May 2003

intercom

Journal of the Air Force
C4 Community

network operations

intercom
May 2003
Volume 44, No. 5

Air Force Chief of Staff
Gen. John P. Jumper

Deputy Chief of Staff for Warfighting Integration
Lt. Gen. Leslie F. Kenne

Deputy Chief of Staff for Air and Space Operations
Lt. Gen. Ronald E. Keys

Deputy Chief of Staff for Installations and Logistics
Lt. Gen. Michael E. Zettler

Director of C4ISR Infostructure DCS for Warfighting Integration
Maj. Gen. Charles E. Croom Jr.

Commander, Air Force Communications Agency
Col. David J. Kovach

Editorial Staff

AFCA Chief of Public Affairs
Lori Manske

Executive Editor
Master Sgt. Karen Petitt

Editor
Tech. Sgt. Jim Verchio

This funded Air Force magazine is an authorized publication for members of the U.S. military services.

Contents of the ***intercom*** are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or the Department of the Air Force.

Editorial content is edited, prepared and provided by the public affairs office of the Air Force Communications Agency.

All photos are U.S. Air Force photos unless otherwise specified. Photo submissions are encouraged in the form of high-resolution digital images or 35 mm prints.

News copy, photos, story ideas and comments may be e-mailed to intercom@scott.af.mil, or mailed to AFCA/PA, ***intercom***, 203 W. Losey St., Room 1200, Scott AFB, IL 62225-5222. Fax is DSN 779-6129 or (618) 229-6129. Editorial staff may be contacted at DSN 779-5690, or (618) 229-5690.

Visit our Web site at:
http://public.afca.scott.af.mil/intercom.htm

4 **'Netspionage'**

Theft of classified and proprietary data over the Internet has become increasingly widespread due to foreign and domestic exploitation of network and information system vulnerabilities.

8 **USAFE NOSC**

What comprises a Network Operations and Security Center and what can it do to maintain network operability and reliability?

12 **AWACs connected**

The aircrews of the E-3 Sentry, Airborne Warning and Control System, have a new communications capability as they continue to fight the Global War on Terrorism.

27 **View of Iraq**

For a combat cameraman from upstate New York, a six-hour ride from Kirkuk to Bashur Airfield in northern Iraq, was an eye-opening experience he will not forget.

This month's cover focuses on network operations.

Cover by Tech. Sgt. George Jumara

AFPCA part of diverse combat support team

By Col. Jed Alexander
Commander, Air Force Pentagon Communications Agency
Washington D.C.

The Air Force Pentagon Communications Agency is in the business of making information technology work. As communications operations professionals, we know this is a daunting task for any of us, and it takes effort and dedication to make it happen.

AFPCA is a Field Operating Agency, with 457 military and 302 civilians plus contractor augmentation. We're proud to be a part of the diverse Installations and Logistics team, which includes an array of combat support activities.

All told, we support more than 15,000 customers spread across these activities and provide a wide range of C4 support from desktops to cell phones and blackberries to specialized C2 systems and deployable communications packages, continuity of operations activities and a wide range of software systems. To put this into perspective, consider what AFPCA accomplished recently – we deployed members of our SECDEF travel team with no notice in support of Operation Iraqi Freedom. The next day, we ran a Defense Red Switch Network "4 Star" secure voice conference for the Air Force Chief of Staff, enabling him to talk to his MAJCOM commanders. At the same time, we supported vital C4 requirements for the Deputy Director for Global Operations in the National Military Command Center. We finalized installation on a data wall in the NMCC to enhance Joint Staff control and reporting responsibilities on current operations and we sat side by side with air and space operators in the Air Force Operations Group operations center ensuring reliable C4 systems around the clock with mirrored support at the alternate operations centers in other classified locations. Finally, we sent communicators to mentor their new Department of Homeland Defense counterparts in deployed communications.

The current emphasis on operations security across the Pentagon is complemented by our team of information assurance specialists defending the network and educating the Air Staff on the importance of information protection through an effective advertising campaign. We also confirmed 100 percent compliance to meet Defense Message System 3.0 requirements and went beyond DMS 3.0 by ensuring all our DMS users were Web enabled to use the Army's sponsored "Decision Agent," which enables DMS sending and receiving without requiring the DMS client or the Fortezza card at the user level.

Meanwhile, we responded to and resolved 450 help desk calls in just one day on our unclassified and classified networks. Separately, we met the C4 needs of our senior leaders with a specialized rapid response team, detecting and resolving C4 problems before they could impact activities. We operate and maintain legacy C4 systems designed in an age when technical orders were a part of the system delivery and cope with the latest in wireless technologies that were designed principally for the commercial market with little technical data or control available to us.

Much has been said about information operations, information superiority, weaponizing C4 systems and transformation. As I write this article, the United States of America along with coalition partners, is engaged in combat operations in Iraq. It is abundantly clear that much has already been done in the integration of C4 systems to generate awesome operational effects. In the echelon of information technology activities underlying our weapons systems, much work remains. Lt. Gen. Michael Zettler has expressed his perspective in the *intercom* on the importance of separating communications operations from the imperative of transforming and integrating comm resources and technologies.

There remain areas of unevenness that make the delivery of highly reliable, fully integrated communications systems a struggle we only accomplish through the efforts of our people. The "man behind the scenes" is likely to be a fast moving communicator or information manager.

I'm proud of the contributions we make to the daily fight, and all of us in AFPCA look forward to the future integrated system improvements we know are coming.

With ever-changing technology 'Netspionage' enters realm of nonfiction

By Maj. Jack Kiesler
Representative to AF/CIO
Air Force Office of Special Investigations
Andrews AFB, Md.

Theft of classified and proprietary data over the Internet has become increasingly widespread due to foreign and domestic exploitation of network and information system vulnerabilities.

An unrestricted, unguarded Internet affords an ideal operating environment for criminals, cyber terrorists and adversarial nations. Skillful exploiters can achieve a degree of plausible deniability and anonymity, and a high return on investment compared to risk. Additionally, they can even find useful tools and techniques of their trade readily available online.

According to a 1997 American Society for Industrial Security survey of Fortune 1000 firms, U.S. companies are believed to have lost roughly $250 billion annually to information thieves. About 56 percent of the 172 companies responding to the survey reported at least one attempted or suspected information misappropriation.

Five years later, a 2002 Computer Crime and Security Survey report revealed 90 percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the previous 12 months and 80 percent acknowledged financial losses due to computer breaches.

As anticipated, the most serious financial losses occurred through theft of proprietary information. Interestingly, 74 percent cited their Internet connection as a frequent point of attack.

In a recent FBI report, U.S. companies revealed that although domestic competitors are engaged in intelligence exploitation of the information domain, there is increased **netspionage** by companies and governments from a number of countries we normally perceive as allies.

"We're seeing more and more cases," said William Perez, acting chief of the FBI's financial crimes unit. "A country like the U.S. is a very juicy target because of the prominence of its high-technology companies," he said. "The Internet arouses the greatest fear because it gives skilled hackers the possibility of entering untold databases with anonymity, often from far-off locations where there are no statutes against computer crime. The criminal element recognizes that international law lags significantly."

It's common to weave attacks through foreign sites in advance of reaching the crown jewels. As law enforcement attempts to resolve the source,

Hackers-for-hire working for foreign nationals are not merely the stuff of James Bond films.

Bill Hancock
Exodus Communications security chief

the investigation often stalls once a foreign ISP is reached – particularly one where no computer crime laws exist.

A well-publicized example of foreign exploitation of U.S. business information occurred in Russia in 1994. A group of Russian hackers stole codes and passwords from corporate customers of Citibank and transferred $10 million to overseas accounts. Six Russians were extradited and pleaded guilty to computer fraud in federal court in New York. Citibank said it recovered all but $400,000. The ability to transfer money from a large banking institution like Citibank serves as a sobering example of the potential vulnerabilities and increasing number of incidents involving even some of the most secure institutions.

Carnegie Mellon University's Computer Emergency Response Center collects data on vulnerabilities and incidents targeting U.S. businesses. Statistics reflect exponential increases.

Further complicating efforts to track the nefarious is employment by foreign entities of go-betweens or hackers-for-hire.

Hackers-for-hire working for foreign nationals are not merely the stuff of James Bond films, according to Exodus Communications security chief Bill Hancock.

He's been chasing a Chinese national for more than seven years who regularly hires U.S. teenagers to hunt down documents. In one case, Hancock said a 17-year-old U.S. hacker was paid $1,000 and promised $10,000 more for stealing design documents for kitchen appliances from U.S. firms.

Hiring hackers-for-hire not only provides foreigners a degree of plausible deniability but also helps stall prosecution, as the go-between is frequently a minor with protection from criminal prosecution.

Four technological factors contribute to the ease of netspionage: increased theft and exploitation of laptops, wireless technologies, spyware and steganography tools.

Theft and exploitation of laptops

Frequently, executives, scientists and corporate financial teams travel with laptops to maximize business efficiencies. In addition to increased productivity and efficiencies, these mobile devices also create additional threats, such as theft and gaining physical access to clone information resident on the laptop. The Computer Security Institute reported that approximately 57 percent of corporations experienced a loss related to laptop theft and an insurance industry estimate states that over 319,000 laptops were stolen in 1999. This is of special concern to executives and to organizations such as the military and law enforcement, where the work force is highly mobile and deals with particularly sensitive information.

A Justice Department internal report revealed that in 1999, the FBI and four other federal law enforcement agencies lost more than 400 of its own laptop computers. This finding reached public attention, particularly since it was discovered that in some cases, the laptops might have contained classified national security information.

That same year, the State Department disclosed that a classified laptop with information about arms control was missing from a conference room. You can imagine the implications should foreign policy strategies, adversary assessments and technical concerns become known to an adversary. The ensuing furor resulted in an FBI investigation and the firing of two high-level diplomats. A subsequent audit of the department's laptops accounted for its remaining 60 classified laptops, but 15 of its 1,913 unclassified laptops were still missing.

Wireless technologies

Wireless local area networks, or WLANs, have become extremely appealing for a number of reasons. You don't have to drop cable to every desktop, and users can connect from just about anywhere within range. WLANs provide always-on network connectivity, while allowing employees to roam throughout a building without being bound by wires.

Further, WLANs are emerging as low-cost, easily-deployable solutions. However, there's a high

cost associated with this capability in terms of increased vulnerability.

Because transmitted data is broadcast using radio waves, any WLAN client within a service area can receive data transmitted to or from the access point. Because radio waves travel through ceilings, floors and walls, transmitted data may reach unintended recipients on different floors, or even outside the building housing the access point. With a WLAN, the boundary for the network has moved. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including the parking lot.

The media recently reported a Massachusetts-based business that drove through the City of London armed with only a laptop, wireless network card and some free software downloaded from the Internet. They discovered they could pick up traffic "leaking" out of buildings from dozens of corporate WLANs, allowing them to grab data without the company's knowledge. A few substantiated reports revealed even an empty potato chip tin can may serve as a wireless antenna or receiver.

Spyware

Spyware is any software that takes information from a system and employs an Internet connection to upload information to a remote server without the user's knowledge or consent.

Unknowingly installed spyware programs can capture online activity; cause Internet browser instability and slowness; consume system resources and cause system errors; and render systems vulnerable to attack or compromise.

Spyware includes executable programs that reside on systems and have the privileges of the person who installed it.

Steganography

Steganography gives an adversary ability to communicate and disseminate sensitive or pilfered information with minimal potential for detection by security personnel. It's the art and science of hiding information by embedding messages within a seemingly harmless bit stream.

Information can be hidden in such a wide range of mediums that it's nearly impossible to detect. Within reason, anything that can be embedded in a bit stream can be hidden in an image – including plain text, cipher text and other images.

Although text and audio steganography can be employed quickly and successfully, it's image steganography that has matured most dramatically in recent years with development of fast, powerful graphical computers, and steganographic software readily available over the Internet.

A recent incident involved duping of a French defense contractor, which suspected its designs were somehow being leaked. Although it had careful guards on how digital information could leave the premises, the company eventually discovered it had unknowingly hired a computer criminal working as part of a team.

The individual had painstakingly embedded trade secrets inside images, and then posted the images on the company's public Web site. An outside team member then stole the secrets right from the company's home page. Investigators became aware of the steganography when it noticed slight variations in image file size.

An effective defense-in-depth strategy for combating netspionage must include layers of security at varying perimeters, with proper use of people, operations and technology at each layer.

At minimum, it involves awareness and education regarding the threat, vulnerabilities, general security practices, and current practice of installing security patches; up-to-date anti-virus software; sound firewall and intrusion detection software (which home users can frequently buy through a common application); testing and auditing; and aggressive use of encryption solutions.

With the correct approach, government, business and private users can close in on neutralizing netspionage.

Avoiding vulnerabilities

According to a 1997 American Society for Industrial Security survey of Fortune 1000 firms, U.S. companies are believed to have lost roughly $250 billion annually to information thieves. To avoid this problem, *officials* want to highlight some of the most common vulnerabilities to Local Area Networks. By following local procedures, users can avoid the majority of security issues. Remember to keep computer training current, and if a security problem is encountered, contact the Network Control Center as soon as possible.

Laptops: The Computer Security Institute reported that approximately 57 percent of corporations experienced a loss related to laptop theft, and an insurance industry estimate states that more than 319,000 laptops were stolen in 1999. This is of special concern to executives and to organizations such as the military and law enforcement, where the work force is highly mobile and deals with particularly sensitive information.

Going wireless: Because radio waves travel through ceilings, floors and walls, transmitted data may reach unintended recipients on different floors, or even outside the building housing the access point. With a Wireless Local Area Network, the boundary for the network has moved. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including the parking lot.

Look who's talking: Unknowingly installed spyware programs can capture online activity; cause Internet browser instability and slowness; consume system resources and cause system errors; and render systems vulnerable to attack or compromise. Spyware includes executable programs that reside on systems and have the privileges of the person who installed it.

USAFE NOSC

how to provide network defense

By Master Sgt. Michael Harris
Superintendent Current Operations
United States Air Forces Europe

What comprises a Network Operations and Security Center, and what can it do to maintain network operability and reliability?

At Ramstein Air Base in Germany, the NOSC applies multiple technologies to provide network defense in depth to thwart the adversaries' intentions. In the past year, the USAFE NOSC had 1.04 billion connections; from that number, there were 416 million suspicious connections, which yielded 500,000 real-time alerts, 1,616 cases opened and culminated into four actual break-ins.

To understand these numbers, imagine every Chinese citizen trying to gain access into your house in just one year. It would be a remarkable feat to have only four people actually gain access to your home with more than a billion attempts. Further, of the four that did get into the network, they were quickly caught and shut out. It is amazing to consider that a network probe happens every minute in the USAFE theater of operations. Imagine if the White House got attacked that often—we would be at war in no time flat.

No other system is attacked more often than its network, which is vital to the nation's defense.

The Ramstein NOSC applies a three-pronged approach to defense: enterprise control, network defense and remote administration, more commonly called RAT for Remote Administration Team. The RAT is divided into infrastructure and applications. Infrastructure includes perimeter routers, switches and firewalls; and Applications includes exchange servers, Outlook Web access servers and Norton Anti-Virus gateways. A large part of network management within the USAFE theater of operations is done via remote administration. The centralized administration of infrastructure and applications enables technicians to quickly apply patches and routing schemes to meet security demands. The benefit to this approach is simple: continuous control of the health of the information systems. To apply the remote function to the RAT section, a specially configured system

Maj. Jeffrey Sorrell, chief of Current Operations, hosts a delegation from Moldovia during a Partnership for Peace tour sponsored by USEUCOM. Also pictured is Krystal Rutter, a contractor with the USAFE NOSC.

KNOWS

is placed within a base's perimeter. The operator accesses the remote administration box using Internet Protocol Security through the base firewall. Once a technician has gained access to the box he or she can easily configure any device within that domain. Yet even if the RAT has done its job correctly, a threat to security still exists.

The Network Defense section of the NOSC tracks probes, connections and malicious logic. As stated earlier, this section has the tough task of discriminating between the 416 million suspicious connections for actual threats. Computers are phenomenal at crunching numbers to determine the slightest change in code. However, humans have a difficult time with this type of task and could never match the computer on speed. On the other hand, what the Network Defense technicians do excel in is research and analysis. Information professionals use their training, experience and intuition to determine intent. The combined effect of human and computer interaction is synergistic in this position.

Network Defense could not happen without reliable data connections. To maintain reliable network connections is the job of Enterprise Control. Controllers have real-time system tools to view link connections. Technicians play a significant role in ensuring the seamless routing and recovery of classified and unclassified information systems. For instance, if a base is involved in a critical mission and loses its command and control data, the Enterprise Control technician must immediately diagnose where a particular failure has occurred and determine how to restore network connectivity. Enterprise Control can be a stressful job due to the amount of coordination and reporting to various levels of leadership and multiple levels of Air Force and joint organizations.

Fortezza & the future

Lajes overcomes hurdles with Defense Messaging System

By 1st Lt Gilbert Hinojosa III
65th Communications Squadron
Lajes Field, Azores, Portugal

Tech. Sgt. Brian Kirkwood, Wing Information Assurance Office, inserts a Fortezza card into his Fortezza reader prior to decrypting DMS messages.

The Department of Defense has set Sept. 30 as the last day for units to use the Automatic Digital Network to send and receive message traffic. If your base messaging center is anything like ours, then you've been working feverishly to ensure all your messaging clients have the capability to send and receive Defense Messaging System messages. The 65th Communications Squadron has found quite a few hurdles to overcome with DMS, but the proverbial light at the end of the tunnel may be in sight.

Without a doubt, a major issue DMS raised involved Fortezza cards. As an end-user, the last thing you want to do is keep track of a card to check your messages. However, nothing is more frustrating to a base messaging center and wing information assurance office than knowing a Fortezza card is missing. After all, without it, customers won't be able to read or send messages.

At Lajes Field, the 65th CS has found a way to alleviate end-users accountability concerns by incorporating an awesome tool called Defense Message Dissemination System. In a nutshell, it's an automated mail client program. When used in conjunction with a cipher server, it allows a user to receive decrypted NIPRNet or SIPRNet DMS messages without having to use a Fortezza card or install a reader on their computer. The end-users Fortezza card is stored on a NIPRNET or SIPRNet cipher server in the messaging center. As a result, the customer doesn't have to worry about losing or misplacing a card or inserting it into a computer to read DMS encrypted messages. Hassle-

free DMS message reading is a definite possibility with DMDS.

DMDS also has a trendy pager-notification system. When enabled, it can notify a user when they receive a message. The best thing about this feature is it allows the messaging center to separate itself from the responsibility of notifying users of high-precedence messages. A small investment of $2,500 and a little time will allow users to begin using this great tool. Not only will external customers love it, internal folks will jump for joy.

Of course, no system is perfect. First, DMDS doesn't allow the end-user to send DMS messages. If the end-user is a daily sender of DMS messages, then storing a Fortezza card on the cipher server is not the best option. If the customer is an occasional or infrequent sender, he or she can always visit the messaging center to send out a DMS message. Second, the cipher server is not limitless. It only allows people to store up to eight Fortezza cards. However, each card can store up to seven DMS V.3 accounts for a total of 56 DMS V.3 accounts on each cipher server. So if you were to have more than 56 DMS accounts, more than one cipher server must be purchased. DMDS has certainly cured some DMS headaches at Lajes Field.

With the closure of AUTODIN around the corner, this may be a viable option for other units around the Air Force.

FORTEZZA FAUX PAUX

Without a doubt, a major issue DMS raised involved Fortezza cards. As an end-user, the last thing you want to do is keep track of a card to check your messages; however, nothing is more frustrating to a base messaging center and wing information assurance office than knowing a Fortezza card is missing. After all, without it, customers won't be able to read or send messages.

Staff Sgt. Chris Ford installs a Fortezza card into the Litronic Cipher server at DMS Message Center

AWACS Securely connected

By Senior Airman Jacob A. Lackey
752nd Computer Systems Squadron
Tinker Air Force Base, Okla.

The aircrews of the E-3 Sentry, Airborne Warning and Control System, have a new communications capability as they continue to fight the Global War on Terrorism.

In the past, there have been instances where AWACS was required to launch without the latest updates to the Air Tasking Order, Air Control Order or other mission essential data. On these occasions, the aircrews have been forced to use voice communications to contact operations personnel on the ground and transcribe the information by hand. Not only does this method tie up critical Ultra High Frequency Satellite Communications channels, but it also distracts aircrew members from accomplishing their mission essential tasks—a potentially dangerous combination.

To address this problem, the 552d Air Control Wing here worked with Headquarters Electronic Systems Center at Hanscom AFB, Mass., and the High Frequency Global Communications System program office to deploy High Frequency Messenger. HFM gives aircrews the ability to send and receive classified electronic mail while airborne, connecting aircrews with commanders that may be hundreds or even thousands of miles away. HFM uses the HFGCS and radios capable of adaptive high frequency communications techniques to establish and maintain a highly reliable wireless link from an E-3 to a Secure Internet Protocol Router Network gateway on the ground. In effect, HFM extends some SIPRNET capabilities to an airborne mission platform.

According to Col. Marty Edmonds, commander 552d Computer Systems Group, HFM is another step toward network centric warfare. HFM gives warfighters information superiority by assuring that critical mission data is delivered quickly, securely and reliably. No longer are aircrews required to squander valuable time and resources transcribing mission data relayed over voice channels. The beauty of the system is its simplicity. The operator uses Microsoft Outlook to compose and read e-mail as naturally as one might use a desktop PC in the office. The computers also have touch screens to use in place of the mouse. The operator can use a stylus, a pen or even a finger to make selections and launch applications.

Prior to each mission, 552nd CSG operations center personnel issue an HFM kit to the aircrew's computer display maintenance technician. Each kit contains a ruggedized notebook computer, modem, an encryption device and associated cables. The kit also contains software that automatically controls the radio link, the operation of the modem and the electronic message traffic.

In its primary mode of operation, HFM communicates using the HFGCS, a global network of HF radio stations. Message traffic on the radio link is encrypted and the signal is relayed over the horizon until it reaches the 789th Communications Squadron's Central Network Control Station at Andrews AFB, in Maryland. From there, the message passes through a gateway linked with the SIPRNET, thus giving the aircrew the capability to securely communicate on a global scale.

If necessary, HFM can also work in point-to-point mode. In point-to-point mode, the AWACS crew communicates using a direct radio link with other E-3s or HF ground stations in theater. The HF ground station is comprised of an HF radio, omni-directional antenna and an HFM kit. This ensemble can be set up in less than two hours. This outside-the-box thinking has allowed warfighters the ability to deliver or receive an ATO within a few hours of arrival at an austere location with no preexisting communications infrastructure. Efforts are under way to allow the ground station to link with the SCOPE Command SIPRNET gateway like its airborne counterpart.

According to Shirley Godsil, 552nd ACW communications requirements manager, personnel from the Electronic Systems Center and Rockwell

Courtesy photo

Master Sgt. John Mason and Staff Sgt. Michael Powers of the 552nd Operations Support Squadron operate an airborne High Frequency Messenger kit.

Collins successfully tested HFM during an E-3 training sortie Jan. 23. While on station some 800 miles from Tinker AFB, aircrew members from the 552nd Operations Support Squadron exchanged e-mail with an HF ground station operated by the 552nd CSG. Lt. Col. Ron Martin, chief of Wing Requirements, called it a rock solid test of the system that proves this technology's military utility for AWACS.

Rather than relying on voice communications to pass detailed information, like time critical targeting, commanders can now use HFM to quickly and accurately direct new taskings and pass updated information.

Originally, HFM was scheduled for implementation on AWACS in late spring of 2003; however, with tensions in Southwest Asia, the implementation schedule stepped up dramatically.

The Full Operational Capability date was accelerated at least two months, according to 1st Lt. Raymond Chester, officer in charge of ground communications, 752nd Computer Systems Squadron. In February 2003, airmen from the 752nd CSS equipped E-3 aircraft deploying to Southwest Asia with HFM kits. The implementation of HFM has brought the air battle into a new dimension by providing E-3 warfighters an integral data-link to theater and home-station command channels.

FAST FACTS

Primary Function: Airborne surveillance, command, control and communications
Builder: Boeing Aerospace Co.
Power Plant: Four Pratt and Whitney TF33-PW-100A turbofan engines
Thrust: 21,000 pounds (9,450 kilograms) each engine
Length: 145 feet, 6 inches (44 meters)
Wingspan: 130 feet, 10 inches (39.7 meters)
Height: 41 feet, 4 inches (12.5 meters)
Rotodome: 30 feet in diameter (9.1 meters), 6 feet thick, mounted 11 feet (3.33 meters) above fuselage
Speed: Optimum cruise 360 mph (Mach 0.48)
Ceiling: Above 29,000 feet (8,788 meters)
Maximum Takeoff Weight: 347,000 pounds (156,150 kilograms)
Endurance: More than 8 hours (unrefueled)
Unit Cost: $123.4 million (fiscal 98 constant dollars)
Crew: Flight crew of four plus mission crew of 13-19 specialists (mission crew size varies according to mission)
Date Deployed: March 1977
Inventory: Active force, 33; Reserve, 0; Guard, 0

PROVIDING *the*

Vital link for nuclear command & control messaging

By 1st Lt. Amber L. McKnight
Commander, SACCS Operations Flight
55th Computer Systems Squadron
Offutt Air Force Base, Neb.

In an age of rapidly advancing technology, the $680 million Strategic Automated Command and Control System, with its 25-year-old legacy equipment including 8-inch floppy diskettes and green screens, remains the nation's premier nuclear command and control messaging system.

The SACCS network remained a key part of U.S. nuclear deterrence to enemy attack for the past 42 years, serving as a cornerstone of America's defense. SACCS provides the means for entry, transmission and distribution of emergency action messages, force direction messages and routine data messages between higher headquarters, unit command posts and missile alert facilities for 1,500 customers at 132 locations throughout the country. Emphasizing SACCS' critical C2 role, the 55th Computer Systems Squadron recently installed new workstations at the U.S. Central, Special Operations and Northern Command headquarters, as well as at Cheyenne Mountain Air Force Base, Colo.

Staff Sgt. Beverly Likert and Senior Airman Jeremy Vonbon are archiving messages from the subnet communications processor by loading a magazine disk unit that holds 10 8-inch floppy diskettes.

Despite the system's advanced age, the 55th CSS Operations flight maintained a 99.8 percent system-wide availability rate. This ensured the delivery of 200,000 nuclear command, control and emergency action messages. Additionally, the flight installed SACCS desktop terminals at seven new sites, expanding the secure military network used to control the nation's strategic forces. The new SACCS desktop terminals saved the Air Force $4.2 million in hardware and maintenance support costs this year alone.

In February 2002, a fire at Barksdale AFB, La., destroyed $15 million of SACCS network hardware and caused a major network blackout affecting many squadrons. Communication specialists from the 55th CSS prepared and shipped three SACCS desktop terminals and rerouted communications lines, restoring message traffic to all sites within 72 hours. Technicians then overhauled and shipped $525,000 of SACCS legacy backbone equipment, restoring full network operations in just three weeks, normally a 60-day process.

55th CSS lobbied for and received $980,000 to fund the largest SACCS network expansion in the system's 25-year past. The team's research maximized performance and minimized costs, enabling the purchase of 460 computer and cryptographic items while saving the Air Force $500,000.

The 55th CSS Operations flight played a major role in planning future system configuration changes and network expansion. As the demand for EAM capability increased, the Air Force singled out SACCS to fulfill the requirement. Technicians and engineers began testing network configuration changes to enable a 50 percent network expansion worldwide. Positive results of initial tests proved several operational concepts, leading to the largest expansion in SACCS history. As recognition for their efforts, the 55th CSS won the United States Air Force Maintenance Effectiveness Award.

By 2nd Lt. Michael Wigley
Officer in Charge of Engineering Services
Randolph Air Force Base, Texas

The Air Education and Training Command Network Operations and Security Center celebrated the opening of its new operations floor April 15 here. Lt. Gen. John D. Hopper Jr., AETC vice commander, was the keynote speaker at a ribbon cutting ceremony that officially opened the new NOSC.

The project took 14 months to co-locate the AETC NOSC with the 12th Communications Squadron's Network Control Center. The facility, triple in size to the previous location, is AETC's, "center of the universe for network monitoring and management," said to Col. Paul F. Capasso, former AETC Director of Communications and Information.

A part of the AETC Computer Systems Squadron, the NOSC and its support offices now have sufficient space to provide network situational awareness, intrusion detection and response, as well as remote network management of the command's networks. The new facility also provides the foundation to support the command's NCC reengineering initiative. This multi-year effort involves transferring responsibility for after-hours help desk support, base-level network infrastructure management and network core services to the NOSC for all 13 AETC bases. Finally, the AETC NOSC serves as the Air Force Computer Emergency Response Team alternate operating location.

Construction of the new NOSC operations floor began Sept. 16, 2002, and lasted until Jan. 21. Upon completion of physical construction, contractors, military members and government civil service workers were brought in to establish all the appropriate connectivity for unclassified and classified data processing. The final product was a new fully networked server room and operations floor to support continued growth of the AETC NOSC.

The move did not just affect the AETC CSS and its network operations. The overall project was broken down into six phases and involved moving portions of four other organizations to new buildings, as well as remodeling those areas to meet the needs of the new occupants. According to Lt. Col. Gary W. Klabunde, AETC CSS commander, the key to success was the professionalism of the men and women of the 12th Flying Training Wing and the Headquaters AETC staff. "Everybody showed a tremendous amount of support to this project. It was definitely a Team Randolph effort!"

The final price tag – $425,000. Not a lot of money considering the movement of five units to different parts of the base, refurbishing these new facilities and also installing a state-of-the-art server room and operations floor.

SCOPE NETWORK

Strike teams tackle AF networks one base at a time

By Capt. Evan Watkins
Air Force Communications Agency
Scope Network
Scott AFB, Ill.

The computer is the entry point into one of the most dynamic systems the Air Force owns—the Air Force Enterprise network.

In early 1997, the Air Force, recognizing the importance of this system, put together a small band of network experts to help combat common issues plaguing this multi-billion dollar system.

Armed with specially trained, highly skilled officers, NCOs and contractors the Scope Network team accomplishes precise network analysis and repair.

Scope Network, a division of the Air Force Communications Agency, is tasked with visiting all 128 active and Reserve base network communication centers and major command Network Operations and Security Centers every 18 months. The goal is to enhance warfighter capabilities and it's accomplished by: securing, fixing and optimizing networks; identifying and sharing best practices; and providing a feedback process supporting the AF enterprise to facilitate the, "One Air Force, One Network" concept. When a Scope Network team leaves the base, they leave the network in far better shape than they found it.

Within the first year, the team developed the Network Maturity Model, the concept, processes and procedures of network assessments, and defined the team composition. They carried out a handful of network assessments of unclassified networks to validate and fine-tune their model. Scope Network's role and effect on the networks has been growing ever since. As Scope Network wrapped up the 12-month, 2002-visit cycle, they numbered 10 five-person teams plus an eight-person support branch and had accomplished 139 base visits across the Air Force.

Each Scope Network member receives a significant amount of training, the amount of training that NCC crews should get, but often far above that available to most NCC or NOSC personnel. People assigned to Scope Network enter with some networking experience, however, usually not to the level necessary for an operational Scope Network engineer. For this reason, all members are put through a rigorous training program that teaches every aspect of their specialty, from basic computer networking to highly specialized architectural engineering. Before a team member is allowed to touch base network configurations, they must know the technology inside and out.

With the ever-changing technology landscape, maintaining adequate expertise at every NCC across the Air Force is a daunting task. This is one of the underlying reasons Scope Network is needed. Training can be focused at a single level and this expertise brought to each base prior to and during network analysis and repair, the team members provide hands-on training to support the recommendations they've identified. In addition, Scope Network can provide training on new technologies and bring best practices from other bases to the NCC.

In addition to regularly scheduled visits, Scope Network partners with the AF Network Operations Center to provide a global rapid response capability for bases in need. AF NCCs and NOSCs request additional assistance from the AFNOC Help Desk when the need arises. If necessary, the

SCOPE NET'S MISSION

▸▸ Enable integration and interoperability of C4ISR systems, while improving operational readiness of Air Force networks through assessment, baselining and optimization.

AFNOC calls on Scope Network with network, server, messaging, and network security problems they cannot address. Frequently, Scope Network and AFCA receive requests for assistance directly from the Communications Squadron commander or MAJCOM. Like scheduled visits, rapid response support is provided globally, from temporary bases in Southwest Asia to permanent CONUS bases as well as those in the Pacific; Korea, Japan and Guam.

Scope Network visits are not limited to established bases; on the contrary, Scope Network visited nearly every AF network resource worldwide. From the CAOC in Southwest Asia to EUCOM HQ, Scope Network maintains a worldwide mission and can be called on to analyze, secure, and optimize networks anywhere in the world. To date, Scope Network has been an integral part in almost every recent contingency, to include Operations Southern Watch, Northern Watch, Enduring Freedom, and Iraqi Freedom. In addition, Scope Network has an existing mission to visit every base across SWA in the CENTAF area of operations on a six-month recurring basis.

While base visits are integral to Scope Network's mission, they also compile common recommendations and best practices seen across the Air Force into one key document. The Recommended Practices guide is updated annually and is available to anyone on a .mil site; see https://www.afca.scott.af.mil/scopenet/rec.htm. The site includes suggestions for technical reading and training to enhance individual capabilities.

A typical base visit is usually scheduled months in advance. During the pre-visit phase, information is gathered from each base using a mix of questionnaires and information-gathering tools so the actual trip can be customized to the needs of the base and NCC. Preparations for the visit are coordinated with Scope Network personnel and NCC staff long before the visit. Upon arrival, the Scope Network team in-briefs the CS/CC and gathers final details about the configuration of the network. During the visit, necessary changes are coordinated with NCC personnel. Those changes that can be made are implemented and the remaining left as recommendations in an after-action report sent to the base after the visit.

Scope Network has visited almost every AF site at least twice over the past few years, fixing and optimizing numerous networks, providing extensive and diverse training, and establishing a reputation as the premier network experts in the Air Force. Although repeat problems are still common, Scope Network is seeing improvements across the enterprise ... improvements that, in the end, enhance warfighter capabilities for all Air Force personnel.

Mandatory computer training still the standard

By Senior Master Sgt. Alan McClellan
805th Computer Systems Squadron
Scott Air Force Base, Ill.

"I think I have to do Security Awareness Training and Education, but where do I do this now?"

This question has frequently been directed to Headquarters Air Mobility Command, and the answer may even surprise many Information Assurance knowledgeable people. SATE used to be required for access to the networks, but it has been replaced.

As some people may probably know, SATE was eliminated in September 2001 when the current version of AFI 33-204 was released. Once people learned that formal SATE requirements no longer existed, the next question that naturally arose was what replaced the SATE program?

The successor program is Network User Licensing. AFI 33-115 version two states that user IA training has been standardized in the IA Internet-based training course. Successful completion of this course satisfies DOD user certification, Air Force SATE training and Air Force network users licensing. Records of user training are contained in the IA IBT database.

This training is mandatory for all new network users and any user who requires a new network user identification. It is also recommended for current AMC network users as refresher training. Additionally, many personnel deploying have been required to show proof of course completion, or they have been required to accomplish the training at their deployed location before accessing the network, causing mission delay.

Network users must access the following URL to complete current network user licensing requirements: **http://usaf.smartforce.com**. Be aware the Web-based IBT courses slow down significantly during peak demand periods, so users might need to try visiting the SmartForce Web site early or late in the day.

Once users access the Web site above, they must formally register to access IBT course material. Registration includes selecting an eight character password that contains at least one character from each of the following categories: number, upper-case, lower-case and any of the following special characters (**! @ ~ # $ ^ ( ) _ =**). The system only accepts passwords with eight characters.

Once users are registered and logged on, they are allowed to select a link labeled IA Courses. This in turn brings up a page with the following course links: INFOCON Network User Licensing, System Administration,Web Administration and Workgroup Manager. Drop-down menu options include 'Launch' course to start, and 'Certificate' to print course completion records.

The normal network user will only need to complete the 'Network User Licensing' module. It is recommended that new users be given supervised network access to complete the required SmartForce IBT course. Then, once new users complete network user license training and receive certificates, workgroup managers can establish network accounts for them.

Although some SmartForce IBT courses allow users to take course exams without first reviewing course content, the basic Network User License course does not. Users must get above 70 percent for successful course completion. After completing each IBT pertaining to duties, users should print the associated certificates.

With the current world situation, it is strongly suggested that all personnel either assigned to an AEF, or with a deployable mission, ensure this network user licensing is completed prior to deployment, and take course certificates with them so there will be no mission delays when arriving at deployed destinations.

Your workgroup managers have the responsibility to track network user compliance for this requirement and can access the SmartForce database to ensure you are registered.

If you have any questions, contact your workgroup manager, base IA office or the AMC IA office at DSN 576-4979.

Traveling the Information superhighway

Security of DOD information technology still a top priority for officials

By Gerry J. Gilmore
American Forces Press Service

WASHINGTON (AFPN) — The U.S. military uses the Internet as an electronic conduit to quickly disseminate information. From a security perspective, however, stretches of that worldwide information highway contain potholes.

"We need to use the Web for efficiency and effectiveness — it's a great medium. But, we have to use it with security and information sensitivity in mind," said Linda Brown, a Department of Defense information technology specialist and the person responsible for the DOD Web site administration policy.

DOD Internet security is getting better, even as more and more military information is being carried over the World Wide Web, said Brown, who works in the office of the assistant secretary of defense for command, control, communications and intelligence.

On the other hand, operations and exercise plans plus installation maps for water, electric and other utility services have no place on publicly accessible Web sites. That kind of information "would be helpful for someone intending to defeat our plans, our intentions," she said.

Classified information, she said, is contained within heavily safeguarded separate networks that can be accessed only by certain individuals. However, there have been cases where the public was found to have access to things that were supposedly only on protected intranets.

Such occurrences, though, are most often inadvertent and quickly remedied when discovered, Brown said.

Other items definitely not for public viewing include anything that is for official use only, detailed computer system information, organizational manning charts and graphics, and photos of base entrances and exits, she said.

Even unclassified, personal information could be of interest — information such as home addresses that would allow Web surfers to harass or target servicemembers' families, Brown said.

DOD's Web policy is accessible at **http://www.defenselink.mil/webmasters**. The site provides guidelines on what DOD Web administrators and content providers can and cannot do on the department's Internet pages.

DOD officials have been concerned about Web security issues for years — long before the war against global terrorism erupted, Brown said.

"The basic DOD Web policy was issued in 1998," she explained. "Maybe we have some heightened concerns because of the world situation today."

U.S. adversaries routinely check out DOD Web pages for information, Brown said.

"It's an ongoing, constant concern."

In a training scenario

Vandenberg comes under attack

Lt. Col. Alan Claypool
Commander, 30th Space Communications Squadron
Vandenberg Air Force Base, Calif.

It's 9 a.m. on a Wednesday morning at Vandenberg Air Force Base, Calif. Suddenly, the Network Control Center is flooded with phone calls. Someone has penetrated the western launch range computer network. The information terrorist created an e-mail account for a nonexistent officer in the Space Communications Squadron and sent an e-mail requesting everyone to reply with his or her network password. Vandenberg is under attack by an unknown assailant located somewhere in the shadows of the electronic world. The message from Capt. Chris Deez, officer in charge, NCC Operations reads:

The e-mail exchange server will be upgraded Feb. 20 at 2 a.m. To prepare for the upgrade, we need everyone to reply to this e-mail ASAP with your password. This will ensure you do not lose any data (e-mails, contacts, address book entries, etc.) in the upgrade and have uninterrupted e-mail service. Thank you for your time and attention to this matter.

The contracted NCC springs into action and notifies the computer network defense office. The CND office is charged with frontline defense of the entire western range network system covering 99,000 acres networked with an aging and complex hodgepodge of fiber, copper and microwave links. The network is critical to 5,500 launch partners, to ensure successful spacelift, ballistic and aeronautical test flights. In the CND office, network specialists smile upon notification of the attack. Smile? Was it because they were tracking the terrorist? No. They *were* the terrorist ... this time. The entire event was part of an inspector general-sponsored basewide antiterrorism and force protection exercise.

The purpose of this exercise event was for the CND to expose vulnerabilities by pretending, with official approval, to be a social engineer. In reality that person could have been a spy, a terrorist or someone after information for other purposes. These people get information by talking, listening, looking or passing themselves off as someone else. This form of intelligence-gathering is known in the trade as social engineering.

Most people attempting to obtain access to a network do their mischief electronically and from

Network specialists from Vandenberg Air Force Base, Calif., discuss the strategies used to protect the base's network infrastructure from attack.

a distance. Vandenberg receives 10,000 probes daily to the network from the firewall. These attempts are blocked using technology and monitoring. But what about the "back doors?" Our greatest vulnerability is the 5,500 people on the inside of the network, not to mention the downloading or running of illegal software, or the choosing of easy-to-crack passwords. What about people who don't load their software security patches, or who leave network ports easily accessible in unlocked offices and conference rooms? How many people bother to check the credentials of someone who shows up to "repair" a computer?

There are many methods to obtain information from within. One is to make phone calls posing as someone who is likely to be trusted, perhaps someone alleging to be higher ranking or someone who mentions a mutual friend. The question to ask yourself is, "Why is this person calling *me* for the information when I'm not the best person to give it?" Social engineers will target new people and people who either don't understand or don't care about the value of their information.

One of the most valuable tools a social engineer can possess is an old phone book that gives names, titles and phone numbers. It's easy to pose as an insider once you have the unit structure and leadership names. A complementary method is coercion: pretending a crisis exists and that you, or they, will get into serious trouble if help is not forthcoming. Faked e-mails are another trick of the social engineer's trade. The e-mail may request help to download and install software from a Web site or help to forward a document because his or her computer is down. Excessive flattery or promise of a better job is also a common trick.

There are two commonly held, and completely misguided, assumptions that our fictitious Deez used to her advantage.

The first: if you are in the e-mail list, you must be authentic. The second: if the display name comes from a known office, it also must be authentic. In both cases, the assumptions are incorrect. Anyone can be added to the global e-mail list and display names can be created to say anything. You get the idea: the e-mail from Deez could easily have come from someone outside of our network, pretending to be on the base.

The captain used two other easy tricks. She threatened the loss of your data and gave you a short, but believable, suspense. As people responded, even if they did not give up a password, they provided an in to the social engineer to confirm their addresses and to begin conversations. Or worse, they may have unknowingly given her warning that she had been compromised and needed to erase her tracks and disappear. She could have done serious damage to the network to distract the NCC or cover her tracks.

Some may consider social engineering a less than honorable medium of deception ... that is why it works so well. There's nothing novel about using deceit and fraud to gain information or penetrate defenses; it's been going on since the beginning of recorded history. Some people may be naive enough to believe the technique would never be used against us, so an exercise such as ours was a waste of time. But the truth is, we devote a disproportionate amount of worry and training to electronic – as opposed to human – vulnerabilities. It's one thing to get into a system, but it's another, much more dangerous thing, to find and understand the critical data.

The exercise kicked off at 9 a.m. and at 9:02 a.m. we had the first password – in two minutes the social engineer had what she was looking for. By the end of the event, after one hour, we had 16 passwords and 162 replies. Six hours later, long after the end of the exercise and long after the issuance of numerous warnings and explanations, we were still receiving passwords and replies. In total, we received 20 passwords and 175 responses.

This exercise was not intended to focus on the failures of individuals, but to raise the entire organization's consciousness and to highlight areas in which security needs to be tightened. The numbers of passwords and replies may seem reasonable compared to the 5,500 users on the network. But it takes only one to expose operations to a mission interruption or security threat. Remember, all of these users had IAAP training and have signed user agreements.

Network security is serious business, and the lesson here is that any one of those who responded could have cost the entire base, and the Air Force, a great loss.

Revolution

Joint Tactical Radio system soon to be RF standard

By Capt. Todd G. White
Air Force Command and Control and Intelligence, Surveillance & Reconnaissance Center
Public Affairs
Langley AFB, Va.

Have you ever imagined the radio frequency spectrum as a weapon system? Software-defined radios in the form of the Joint Tactical Radio System, referred to universally as JTRS, have led warfighters throughout the Department of Defense to join forces and look at the RF spectrum from a completely new perspective.

"JTRS is much more than just another radio…it's a revolution in the way warfighters will access and employ the RF spectrum in the Department of Defense in the future," said Col. Charles Whitehurst, director of the Global Communications, Information Directorate of the Air Force Command and Control and Intelligence, Surveillance and Reconnaissance Center at Langley Air Force Base, Va. "The JTRS revolution ranks among the most significant transformation events within the world of communications taking place in the RF spectrum domain today, delivering virtually the entire RF spectrum to the warfighter in a single family of radios. JTRS cuts across all operational platforms, all services, all frequencies, throughout the tactical, operational and strategic levels of warfare."

Capt. Todd G. White, AFC2ISRC/PA

Col. Charles Whitehurst demonstrates a current JTRS Cluster-1 radio (left) and a two-channel JTRS Cluster-4 prototype radio (right).

As the military moves toward a network centric communications environment, it is imperative that we move from legacy equipment that performed one function (HF, UHF, VHF, SATCOM) to a family of radios that provide the means for digital information exchange. JTRS supports joint operations by providing the capability to transmit, receive, bridge and gateway among similar and diverse waveforms and network protocols within the RF spectrum. Connectivity to civil and national authorities is possible as well as connectivity to vertical, horizontal and joint and coalition warfighting elements.

Advances in areas such as embedded processor technology, digital converter performance and object-oriented programming have enabled a shift from hardware-intensive radios to flexible, multiband, multi-mode software radios, in which functionality is provided through software rather than hardware. A software-defined radio permits operators to tailor the radio to meet specific operational needs by using relatively generic hardware and loading multiple software waveform applications that meet identified requirements. The flexibility of a programmable, software radio allows the warfighter to accommodate various physical layer formats and protocols. This allows the services to host the entire RF spectrum, HF, UHF, VHF, SHF, etc., on a software format and install those waveforms inside the JTRS radio system. JTRS is a family of radios that is "platform-agnostic" yet "mission-specific" for each platform, and represents the OSD solution for spectrum domi-

nance.

On Oct. 14, 2002, the Assistant Secretary of the Air Force for Acquisition tasked the AFC2ISRC to develop the Air Force JTRS migration plan, using the current 32 different primary waveforms being developed by the JTRS Joint Program Office.

Six months ago, we were talking in terms of 2 MHz to 2 GHz," Whitehurst said. "We looked at the JTRS airborne radio only in terms of the channels on the radio, a power amplifier and additional RF frequencies. That way of thinking was fine to meet current operational requirements, but it didn't address future requirements (which we anticipate to reach 54 GHz). JTRS is far more than a radio replacement program…it's a totally new way of thinking about communications," he said.

A major tenet for JTRS is the easy insertion of advanced technology. Since the radio is software driven, any inherent change in the software capabilities has minimal, if any, impact on the resident hardware. In the first iteration of the JTRS system, it was possible to install a variety of different frequencies on available ports, but the number of ports was limited. While this equated to a major leap forward from previous technical solutions, it did not fully exploit the capability of JTRS since it didn't fully exploit the processing capacity of the radio. The latest JTRS system will migrate away from this type of thinking entirely and incorporate all programmable components within one relatively small unit.

When we think of a multi-mission platform, that is, an airborne platform that can perform more than one mission, we usually think in terms of large wide body platforms. We're driven to this, as often as not, due to the space required to host the electronic, communications and support equipment. One example of this is employment of the Roll On/Off Beyond Line of Sight Equipment (ROBE) on the RC-135, which allows the aircraft to perform both the air-refueling mission and Line of Sight/Beyond Line of Sight extension of Link 16. The scalability of JTRS will allow it to be easily installed in virtually any platform within the Air Force inventory, to include hosting waveforms on missiles and smart bombs.

Imagine a flight of F-15s enroute to a theater of operations. On their ingress/egress, equipped with JTRS radios, they perform a variety of missions currently being conducted by large, wide body platforms. They transmit and receive RF signals over the entire frequency spectrum, functioning as both fighter aircraft as well as communications and gateway nodes to perform such missions as signal intelligence collection and radio jamming, performing whatever RF mission is required to deny enemy access to the RF spectrum.

JTRS will eventually be integrated into 64 different types of aircraft in the Air Force inventory, as well as a myriad of ground-based platforms, during scheduled depot level maintenance.

JTRS will eventually be integrated into 64 different types of aircraft in the Air Force inventory, as well as a myriad of ground-based platforms, during scheduled depot level maintenance. JTRS is programmed to replace 750,000 radios within the inventory covering operations such as navigation, positioning, location, identification, air-to-ground, air-to-air, ground-to-ground and satellite communications. Capitalization of integration costs will be realized by reducing 124 different radio sets to approximately 10-20 form-fit radio sets.

Several challenges are yet to be resolved to fully exploit the inherent capabilities that JTRS will bring to the battlefield. Two of these include antenna research and legal constraints affecting all radio systems, especially those designed to access the entire RF spectrum, due to potential conflicts with non-US authorized frequencies and non-military systems. While several challenges have yet to be resolved to fully exploit the capabilities that JTRS will bring to the battlefield, JTRS is a revolutionary way of doing business. Once fielded, warfighters will no longer think of the RF spectrum in terms of hardware but as capabilities. Multiple software applications will allow implementation of different standards in the same radio system. Radio receivers will be reconfigured over-the-air, thereby reducing maintenance requirements.

"In the past, platforms equipped with an HF radio were limited to communicate with HF waveform subscribers. Once JTRS has been fielded, a warfighter will be able to talk to another warfighter on multiple waveforms, and it will be totally transparent to him that this is what he is doing. We are only beginning to appreciate the realm of the possibilities that JTRS brings to the battlefield," Whitehurst said.

USTRANSCOM stands up state-of-the-art integration center

By Master Sgt. John L. Andrashie
Chief, Intelligence Systems
Administration Branch
U.S Transportation Command
Scott Air Force Base, Ill.

Now more than ever, employment of strategic mobility forces depends greatly upon accurate, reliable and timely information.

Information Technology is now seen as one of the major force multipliers for U.S. Transportation Command activities and is vital to the successful completion of all military operations.

"It is information technology that allows us to do the things we do today," said Gen. John W. Handy, commander of USTRANSCOM.

In an innovative move, USTRANSCOM's Intelligence Directorate (J2) depends on emerging IT capabilities as a means of integrating key intelligence functions with Operations and Logistics (J3). Dubbed, "Joint Operations Integration Center (JOIC)," the center supports the Global War on Terrorism, home land defense and other contingency operations. To integrate key command intelligence components, the center incorporates modern computer systems and networks to support a single intelligence hub. The hub is responsible for orchestrating intelligence and force protection support for ongoing operations and mobility-force elements. Enabled by technology, the JOIC fulfills the Intelligence Directorate's responsibility by providing operational intelligence and security information in support of rapid execution planning, deployment, employment and sustainment of mobility forces around the globe.

Not only does the JOIC integrate operations and intelligence, but it also provides intelligence support to the Joint Mobility Operations Center, the command's Crisis Action Team and component command organizations. Co-location of these functions make the JOIC an agile, synchronized focal point capable of responding to operational needs by recognizing threats and potential impacts on defense transportation operations. Complete with a top-of-the-line projection system, the JOIC provides specific, tailored, operational intelligence, to enhance the command's overall effectiveness.

Since no operation is complete without the support of communication warriors, 23 communications and intelligence specialists leapt into action by removing more than 100 aging office partitions, computers and storage units. The team also installed more than 300 feet of conduit and fiber-optic cable to connect existing networks and systems. To complete the operation, 27 individual computer systems along with audio-visual connectivity were tested and retested to ensure all applications ran flawlessly.

This team was involved in every phase of development, from equipment procurement and testing to complete systems integration. Their efforts guaranteed the completion of the JOIC in less than six months and well under initial cost estimates of $260,000.

Since its conception, Col. Kevin B. Noonan, the JOIC's commander, has deemed advanced and scalable Information Technology equipment vital to continued and sustained operations. Noonan contends, "With one mouse-click, we can receive intelligence support from three different networks. Information Technology allows us to collect real-time worldwide intelligence, giving us the capability to complete the daily intelligence update, giving USTRANSCOM commander and staff information from all theaters affecting USTRANSCOM assets." The successful activation and effective operation of the JOIC provides USTRANSCOM, component commanders and their staffs situational awareness of current crises and strategic warning of potential conflicts while enhancing integration and cohesive work environment between JMOC/CAT.

Photo by Staff Sgt. Jeremy T. Lock

OPERATION IRAQI FREEDOM — The Predator is a high-altitude unmanned aerial reconnaissance aircraft that serves as eyes in the sky for ground forces.

Predators: UAVs provide crucial support in skies above war torn Iraq

By Louis A. Arana-Barradas
Air Force Print News

SAN ANTONIO — Flying over coalition troops racing toward Baghdad, RQ-1 Predators are providing ground commanders up-to-the-second information on what lies ahead.

That is helping make the ground war a success by minimizing coalition troop losses, said Predator pilot Capt. Traz Trzaskoma by telephone.

"We immediately pass on any data we gather to the people on the ground who need it, and we provide it around the clock," said Trzaskoma.

The Predator is a medium-altitude, long-endurance unmanned aircraft. It is mainly used for reconnaissance and surveillance missions, and the information gathered cuts battlefield "decision-making from hours to minutes," Trzaskoma said.

"A special forces team was going into an area, and at the last minute (a Predator) saw their landing zone was not the best," he said. "We helped change the mission at the last second. Then we helped them find a better place to land."

Before each mission, Predator crews get an intelligence briefing. Staff Sgt. Alexander Britt, an intelligence applications specialist, does that job. His "info" helps the Predator survive over the battlefield.

Britt said that is an awesome feeling.

"The training back home is all good, no doubt, but it's all (simulated)," he said. "Not here. The intel I provide helps keep the airplanes safe ... that's mind blowing."

The Predators do their job quietly in all weather, and though the composite birds are in the air around the clock, they have had few problems, said Staff Sgt. Randy Townsend, a Predator crew chief. Unlike crew chiefs of other aircraft, Predator crew chiefs do all the work on their charges.

"I catch it, launch it, service it and do all the maintenance on the engine," said Townsend. As for how the aircraft is performing, he said, "We haven't had any problems at all."

Not a bad track record, Trzaskoma said, considering what the aircraft go through.

"We put 'em in the air, one after another, every day of the week, in all kinds of weather ... they fly and keep doing the job," he said. "They're helping win this war."

Comm 'jumps' into action for OIF

Senior Airman Mitchell Yang of the 86th Contingency Response Group prepares for his jump into northern Iraq with paratroopers from the 173rd Airborne Brigade, based at Ramstein Air Base, Germany.

Photo by Tech. Sgt. Rich Puckett

By Staff Sgt. Chad Padgett
USAFE News Service

RAMSTEIN AIR BASE, Germany (USAFENS) — In one of the largest airborne operations since World War II, 1,000 paratroopers from the 173rd Airborne Brigade dropped out of 15 C-17 Globemaster aircraft over Iraq March 26.

Taking part in the mission were six members of the 1st Combat Communications Squadron here.

1st CCS members installed tactical-satellite radio communications systems into seven of the C-17's. These systems allowed the members to talk directly with the jump commanders and keep them up to date on information that could affect the mission such as weather, enemy threat conditions and the status of the aircraft flying.

"The first two aircraft are linked through satellite communications with special operations forces on the ground," said Master Sgt. James Robertson, 1st CCS network radio systems superintendent. "Each plane after that would keep in touch with the plane ahead of it for the latest information."

The crew flew out of Aviano Air Base, Italy. 1st CCS members spent the two-hour flight to Iraq in the dark yelling over the noise of the aircraft.

"The windows of the planes were blackened out for safety reasons, we didn't want people on the ground to see the lights from the aircraft," said Senior Airman Michael Sweet, 1st CCS. "The roar of the plane was so loud that we were yelling messages to each other two or three times."

The one time they were able to see outside the plane was when the paratroopers were jumping.

"The only time we were able to see anything was when the back of the plane opened up and the paratroopers jumped out," said Senior Airman Brian Wacnik, 1st CCS. "It was pretty incredible to see more than 100 people exit a plane in less than a minute."

Before flying out, Sweet was given the message that since his plane was the last to fly out, his was the most at risk of enemy fire.

"I wasn't too worried because we were flying over the Kurdish part of Iraq," said Sweet. "I just focused on the job I had to do."

Gen. John W. Handy, commander of U.S. Transportation Command and Air Mobility Command, highly praised the jump.

"This is a historic milestone in the evolution of the C-17," said Handy. "The C-17, and more importantly the crews that fly it, have proven their mettle repeatedly while operating in the most demanding environments imaginable throughout the global war against terrorism. Now this workhorse has proven its capabilities in a combat airborne operation."

After the jump, the 1st CCS members had have a seven-hour flight back to Ramstein to pack up their equipment, rest and enjoy a job well done.

Trip changes airman's view of Iraq

Tech. Sgt. Steve Faulisi

By Louis A. Arana-Barradas
Air Force Print News

OPERATION IRAQI FREEDOM — For a combat cameraman from upstate New York, a six-hour ride from Kirkuk to Bashur Airfield in northern Iraq, was an eye-opening experience he will not forget.

Trained to look for and document with his camera those moments that tell a story, Tech. Sgt. Steve Faulisi said he put away his camera and just took in what he saw.

He became part of the story and excitement unfolding in Iraq. What snapshots he took were from his moving Humvee of a changing country and were for the people back home.

"What struck me most was how the people, especially the kids, ran from their homes just to wave at us, to give us the peace sign," said Faulisi, of the 1st Combat Camera Squadron at Charleston Air Force Base, S.C. "Every one was smiling. That made me feel good, like we were really wanted, appreciated."

What he had seen on television back home before he came to Iraq was a sharp contrast to what he experienced once in the country. On the television news each night, all he had seen were screaming, U.S.-flag burning demonstrators in other Middle East countries.

He did not see that on his long ride to Bashur.

"I saw a lot of kids waving homemade U.S. flags," Fausili, of Corning, N.Y., said. "I can remember saying, 'Wow! This is crazy.' And it brought a lump to my throat."

Faulisi left Bashur for Kirkuk on an Army five-ton truck, part of a long convoy. He went there to document the resupply of the Army's 173rd Airborne Brigade at an Iraqi air base. He returned in another convoy, only this time in a Humvee.

The images he saw etched themselves in his mind forever. They will provide a lifetime of "war stories" he can recount to his family, especially to his 13-year-old daughter, Danielle, and 10-year-old son, Anthony.

In his 20-year Air Force career, Fausili has never put his camera down for as long as he did on this trip. The events around him took his mind off taking pictures.

"When I did pick up the camera, it was to take a happy snap, something to remind me of the moment," he said. "Something to show my family."

At the Iraqi air force base, Fausili saw gutted and looted offices and buildings. There was a dilapidated MiG fighter on display at the entrance to the base. Everywhere he looked, there were signs of destruction, but the U.S. bombing campaign had not caused it.

"To me, it looked like it was just the locals taking things they'd been deprived of for so long," he said. "I saw people hauling desks and office equipment."

On the road were people everywhere, standing around at coffee shops, gas stations and sidewalks, waving at the passing Americans. There were many cars on the road.

"Our Humvee cut some guy off the road but he didn't take offense," Fausili said. "He just beeped his horn, smiled and gave us the thumbs up sign."

Fausili said he did not have a clue as to what to expect when he got to Iraq, but he knew it would not be like what he saw on television so he did not draw any conclusions.

"These people are trying to get on with their lives, I see that now," he said. "They know they don't have to fear Saddam Hussein ever again."

Honoring her fallen husband

Airman shares experience on national television show

By Staff Sgt. Shannon Collins
92nd Air Refueling Wing Public Affairs
Fairchild Air Force Base, Wash.

One Fairchild airman has a song in her heart and her eyes on the future. She seeks to overcome tragedies through music, competition and a national television show.

Senior Airman Christina Slocum, an assistant content manager and forms designer with the 92nd Communications Squadron, who was born on Fairchild 24 years ago, told her story of loss and triumph on the national syndicated daytime show, "Life Moments" Feb. 13.

"Just knowing you are going to see yourself on television and being able to tell your personal story is just amazing," she said. "My family was very excited."

During the taping of the show, Slocum competed in the World Championships of Performing Arts in California. More than 800 people from around the world competed for the gold in different categories.

For the original song category, she sang "Legacy," dedicated to her son and late husband, and for the gospel category she sang, "Happy," another song she had written. Though she didn't go further in the competition than the semi-finals in the gospel category, she made good contacts with producers and directors, and after her to Airman First Class Nevin Pratt, 92nd CS, she headed to Texas to record a gospel compact disk.

Though Slocum has been singing all her life in choir, her inspiration happened two years ago.

Slocum met her first husband, Michael, in the Air Force while they were stationed at the same base. They married one year after they started dating.

"He had a great personality, and I loved his eyes. He was a very dedicated man. If he said he was going to do something, he did it," beamed Slocum. "He first heard me sing in church. I looked over at him, and he had tears in his eyes. It made me feel that he could feel my heart."

Senior Airman Christina Slocum, 92nd Communications Squadron, looks over forms. (Photo by Staff Sgt. Shannon Collins)

"He had been in a car accident, and he had already passed away by the time I got to the hospital. I just screamed. I felt like I was in another world."

When Slocum became pregnant, she said Michael was excited.

For the first seven months, everything was fine, until she went into premature labor. Hours later, she gave birth to Michael Jr., who was 4 pounds, 3 ounces.

"Michael enjoyed holding our son so much. He was very good with him. He was extremely happy to be a dad. He was very proud," she said, her voice wavering.

Six weeks later, tragedy struck the family.

"I got up as usual and got Michael's lunch ready. I handed him his lunch, he handed me Michael Jr. and the last words out of my mouth were, 'I love you,'" Slocum said, tears running down her face, barely getting the words out. "I was woken up later by a knock on my door. He had been in a car accident, and he had already passed away by the time I got to the hospital. I just screamed. I felt like I was in another world.

"Michael Jr. was born six weeks early and if he had been on time, Michael wouldn't have ever seen him," she added, her voice full of emotion.

After her loss, Slocum returned to the one continuous comfort in her life, her music. She wrote her song, "Legacy," as a tribute to Michael's legacy he left behind, Michael Jr.

"I pour my soul into my singing. My music is very important to me. It is my life. And my son has a lot to do with my life and my soul. My husband's memory has everything to do with me starting to write music; he is my inspiration," said Slocum.

Slocum has had her ups and downs through tragedy, competition and her music. She encourages others to follow their dreams and to honor loved ones with music.

"Even though you are down, you can get back to the top and go further than you ever dreamed. There will always be struggles that lie ahead; you just have to get through them and say to yourself that you can and will make it through. I know that if I did not have God by my side, I wouldn't have made it this far," said Slocum. (Courtesy AMCNS)

New ID cards are secure, ready

AIR FORCE PERSONNEL CENTER - The high-tech identification Common Access Card, or CAC, currently replacing familiar green IDs worldwide is secure and proven in combat, despite some rumors to the contrary.

"Worries are unfounded" that the new IDs are easily accessible to identity thieves or even hostile forces, said Chief Master Sgt. Ricky Arnold, Survival, Evasion, Resistance and Escape program manager at the Pentagon.

"These cards are not a risk to anyone's privacy or security," said the chief.

"We thoroughly researched the security risks before we even began to issue common access cards," said Maj. Gen. Richard Mentemeyer, director of operations and training at the Air Staff.

"We were satisfied then, and recent events have reinforced our belief that common access cards are not only secure and safe but also provide required Geneva Conventions information in the event an airman is captured," the general said.

"In a war zone or at home station, there should be no hesitation: Don't leave home without it," he said.

The card does not contain any personal information electronically that isn't already printed on the card, officials said. What it does is allow for is electronic access to computer systems that contain personal data. Also, an extra layer of protection is provided when a card is reported lost or the cardholder goes into missing or captured status. At that point computer and data system access is turned off, officials said.

And built-in electronic security measures make getting access to what information is on the chip extremely difficult, if not impossible, officials said.

Rumors that some deployed airmen destroyed or lost their CAC cards in an effort to get an old-fashioned green ID card reissued to them spurred officials to conduct an informal study into the matter, the chief said.

"The results showed no evidence of that sort of activity—which would be illegal, since the cards are government property," he said.

Even in hostile areas, the new CACs do not put peoples' privacy and security at risk, officials said.

Each card bears a color photo and service seal of the holder, required visible personal data, a magnetic strip, linear and two-dimensional barcodes, and a 32 kilo-byte computer chip.

Even if someone had the extensive knowledge and expensive equipment needed to get information off the chip, an attempt would take longer than eight hours per card, and cause the card to be deactivated and/or destroyed in the process, he said.

More information on the Common Access Card can be found at **http:// www.dmdc.osd.mil/smartcard.**

A past of pride

May 21, 1927: Charles A. Lindbergh completed the first solo flight across Atlantic without any type of radio.

May 11, 1949: Berlin Airlift officially ended.

May 1, 1962: In response to the need for fixed rather than mobile comm in Southeast Asia, Air Force Communications Service activated the 1964th Communications Squadron at Tan Son Nhut, South Vietnam.

May 14, 1963: AFCS first became involved in the space program when the 2nd Mobile Communications Group deployed single sideband radio teams and equipment to seven African sites in support of the Project Mercury "Man in Space" program. AFCS members also participated in subsequent space programs such as Gemini and Apollo.

May 22, 1979: Air Force Satellite Communications System achieved initial operational capability.

The Air Force established a new era in long-haul communications when it activated the Automatic Digital Network. The AUTODIN network became fully operational in 1963. Here, a communications center specialist operates a UNIVAC 1004 AUTODIN computer.

Survey sent to improve civilian leadership development

By Staff Sgt. A.J. Bosker
Air Force Print News

WASHINGTON — A sampling of Air Force civilians in the grades of GS-12 through GS-15 have received and completed the civilian long-term training survey via e-mail in recent days.

The 12-question survey is an opportunity for people to express their thoughts or concerns about the civilian competitive development program, according to Bill Swigert, chief of civilian education and training at the Pentagon.

The CCDP, designed to meet the long-term civilian leadership needs of the Air Force, prepares selected civilians for increased responsibility and leadership, Swigert said.

It does so by offering highly qualified civilians the opportunity to attend in-residence professional military education, graduate-level programs in management and policy, and the Department of Defense executive leadership development program and excellence in government fellows program.

The Air Force does well matching civilians to these positions, but there are often too few nominees to select a pool of alternates, Swigert said.

"At times, we've had to leave some of these positions open when our primary has been unable to attend a course or program," he said. "This survey will help us identify our people's knowledge of the CCDP and whether any roadblocks exist that discourage more people from taking advantage of this great program."

A former CCDP participant himself, Swigert said the experience not only broadened his knowledge of the Air Force mission and history but also let him interact with military officers.

"It gave me a greater understanding and appreciation of (the military) component of the total force," he said.

Roger M. Blanchard, assistant deputy chief of staff for personnel at the Pentagon, said the survey will help ensure the continued effectiveness of the civilian competitive development program.

"Developing our future civilian leaders is critical to the Air Force," Blanchard said. "We're asking our people for their feedback (through the survey) to get a better understanding of their wants and needs to improve our force-development efforts."

SGLI premiums going down in July

By Army Sgt. 1st Class Doug Sample
American Forces Press Service

WASHINGTON (AFPN) – The Department of Veterans Affairs has announced that premiums for the Servicemembers Group Life Insurance will be reduced, handing military members a few extra dollars in their pockets each month.

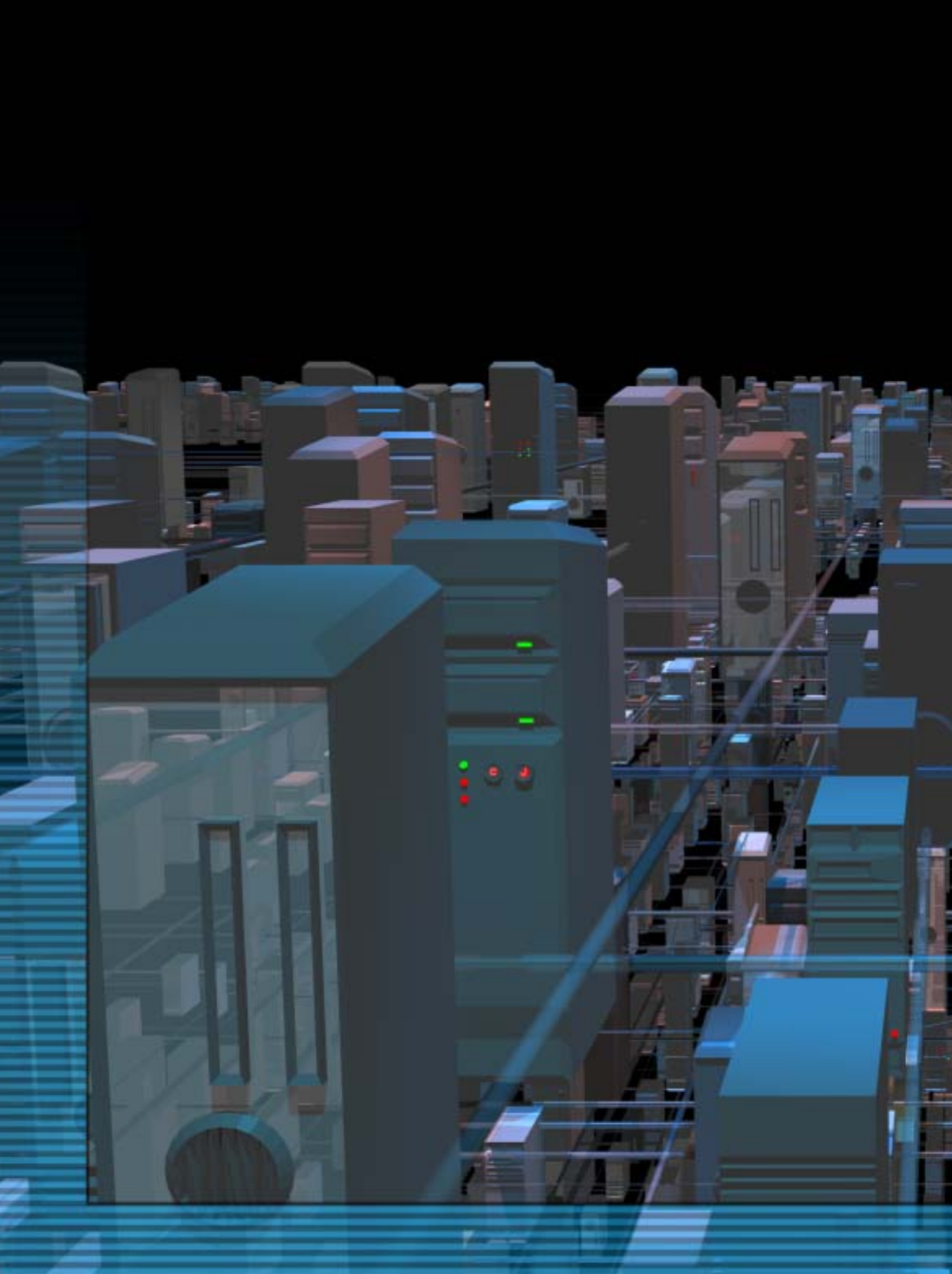
Beginning in July, the cost for a $250,000 policy – the maximum coverage – will drop from $20 to $16.25 monthly, a $3.75 savings. The Department of Veterans Affairs reports that rates for Veterans Group Life Insurance will not change.

Tom Tower, DOD's assistant director for military compensation, welcomed the reduced premiums, adding that anytime you put "more money in the pockets of military members, it's always a good result."

Premiums will also be reduced for SGLI family coverage, with rates varying among age groups.

The largest saving will go to spouses 35 to 39 years old, whose premiums will be nearly cut in half. Servicemembers currently pay $13 for a $100,000 family policy. That policy will cost $7.50 beginning in July – a $5.50 savings.

The reduced rates mean a military family will save an average of $100 a year. VA officials estimate that servicemembers collectively will save about $96 million annually in premiums, and $42 million in family coverage premiums each year.

Tower said the reduced premiums are a result of an ongoing process to keep costs down for military members.

Information about the change in SGLI premiums can be found at www.insurance.va.gov, or call the office of Servicemembers Group Life Insurance toll free at (800) 419-1473.