through an established command structure. It was no accident that the secretary assigned the DISA director additional responsibility as the first JTF-GNO commander. DISA's extensive capabilities form a powerful platform in supporting emerging national-level and Defense Department cybersecurity requirements.

Recently, a special Commission on Cyber Security for the 44th Presidency was established to address national-level concerns in this critical area. This commission is led by the Center for Strategic and International Studies, where Hamre now serves as its president and CEO.

As deputy secretary of defense in 1997, Hamre warned Congress, "We're facing the possibility of an electronic Pearl Harbor." President George W. Bush also has identified cybersecurity as a key focus area, and many others now are placing their oars in cybersecurity waters to influence this emerging critical mission area. These are exciting times, and cybersecurity is only beginning to gain the focus and attention it deserves.

The *SIGNAL* Blog

We welcome your comments on this column at **www. afcea.org/signal/blog**, or e-mail us at **signalnews@ afcea.org**.