

intercom

*Journal of the Air Force
C4 Community*



***Comm and Info
is key to effectiveness
of space assets***



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. Charles F. "Chuck" Wald

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

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

Editorial Staff

AFCA Chief of Public Affairs
Lori Manske

Executive Editor
Len Barry

Editor
Tech. Sgt. Michael C. Leonard

Contributing Editor
Lt. Col. Laurie S. Healy
AFSPC/SCXB

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 35mm 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.

intercom can be found on the World Wide Web at <https://public.afca.scott.af.mil/intercom.htm>



AFSPC communications and information

AFSPC transforms space capabilities for 21st century Page 4

Air Force Space Command commander discusses the transformation and integration of space capabilities into the warfighter's tool set.

New radar first in AF to use off-the-shelf parts Page 6

The Galaxy 2000 tower display radar system went online at Vandenberg AFB, Calif., and will save the Air Force \$300,000 annually in manpower and repair costs, while simplifying work and helping maintainers and operators be more productive.

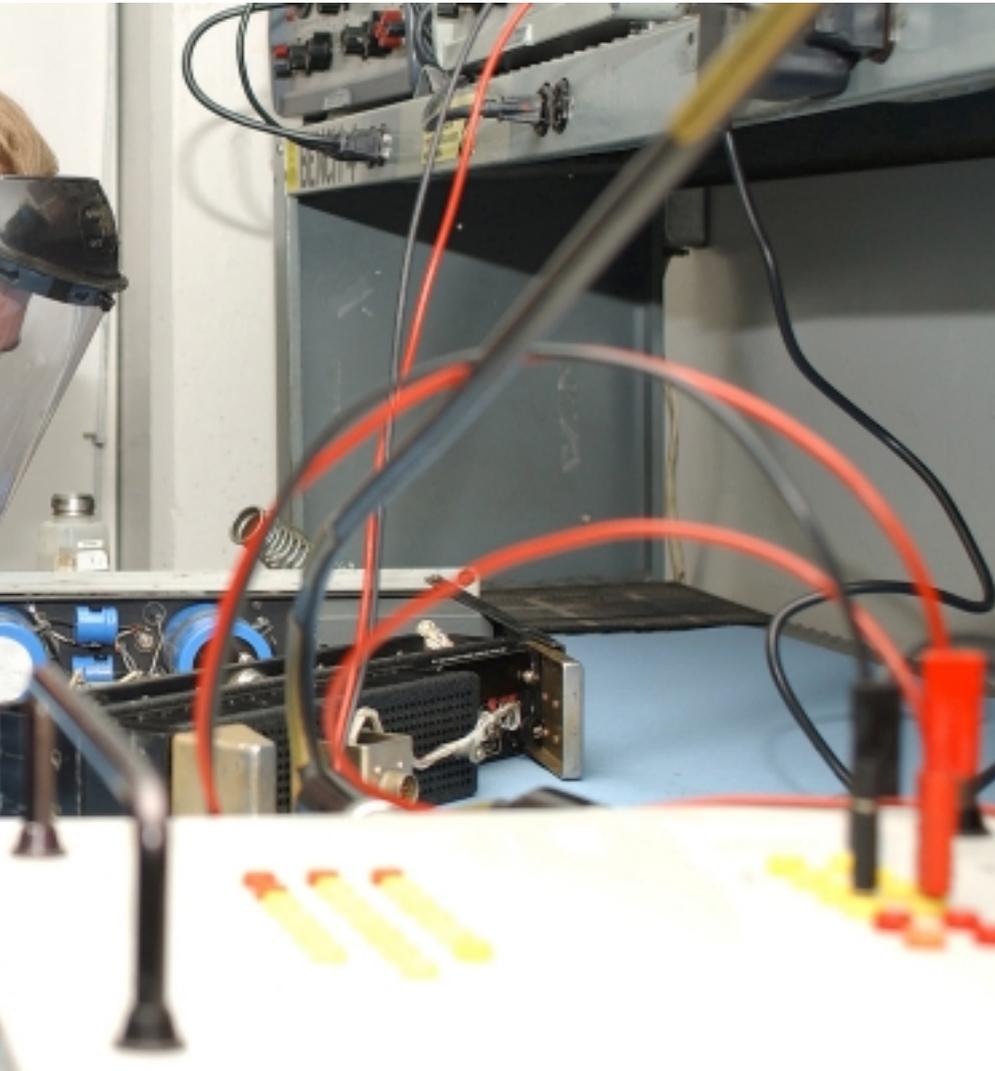
System pinpoints missile cable problems with electronic speed, accuracy Page 10

New system allows 90th CS to quickly locate problems in the buried missile cable for 220 intercontinental ballistic missile sites and alert facilities.

Missile comm maintenance:

It's a different world up here Page 16

Today, America's land-based leg of the nuclear triad is poised and



ready, thanks in part to the dedicated work of hundreds of communications maintenance professionals at the three remaining ICBM wings at F.E. Warren AFB, Wyo.; Minot AFB, N.D.; and Malmstrom AFB, Mont.

Information Assurance Campaign 2002

AFMC takes enterprise view of secure wireless networks Page 18

Network administrators make fundamental changes in deploying and managing wireless networks to help deal with several conflicting forces where wireless technologies are concerned.

AF needs you to defend enterprise network Page 20

While using IT to dominate the battlespace gives us advantages, it also creates vulnerabilities and we must ensure the network is ready and reliable.

AFIWC, AFCERT team up for common mission Page 22

Two agencies come together to detect and identify network intrusive activity and to help prevent adverse impacts on Air Force network operations.

Departments

in other news

AFCA conducts change of command ceremony Page 26

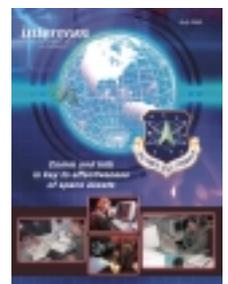
features

AFPCA keeps HQ AF connected Page 28

ECATS champions collaboration Page 30

On the cover

This month's cover focuses on Air Force Space Command's communications and information mission.



Cover by Lori Manske



Visit the Computer Based Training System Web site at <http://afcbt.den.disa.mil>

AFSPC transforms space capabilities for 21st century

By Gen. Lance W. Lord
Commander, Air Force Space
Command
Peterson AFB, Colo.

Transformation is sweeping the Department of Defense and our Air Force. When I took command of Air Force Space Command in April, we fulfilled the recommendation of the Space Commission to have its own commander, separate from NORAD and USSPACECOM. AFSPC is leading the Air Force in transforming and integrating our space capabilities into the

warfighter's tool set. Harnessing the capabilities of space assets, integrating them with current weapons systems, and creating new synergies are exciting tasks for all of us.

AFSPC has the same mission as any other major command – to train, organize and equip. But the Space Commission left us with no doubts that we must continue to transform the role of space in our Air Force. We'll work hard as a command to

“The road to space goes through Air Force Space Command. Central to this transformation is the role of communications and information. It’s a central pillar that every aspect of our space systems rests upon. It’s key to the effectiveness of our space assets.”

Gen. Lance W. Lord



every aspect of our space systems rests upon. It’s key to the effectiveness of our space assets.

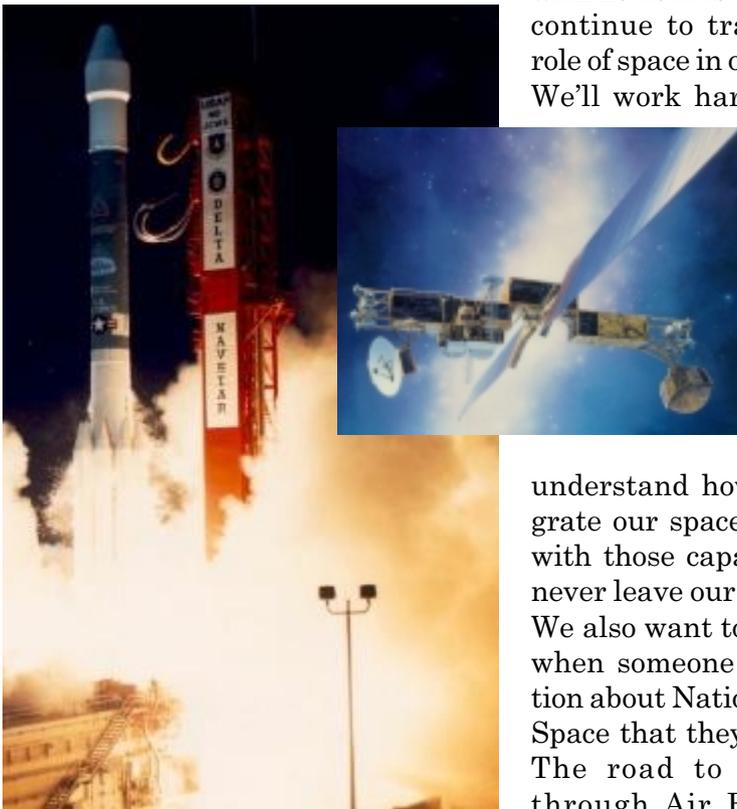
But transformation in communications and information is not just about moving data faster ... it’s much more than that. It’s about collecting information and putting it together in a usable format for the decision-maker. We can put in another circuit, expand our bandwidth, buy a faster computer, but if we don’t leverage our existing networks and communications capabilities and people, then explore the asymmetrical use and integration of state-of-the-art technologies, we’re not transforming anything ... just getting bits and bytes back and forth more efficiently. We must achieve an effect.

The bottom line is we’re in this business to provide deterrence and space capabilities for joint warfighters, so they can use them to create combined effects on the battlefield. This is what I call “componency.” Information is a crucial part of the “kill chain” – find, fix, target, track, engage,

m a k e sure we’re skilled in air, land and sea, and experts in space. We’ll also

understand how we’ll integrate our space capabilities with those capabilities that never leave our atmosphere. We also want to assure that when someone has a question about National Security Space that they come to us. The road to space goes through Air Force Space Command.

Central to this transformation is the role of communications and information. It’s a central pillar that ev-



Inset: the Navstar Global Positioning System. Above: The Delta II is an expendable launch, medium-lift vehicle primarily used to launch Navstar GPS satellites into orbit.

See AFSPC Page 7

Infostructure integration transforms communications

By Maj. Gen. Dale W. Meyerrose

*Director of Communications and Information
Air Force Space Command
Peterson AFB, Colo.*

Integration is the buzzword for this decade – “Integration of Air, Space and Information Assets” – “Integration of Air, Space and Information Operations” – “Integration of C2ISR.” General Jumper said recently, “I’ve talked about it (integration) before and I will talk about it again. We will get it right.” I support his assertion and we will get it right, but I’d like to elaborate in the context of “infostructure integration.” Let me start by making clear what I mean by infostructure. Infostructure is the complete set of computers, communications equipment, software, and related procedures, services, people, and other resources used in the acquisition, management, display, or interchange of data or information in any format supporting information technology or national security systems. Integration of our infostructure is my highest priority in supporting our warfighters, whether it’s in today’s war on terrorism or in providing for our homeland defense. In order for our infostructure to support network-centric warfare, we need some transformational thinking in terms of integration.

Integration of our infostructure is our national obligation. Integration is essential to ensure relevancy of the Transformational Communications Study, the Air Force’s Task Force Concepts of Operations, Homeland Defense, the deputy chief of staff for Warfighting Integration (HQ AF/XI), and the Space Commission recommendations. Each one of these key initiatives significantly affects infostructure – infostructure that needs to be integrated among organizations that provide for our national defense. This certainly means increased ops tempo for every communicator. It also means we must forge an iron link between infostructure and the operations that depend on it. Communicators must understand the missions their infostructure supports, almost as well as they understand the infostructure itself. Infostructure is absolutely essential for information superiority,



“Communicators must understand the missions their infostructure supports, almost as well as they understand the infostructure itself. Infostructure is absolutely essential for information superiority.”

*Maj. Gen. Dale W.
Meyerrose*

and when infostructure is disrupted the communicator must be able to describe the impact in mission terms that are consistent with the operator’s and customer’s lingo.

As communicators, we must engage with the entire Air Force in offering infostructure services to accommodate “effects-based” planning. These effects are the same operational effects targeteers talk about. So consider this planning chain: A theater warfighter tells the Air Force component that the desired effect is to eliminate the enemy’s air superiority in two days. Air planners come up with the options to achieve this effect through airpower. We, the communications community, must then come up with options to support these options to achieve this effect. The communicator’s contract with the operator shouldn’t be in terms of megahertz, but in terms of infostructure capabilities. This puts the onus on the “comm guys” to deliver that capability. We must think “capabilities-based,” “effects-based,” “transformational” and “integration.”

The true key to integration is to bring together all the pieces to provide unity throughout not just the Air Force but of all the DOD, federal and civil agencies involved in our national security. I assert there’s far more value in the sum of the parts than just the parts. Integrating the infostructure makes it easier to defend, easier to scale, easier to evolve, easier to manage, and easier to keep flexible. If all the parts are managed and coordinated as a complete whole, then communicators have the

See **INFOSTRUCTURE** Page 7

New radar first in AF to use off-the-shelf parts

By Staff Sgt. Andrew Leonhard
30th Space Wing Public Affairs
Vandenberg AFB, Calif.

Maintainers and operators of Vandenberg AFB's 30th Communications Squadron and members of its 30th Operations Support Squadron are now die-hard Galaxy gazers. The Galaxy 2000 tower display radar system, the only off-the-shelf radar system maintained by the military, went online after more than six months of operational testing.

The new radar will save the base more than \$300,000 annually in manpower and repair costs, while simplifying work and helping maintainers and operators be more productive.

A big improvement for maintainers is the ability to monitor, troubleshoot and train from a remote site without downtime to the primary Galaxy system, said Master Sgt. Richard Chavez-Hatton, 30th CS NCO-in-charge of ground radar systems.

Maintainers hold a 99.8 percent uptime rate – the best in the military with the older GPN-12 radar system replaced by the Galaxy 2000.

Air traffic controllers also benefit from the new system. "We now have a flat-screen color monitor that can receive multiple radar feeds at one time," said Master Sgt. Richard Czap, 30th OSS chief controller. The GPN-12 had one radar and one display.

The Galaxy 2000 gives operators multiple feeds from separate radar sites along the central coast. Its coverage extends to 800 nautical miles, compared to 60 with the older system.

The Galaxy also uses next-generation weather radar information, to give pilots real-time adverse weather advisories, said Sergeant Czap.

"We're the first Air Force base to install this off-the-shelf technology," Sergeant Czap said. "It's reliable and will reduce operations costs."

The GPN-12 shut down in August, after 19



Photo By Senior Airman Jeanette Copeland

Members of the 30th CS, ground radar systems flight, dismantle the old GPN-12 radar site. The GPN-12 radar was replaced with the first off-the-shelf Galaxy 2000 tower display maintained by the military.

years of service, making the Galaxy the base's primary radar system. Only nine GPN systems are left in the Department of Defense inventory.

Parts will be sent to Tinker AFB, Okla., to be refurbished and reused for existing GPN-12 systems. One critical element will be transferred to Soto Cano, Honduras, to support anti-drug operations.

INFOSTRUCTURE

From Page 5

flexibility they need to accomplish effects-based planning. As operational missions change, the manager has a larger trade space to quickly accommodate the change. If something goes wrong, those responsible for network operations and C2 have a larger trade space of resources to reallocate in a way that minimizes overall impact. When an operational surge occurs, it's more likely that enough reserve is available without putting any one customer at risk. These principles are key to the success of integration.

In Air Force Space Command, we're forging ahead in application of these integration principles. The Space Commission was the catalyst as it mandated better integration. The resultant Air Force Program Action Directive 1-04 gave Air Force Space Command's director of Communications and Information the mandate to ensure cross-program integration for the purpose of improving interoperability and efficiency. We call this activity the "single comm integrator" for space systems. Since the Air Force is now DOD's executive agent for space, the single comm integrator responsibility reaches beyond Air Force Space Command. The single comm integrator is



off to a high impact start by forging synergistic relations with other large space organizations, like the National Reconnaissance Office. We're building roadmaps that melt long-standing stovepipes on our launch bases. We're making sure new space systems have a common infostructure along the Rocky Mountain corridor. We're also partnering with Air Force Space Command Space and Missile Center to influence new space systems like the space-based radar. As a result, new systems will come out of the chute as "infostructure-enabled."

All of the principles being actualized by the single comm integrator are applicable to the Air Force at large. The integration mandate must be institutionalized. We can no longer deal with individual efforts and stovepipes, but rather a united, transformational infostructure that brings together all our capabilities. Infostructure processes must be woven into the processes within each MAJCOM, and a disciplined integration process is the enabler. At the Air Staff level, we see this in establishment of HQ AF/XI.

We as military leaders are up to the challenge. Infostructure integration brings together a powerhouse of capabilities that will ensure information superiority and decision dominance for America.

AFSPC

From Page 4

assess. We may be very good at separating and translating data into information ... but there's still another step – an action step. The warfighter needs to know how to use that information to engage and kill targets.

One of the true airpower pioneers, Billy Mitchell, told us that in the development of air power, you've got to look ahead. It's a great start ... look where it brought us. But it's simply not enough. We need to step boldly forward and seek to shape and influence the future. While this "transforming" might be harder than if we try to react to what

happens, I'm convinced the rewards are more lasting and our work will result in a better set of capabilities for the future.

The Air Force, as the Department of Defense's executive agent for space, has been given an enormous responsibility. We must transform our partnerships with others in the space business, and work closely with other services, contractors and agencies. Together we'll transform the warfighter's capabilities.

There's no doubt that space is one of the key enablers of military operations in the 21st century. Our forces are providing support 24/7/365 with capabilities that were developed during the Cold War, demonstrated on

the battlefields of Iraq and Kosovo, and have "come of age" in Afghanistan. The men and women of AFSPC are eager to move forward during this exciting time in the history of our great nation. Our transformation is far from complete, but we're making great strides in our pursuit of the leading edge. While I know we've got technical challenges to overcome, they aren't our biggest challenge. Our biggest challenge is unleashing the rich human potential that we already have in our organizations. AFSPC warriors are energized and focused, and shaping the future. Remember, "If you're not in Space, you're not in the race!"





Photos by Jodie Lockard, 50th CS

Personnel from 50th Security Forces Squadron, 50th Civil Engineer Squadron and the 50th Communications Group confer at an on-scene location.

Schriever upgrades land mobile radios

By **Capt. Ronojit Nathaniel**
Chief, Strategic Plans and Policy
850th Communications Squadron
Schriever AFB, Colo.

Long before Sept. 11, plans were already under way to upgrade the Schriever AFB land mobile radio system. Col. David B. Warner, 50th Communications Group commander, made it a strategic priority for the group to “assure command and control of space assets by providing effective and efficient communications and information systems.” He charged us to equip our warfighters with the best possible LMR solution. Additionally, the National Telecommunications and Information Administration mandated migration to narrowband technology for the LMR frequency bands most commonly used by the Air Force. This meant existing 138-150 MHz systems were to come into compliance by 2008, and initially the upgrade was scheduled to kickoff in FY 2003.

Sept. 11 changed all that. As a critical factor in protection of the Air Force Satellite Control Network and other Air Force Space Command assets at Schriever, the LMR upgrade program gained new momentum. Driving factors included: outdated equipment with limiting infrastructure, topographical obscura, interoperability issues with local county government agencies, and finally – funding the upgrade.

In July 2001, a LMR action team headed by the 850th Communications Squadron was formed with 50th Space Wing members representing the security forces squadron, fire department, civil engineer readiness flight, wing operations center, emergency medical response team, and the Joint National Integration Center. They joined forces with our program management office, 50th Communications Group resource advisors and 50th Contracting Squadron representatives. They met monthly to define, analyze and review requirements.

Galvanized after the 9-11 attacks, this multi-disciplinary team led by highly motivated communicators hammered out technical requirements and a timeline for the new system within a month. Guiding forces included an intelligent and flexible system design, interoperability with other military, government and civilian counterparts, future expandability, and a substantial return on investment.

Requirements survey results were reviewed by our resource advisor, LMR manager, and wing frequency manager, and costed out by the contracting squadron for competitive pricing and bidding, with a comparative analysis conducted for best value. After considering several options, including the General Services Administration, previous contractors and other vendors, it was determined that a joint venture with Motorola and TekStar, Inc., was the best choice. Motorola will provide project management in coordination with the 850th Communications Squadron. The Motorola and TSI team immediately conducted a site survey and made recommendations for facilitating the upgrade. In January, key players met at Motorola's facility in Hanover, Md., to review the proposed system hands-on. This allowed them to actually operate the proposed system and inspect the infrastructure parts list for completeness and accuracy. By mid-February, the site support specifications were finalized, and a system design



From left: LMR users include Airman 1st Class Eric Masur, 50th Civil Engineer Squadron; Senior Airman Mandy Seaba, 810th Medical Group; and Tech. Sgt. Jim Tate, 50th Security Forces.

analysis with a final proposal was delivered.

After reviewing the system design analysis, we pressed forward to a fully functional upgraded system last month. We will tie into the local military trunking system through Fort Carson switch to allow ample coverage for Schriever personnel as they travel through the Front Range Military District, which includes Fort Carson, Cheyenne Mountain Complex, Air Force Academy, Peterson AFB and Schriever. This 800 MHz system will provide seamless integration and interoperability with local government and civilian emergency agencies. The system will also provide over-the-air re-keying and "bulletproof" compliance with DOD encryption standards. The OTAR feature will allow handsets to be re-keyed in the field, potentially saving thousands of man-hours over the life of the system.

This upgrade will also bring us into compliance with NTIA mandates three years ahead of schedule. The new system will provide a solid foundation for force protection and homeland defense. A parallel initiative at the New Boston Remote Tracking Station site is already up and running with great success. Col. Larry James, 50th Space Wing commander, said, "Our entire wing team did a superb job in responding to the critical demand for upgraded communications that the LMRs provide. Because of their efforts, we're well on our way to fielding a state-of-the-art system that will ensure superb force protection and response well into the future."



From left: Staff Sgt. Nathan Beggs, William Smith and Capt. Ronojit Nathaniel, are LMR team members.

System pinpoints missile cable problems with electronic speed, accuracy

By 2nd Lt. Jonathan H. Swyers
and Scott Jones
90th Communications Squadron
F.E. Warren AFB, Wyo.

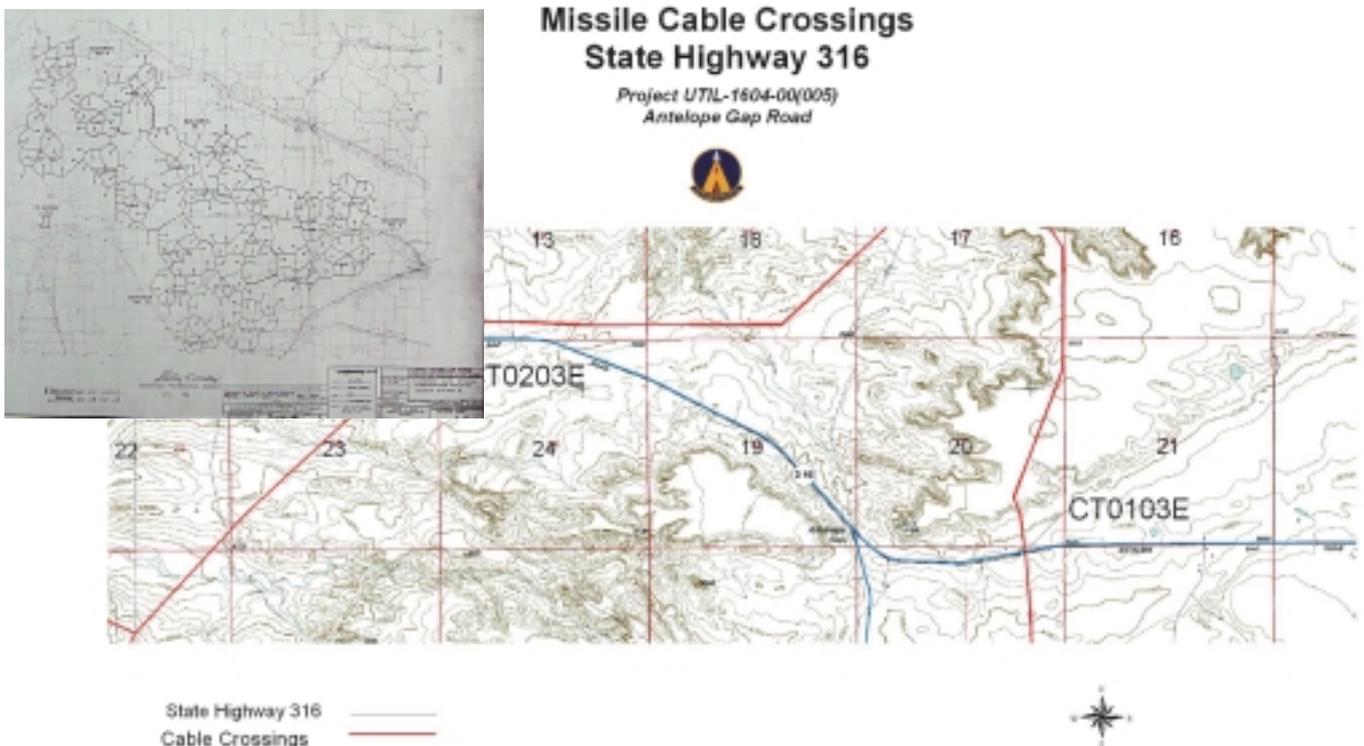
Scattered in eight counties throughout Wyoming, Nebraska and Colorado are 220 intercontinental ballistic missile sites and alert facilities of the 90th Space Wing, the world's most powerful ICBM force. Connecting the sites for operational control is a buried cable network called the hardened intersite cable system, or HICS, which is maintained by the 90th Communications Squadron. These critical lines of communication ensure the missiles are 100 percent combat ready for defense of our country.

HICS is a pressurized system consisting of 2,194 miles of cable with more than 4,000 splices. Communications system installation records required to support maintenance included 460 pa-

per maps, 4,665 circuit cards, and volumes of plant in-place records. Under these conditions, the 90th CS recognized some problems and resolved to improve the system. Having to pull together field maintenance information was time-consuming, and 30-year-old maps, often flawed, led to some confusion. So the squadron embarked on a project to convert this information to an electronic form. This project is the HICS geographical information system, or HICS GIS.

The process began with HICS maintenance crew members using all-terrain vehicles to install Trimble global positioning system survey equipment. GPS pinpointed locations of the cable and significant features such as splices, fence lines, utilities and missile sites. The squadron's cable affairs office converted field data to a manageable format, and stored it in a local file server dedicated to the large GIS database.

Overall maintenance usefulness of HICS GIS



The map for a state highway upgrade project locates missile cables to help construction engineers avoid them. Workers may also call the 90th CS for assistance. Inset photo: Example of earlier missile map.

Buckley AFB looks to a promising future

By Lt. Col. Kim M. Johnson

*Commander, 460th Communications Squadron
Buckley AFB, Colo.*

Buckley became the Air Force's newest base in October 2000 – and just one year later, home to its newest wing, the 460th Air Base Wing. With activation of the 460th, and Air Force Space Command taking over host responsibility from the Colorado Air National Guard's 140th Wing, the base has undergone many changes. One initiative was activation of the 460th Communications Squadron, which was given the rare opportunity in today's Air Force to build a communications infrastructure from the ground up.

Over the next seven years, Buckley will complete more than \$125 million in military construction projects including two new dormitories, a medium-sized gym, an air base wing headquarters, and a new communications facility. As a new comm squadron, with a new base operating support mission, the unit faces tasks that are large, but not insurmountable.

The first challenge was to transfer 116 Colorado ANG civilian employees to active duty positions under AFSPC, and to incorporate 14 of those positions into the squadron.

Not so long ago, the Air Force local area network at Buckley was spread over five small buildings and was centrally managed from a small room. Today, the BuckNet LAN supports more than 1,800 users and can be found all over base, as well as in the hospital in Aurora, Colo., and at the Interim Mission Control Station-Backup at Boulder, Colo. Planning has begun for the information technology infrastructure Combat Information Transport System, which should be installed by February. CITS will increase BuckNet's reliability and maintainability, and provide redundancy within the system. Network Management System/Base Information Protection was installed in Buckley's network control center, providing the highest available degree of information protection.

The 460th CS has the new mission of adding an inside plant (i.e., internal wiring within buildings). CITS ensures all ANG and active duty buildings will be ready. The project should be complete by December.



From left: Lt. Col. Kim M. Johnson, 460th Comm Squadron commander; Col. Leslie W. Brockman, 460th Support Group commander; and Bill Cubbage, General Dynamics team leader, break ground for CITS.

Multimedia at Buckley is a huge success. Spending more than \$500,000, the visual information team created a state-of-the-art work center. Their first major project was documenting the 460th ABW activation ceremony. Five technicians toting digital cameras photographed and videotaped the event. They created numerous posters for wing events and provided a highly praised slide presentation for the annual wing awards ceremony. Their latest project includes helping to design and create several squadron emblems.

The next challenge was to establish the information management section. The first hurdle was to give the base's 26 tenant organizations information about services, and guidance for creating publications and forms for the active duty organizations. A new records staging area was estab-

lished, completing the requirements for a base destruction capability. Working various issues with the U.S. Postal Service was a “learn as you go” process. We now provide general delivery, as well as mail service to the dormitory residents, and more than 6,200 active duty 460th ABW and tenant personnel.

Another new addition to the comm squadron was the air traffic control and landing systems maintenance shop, including five civilians transferred from the ANG comm flight. While jobs remain unchanged, maintaining the ATCALs along the runway, and purchasing ATCALs equipment remain a challenge. The new inter-service support agreement will help spell out these issues for all concerned.

Personal wireless communications, including frequency management, has faced numerous demands. It was relatively easy to provide enough land mobile radios, cellular phones and pagers to newly generated readiness and disaster control groups, new law enforcement personnel and commanders. However, designing a new trunked land mobile radio system for Buckley was another matter. This initiative will attach Buckley to a 19-channel UHF narrowband digital wide area radio network with encryption capability. AFSPC provided the needed \$400,000 for infrastructure, along with \$1.8 million for various radios and equipment. This will give Buckley personnel the ability to use a LMR in the metro Denver and Aurora areas. As the trunked system potentially expands throughout the state, capability for all trunked users could eventually stretch from F.E. Warren AFB, Wyo., to Pueblo, Colo.

Obtaining and maintaining correct frequencies for base users is another challenge. Frequency issues often pop up, potentially impacting the missions of tenant organizations.

One thing remains constant: 460th Comm Squadron maintenance of the Defense Support Program missile warning legacy system. The Space-based Infrared System will soon replace DSP, and maintaining the legacy system places a high demand on supply and maintenance technicians. All training must be completed in-house by Air Force Engineering and Technical Service personnel, since “school-house” training shut down in 1999. While contractors complete SBIRS maintenance, the comm squadron continues to maintain



Staff Sgt. Stewart Thoue examines new NCC equipment.

circuit actions associated with the system, as well as other actions.

The future of Buckley and the 460th CS is bright, with many new challenges on the horizon. The 460th CS’s relationship with the ANG’s 140th Communications Flight continues to blossom. For the most part, it’s the same job with the same regulations and similar equipment, making collaboration easy. The future holds consolidation of our networks and planning functions. With the expanse of new buildings being constructed through active duty MILCON and ANG, there is plenty of communications planning ahead.

The services division and comm squadron have a primary goal of providing the best possible communications services for the projected visiting quarters and temporary lodging facility.

Increasing bandwidth across the base, with Defense Information Systems Agency assistance, will fully employ the planned switch room. Planning has begun for purchase and movement of the telephone switch. The 460th CS is also reviewing feasibility of moving systems control into the new communications facility, or keeping it in the restricted area with mission systems.

These are only a few of the 460th CS’s upcoming projects. If you want to see a base take shape before your eyes, Buckley’s the place to be. It requires a lot of hard work, planning and flexibility to complete these new multimillion-dollar projects.

As the evolution unfolds, the 460th CS will continue to do its part to keep Buckley on course and fully equipped with the most reliable, available, secure and authentic communications possible. What a future!

Schriever consolidated NCC: *One Wing ... One Network*

By **Capt. Francisco R. Gonzalez, Jr.**
OIC, Network Operations
50th Communications Squadron
Schriever AFB, Colo.

"50th Space Wing NCC, this is Jim. How may I direct your call?" And so goes a typical day for Jim Ponders, head of maintenance control for Schriever AFB. In fact, Ponders and his crew repeat this statement about 300 times every day. Why? In December, the 50th Communications Squadron brought to final operating capacity the Schriever AFB Consolidated Network Control Center, and maintenance control is one of the eight vital functions making up the NCC.

Serving as a "one-stop shop" for customer support and circuit management for the 50th Space Wing, the NCC does what no one else in the Air Force has done before: It brings command and control of administrative base-level and mission-critical satellite communications networks together in a centralized location. Now customers at every level can call one phone number to get a fix action initiated, or to check the status of all communications problems affecting Schriever and geographically-separated units.

Standing up an NCC is no easy task. It's even harder when you're breaking new ground. Culminating a year-long effort of more than 35 people, Schriever's consolidated NCC combined eight work centers into one cohesive unit. "There were challenges," said Richard Evers, 50th CS Information Systems Flight chief. After all, how do you bring diverse people and missions together and make a team able to handle any comm problem? Even harder, how do you do something that no one has done before? The answer came from 2nd Lts. Mark Slik, Richard Gayle and Mark Sullivan. Spearheading a crash course in program management, the lieutenants transformed the NCC from concept to reality. "I'm fortunate to have these motivated and talented ACE lieutenants," said Lt. Col. Lisa Tucker, 50th Communications Squadron com-

mander. "I gave them the ball, and they ran with it."

The first order of business for the lieutenants was to research the wealth of documentation and Air Force Instructions on conducting NCC operations in relation to administrative network communications. There was no such wealth on handling mission satellite communications. Knowing there was a knowledge deficit, the three consulted everyone they could find with experience on handling mission communications. After the dust settled, they developed initial training plans, checklists and procedures for effective C2 of mission assets. Finally, they took all the plans and began selling and teaching each of the contractor, civilian and enlisted personnel charged with implementing the vision, and formed the group into a cohesive team.

Then we faced our biggest challenge: getting out the word.

Col. David Warner, 50th Communications Group commander, attends early-morning meetings on the health and wellness of his communications services, performs a daily vector check, and without fail, talks about the NCC. "We're the hub, the focal point for the wing commander and the entire 50th Space Wing," Colonel Warner said. But the NCC can't be effective if others aren't aware and involved, so Colonel Warner ensures the word gets out. His salesmanship with fellow group commanders, wing staff and higher headquarters, catalyzed rewriting of base operating instructions, from 10 series to 33 series, to reflect the NCC's new capability. According to Air Force Space Command, Schriever is setting the pace for the communications community. Referring to the help desk, job control and mission communications consolidation, Maj. Gen. Dale W. Meyerrose, director of Communications and Information for Air Force Space Command, said on a recent visit, "You're the first ones to get it right."

Though the NCC is still in its infancy, every

The 50th Space Wing's NCC does what no one else in the Air Force has done before: it brings command and control of administrative base-level and mission-critical satellite communications networks together in a centralized location.

See **SCHRIEVER** Page 17

July 2002

DMZ connects Kennedy and Patrick LANs

By Dennis Thompson
45th Communications Squadron
Patrick AFB, Fla.

The 45th Space Wing and National Aeronautics and Space Administration pooled their resources and let a joint contract in 1998 for all base operating support for Kennedy Space Center and Cape Canaveral Air Force Station. The program posed the challenge of providing network connectivity for joint base operating support contract personnel, who sat between two large local area networks with two different philosophies of network security. The joint program management office overseeing JBOSC was made up of both Air Force and NASA people working in Air Force facilities at Patrick AFB and CCAFS. They were connected as clients to the Air Force network, but needed access to systems on the NASA KSC network to perform their duties. It would have been costly to install a parallel network in the facilities for these individuals to access their systems.

The 45th SW and NASA tasked the logistics group and JPMO to design and implement a cost-effective solution for providing connectivity to support the Eastern Range, while protecting the integrity of Air Force and NASA networks. A tiger team led by Dennis Thompson, 45th Communications Squadron network control center, was formed to design the solution. Team members included Glenn Exline and Monica Lombardo, of Computer Sciences Raytheon, and others from NASA and Space Gateway Support. The team's challenge was to determine how to connect two agencies, Air Force and NASA, with different degrees of network security requirements, while maintaining the security posture required of all Air Force networks.

The team designed and implemented a network demilitarized zone on the perimeter of the 45th SW LAN/MAN. Based on the Air Force Barrier Reef architecture, the DMZ employed two firewalls to provide protection. One was external to the DMZ and the other was internal and resided on the perimeter of the base network. The clients that resided in the DMZ were afforded connectivity to their assets through ports opened at the external

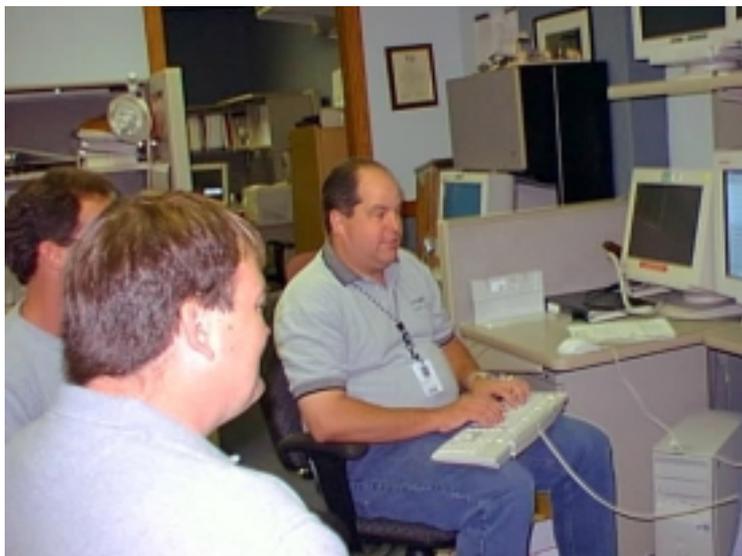


Photo by Carol Countryman, Patrick AFB, NCC

Patrick AFB local area network managers discuss the DMZ and associated security topology with Dennis Thompson, center, NCC chief.

firewall. The internal firewall ports remained closed to provide continued protection for 45th SW assets from hackers and intrusions by outside agencies.

Thompson said, "The DMZ gives customers connectivity to resources in other network environments that are required to perform day-to-day mission support for the government." The customer base can range from contractors to other government agencies that are not part of the 45th SW. Information security provided by the DMZ protects assets of the Air Force and other organizations connected through it. DMZ deployment is based on network security directives and instructions of all entities using its services. While each organization is responsible for daily maintenance of its clients residing within the DMZ, the NCC provides oversight management of the network supporting these clients. Vulnerability scans are run monthly to ensure the systems don't introduce any security problems to themselves or the systems they access.

The DMZ has proven its worth in providing critical network security for the 45th SW. It affords connectivity, while assuring protection of resources of all agencies involved in the multi-faceted environment of the Eastern Range.



Airman 1st Class Casey R. Sheeham, STRATCOM maintenance center, works on launch facility support information networks.

Missile comm maintenance:

It's a different world ...up ...here

By Senior Master Sgt. Dwight B. Holmes
341st Communications Squadron
Malmstrom AFB, Mont.

Almost 40 years have passed since President Kennedy announced America had an “ace in the hole” during the Cuban Missile Crisis of October 1962. Great effort was put into readying the 10th Missile Squadron’s Minuteman I for possible launch, and communications professionals played a vital role in that effort. The operational system at Malmstrom AFB was a significant deterrent, helping to maintain our nation’s security and preventing an attack that could have escalated into nuclear war.

Today, America’s land-based leg of our nuclear triad is still poised and ready, thanks in part to the dedicated work of hundreds of communications maintenance professionals at the three remaining ICBM wings at F.E. Warren AFB, Wyo.; Minot AFB, N.D.; and Malmstrom. The missile fields provide a nuclear deterrent 24 hours a day, seven days a week, but they couldn’t do the job without command and control systems. If emergency action messages don’t reach the control crew’s capsule, or launch signals don’t make it to the missile silos, the missiles will not launch.

Keeping missile command and control systems operational takes a tremendous effort from extremely dedicated airmen and civilian profession-

als at all levels. They maintain a variety of systems, from radio and satellite, to telephone and more than 2,400 miles of hardened command and control cables. Keeping these systems operating at optimum levels is hard work, especially when you consider the operating location, weather, safety and training factors.

Maintaining robust communications links between the National Command Authorities, missile alert facilities, and launch facilities is no small task, given the vast geographical separation of assets and the less than perfect terrain encountered at U.S. northern tier bases. Malmstrom's missile field covers 23,500 square miles, requiring communications maintainers to travel tens of thousands of miles each year to perform scheduled and unscheduled maintenance, ensuring the integrity and availability of critical nuclear command and control links.

Compounding travel problems is extreme winter weather. Below-zero temperatures, fog, "white-out" snow conditions and 60-plus mph winds are some of the hazards that must be endured to keep our C2 systems operational. Overcoming these factors is only possible with concerted emphasis on safety.

At Malmstrom, safety is "job one" and our communications personnel have handled "the largest missile field in America" with an unsurpassed safety record. The 341st Comm Squadron has not had a reportable vehicle safety mishap in over two years, despite routinely traveling up to six hours a day to maintain the C2 systems. Safety and geographical separation aren't the only challenges our personnel encounter – training is another.

There have been many C2 sys-

tem upgrades over the past 40 years, but most are still manually-intensive. Our 2EXXX maintainers spend most of their time in the field troubleshooting faulty systems, or back at the base on the workbench with circuit testers and soldering irons repairing the equipment. Now that's real maintenance! In addition, a majority of the communications systems are unique to the missile communications business, and require extensive training time for maintainers to become fully qualified. We've implemented rigorous training schedules for all of our work centers in order to ensure 100 percent coverage for all maintenance tasks. By keeping focused on the operational mission and sticking to the training schedule, we guarantee our hard-working technicians are prepared to meet any challenge.

Given all these factors, the job still gets done and done very well. We deliver the "Best ICBM Communications Maintenance in the Air Force" with unparalleled success. The dedication and pride of the communications maintenance teams is evident when you look at our metrics. Uptime rates for missile communications systems at Malmstrom averaged 99.75 percent last year. The continuous evaluation program tests missile communications systems' ability to receive EAM traffic over several platforms – last year, Malmstrom's average reception rate was 97 percent, exceeding the Air Force Space Command average by more than 3 percent, and giving testimony to the legacy of professionalism displayed over the past 40 years. From the first "ace in the hole" to the present, our motto is still, "No Comm – No Bomb!"



SCHRIEVER

From Page 14

day new procedures are developed, new tools are implemented, checklists are modified, and relationships are built.

A recent addition is the Mission Problem Report Web page, which is unclassified and provides a complete communications site picture for the wing commander, Col. Larry James, and his key leaders.

Colonel James has a comprehensive review of his communications weapon system's status on his computer in a stop-light chart format. This page is also broadcast to Peterson AFB, giving its network operations security center complete visibility into the health and wellness of 50th Space Wing assets.

This real-time knowledge helps leaders make informed, timely mission-related decisions. Coupled with the NCC construct, this tool makes the *One Wing ... One Network* concept a reality, and helps move the Air Force a step closer to achieving its vision of *One Air Force ... One Network*.

AFMC takes enterprise view of secure wireless networks

By Corey Young

Directorate of Communications and Information
Air Force Materiel Command
Wright-Patterson AFB, Ohio

A squadron commander leaving the headquarters building reaches into her pocket to retrieve her wireless-enabled palm computer. The new data roll-up capabilities of the Air Force Portal have gathered information from dozens of automated information systems and compiled it for her into a single mission-readiness snapshot. Having just reviewed this snapshot as she heads for the flight line, the commander prepares to drill down into the details as she meets with her maintenance staff.

But in the hangar, her palm computer displays a communications error. Looking up, she spots a wireless access point mounted on a support beam, with its green light on – so she’s clearly in range. The flight line crew’s handhelds are working, but still she gets no signal.

This scenario and others like it play out often throughout the Air Force, as wireless networking becomes more common. The problem is that the *One Air Force ... One Network* message is only now starting to reach the wireless environment.

Currently, Air Force network administrators face several conflicting forces where wireless technologies are concerned. The logistics, medical and flight line communities are understandably embracing wireless applications as force multipliers. Meanwhile, Information Assurance experts and information technology trade magazines continue to warn of vulnerability to hackers. The communications squadron staff, already spread thin and engaged in a continuous battle to maintain security of their wired network, is now being asked to secure and maintain a growing number of wireless devices. Finally, while not yet a requirement in most environments, the ability to roam while connected is crucial as Air Force customers strive to reduce their “degrees of separation.”

To satisfy all of these interests, network administrators are forced to make some fundamen-

tal changes in the way wireless networks are deployed and managed. An enterprise approach is warranted, with the following considerations.

Treat wireless networking components as part of the infrastructure. Too often, wireless segments are deployed, and subsequently treated, as part of a specific wireless application. Security of the wireless components is managed by the application owner, if at all. Taking an enterprise approach, as with conventional network applications, the connectivity between the server and its clients should be provided by the centralized IT organization.

Centralize control of the wired side of wireless. Between every wireless client and the trusted network is an access point. These access points must be centrally controlled to ensure that they don’t provide unauthorized users direct access to the trusted network. Look for devices and software which allow centralized, secure and remote administration of components.

Leverage standards. Avoid proprietary devices, protocols and clients. Similarly, pass up products that blur network layers. The number of wireless clients will grow significantly, so avoid getting locked into one solution.

Establish a device registration process. Access points should only communicate with authorized devices. The process by which a wireless device becomes authorized should be similar to the current process used to grant desktop PCs access to the network. Registration might include recording the device’s MAC address and installing any required VPN or antivirus software.

Allow for roaming. Roaming, the ability to move from one wireless enclave to another, isn’t currently listed as a requirement for many wireless systems, but it soon will be. When considering any hardware or software purchase, remember the commander in the opening example. The systems described are typical, they work well in their established enclaves, but they don’t allow visitors, even from the same trusted domain.

See **WIRELESS** next page

'Virtual network' protects information

By Stephen Scherr
*Deputy Chief Information Officer
Air Force Research Laboratory
Wright-Patterson AFB, Ohio*

In our personal life, when we use the telephone or send a letter through the mail, we have a certain expectation of privacy. No one may intercept our call or open our letter without our permission, or a court order. In the Air Force work place, we don't necessarily have that expectation. We know first class mail may be opened, and telephone calls monitored, because the information we deal with every day is sensitive and must be protected.

In our work and on our computers, we deal with many different kinds of sensitive information, such as Privacy Act, acquisition-sensitive, planning and budgetary, logistics, and information proprietary to one of our industrial partners, not to mention data related to weapons systems and military operations. Even though classified information isn't on our unclassified computers and networks, our local operations security professional will confirm there's plenty of unclassified information that can be gathered to deduce something that's classified. To guard against eavesdropping or interception of data traveling between computers on the Air Force enterprise network, DOD regulations and Air Force instructions require that sensitive information be encrypted.

Last year, since most unclassified network traffic, including everyday e-mail, wasn't being encrypted, the Air Force Network Operations Center implemented the common user virtual private network to protect information on the Air Force enterprise network. CU VPN encrypts information transmitted on the Internet to assure it remains "private." In effect, VPN provides a private line between users, creating a "virtual network."

VPN is used to restrict access to information to a particular set of users. Examples include communications between users within an organization, or between a system program office and its prime contractor. The CU VPN protects the entire Air Force enterprise network by encrypting all network traffic for all users between all bases. That's why it's called the common user VPN.

This system puts us, as Air Force network users, in good shape. We protect each of our bases, follow the rules for protecting information within a base, and any information we send from base to base is automatically protected while in transit. Examples of covered data include e-mail, Web access to personnel records (encrypted a second time with the https protocol), and transmittal of logistics or financial data to older "legacy" systems.

Now for the fine print. Even though the CU VPN automatically protects information, you still need to think before sending it off base. While the system safeguards data within the Air Force enterprise network, e-mail and other connections outside af.mil are not protected all the way to the destination. Special networks, like the hospital network or the DREN, are not included, but they are protected in other ways. Coverage doesn't extend to personnel at detachments outside Air Force bases. And since the Army runs the Pentagon network, the initial deployment of CU VPN doesn't currently encrypt data sent there from Air Force bases, although the AFNOC is working to incorporate Pentagon offices into the system.

The common user virtual private network protects e-mail, Web and other communications throughout the Air Force enterprise network, helping to assure secure and effective command, control, communications and information support for the entire Air Force community.

WIRELESS

From previous page

Ensure compliance. Perform periodic, unannounced scans to locate rogue access points. This includes "war-driving" exercises in which network support personnel use a mobile

scanning system to locate unauthorized access points. Though not currently as effective, scans can also be performed "on the wire" to detect wireless connections.

The ultimate goal is to provide a secure, manageable wireless infrastructure as a seamless

element of the overall network enterprise. These few strategic steps taken now, during early implementation, will pay large dividends in maintaining network security and customer satisfaction with wireless applications.

AF needs you to defend enterprise network

By **Kenneth Percell**

*Director of Communications
and Information*

*Air Force Materiel Command
Wright-Patterson AFB, Ohio*

The Air Force is doing more with fewer people than we ever imagined. Much of this is made possible by exploiting information and technology to increase our combat effectiveness and daily mission performance. We'll continue to improve our combat power by infusing information technology into our weapon systems, and our command and control, and support infrastructures. However, while using IT to dominate the battlespace gives us advantages, it also creates vulnerabilities. Our adversaries will use cyber attacks to bolster their warfighting capabilities. They'll do this by attacking our networks from anywhere in the world, and at any time, to slow or disrupt mobilization, deployment, re-supply and operations of U.S. military forces.

This year's Information As-

urance campaign theme, "Defeating Global Terror ... Demands Effective Information Assurance," reflects the nature of the new war we face. We have new adversaries with new targets and tactics. Cyberspace has become a battlefield, and we're the Air Force enterprise network defenders. Military victories won with weapons and soldiers will depend on our ability to assure the exchange of information through the AFEN to many different weapon and support platforms.

Therefore, the AFEN must be ready and reliable. We must know that our systems are vulnerable, and that we have to plan and prepare for, and be able to operate around, these cyber attacks. For example, an AFCERT breakout of network incidents indicates the number of AFEN intrusions doubled in the last year alone.

As we continue to exploit the power of IT, tightening our network defenses is crucial. Over the last several years, the Air Force

has implemented a layered network management approach to meet this challenge. Each layer, including the Air Force Network Operations and Security Center, major command and numbered Air Force NOSCs, and the fixed and deployed base network control centers, has its own area of responsibility for protecting the AFEN. This tiered approach improves the Air Force's ability to defend its information exchanges by using a standard set of security products and protection mechanisms across the AFEN technical framework. That helps protect our customers' vital information, by forcing our opponents to penetrate each layer of the architecture before they can gain unrestricted access to a user's information.

We all recognize that the people who put bombs on target, or deliver parts that keep planes flying, depend on the Air Force enterprise network to do their job. Cyber combat is your battlespace. Be sure you do your part to defend it well.

Want to learn more about OPSEC?

The Interagency OPSEC Support Staff offers the "Operations Security Fundamentals" computer-based training course, OPSE130. The CBT CD-ROM is self-paced, approximately four hours in length, and free.

The course is designed to provide federal employees and federal contractors with a basic working knowledge of OPSEC and how it applies to executive branch agencies and departments. It focuses on the history of OPSEC and the OPSEC process as described in NSDD-298. Students have



an opportunity to choose scenarios to practice OPSEC in different environments.

To order a copy, you can:

Contact the IOSS at (301) 982-0323 or visit their Web site at <http://www.ioss.gov>

Or the Air Force Information Assurance Web site at https://www.afca.scott.af.mil/ip/training/training_options.cfm?type_id=2

To view NSDD-298, "National Operations Security Program," go to <http://www.fas.org/irp/offdocs/nsdd298.htm>

@1*Y,F(Z+3

,5\$.]HLQ#V

L*@IU,2J8&

A strong password begins with you

By Master Sgt. H. Leonard Strong, Jr.
*Information Assurance Program Office
Air Force Materiel Command
Wright-Patterson AFB, Ohio*

A strong password is essential to maintaining security and integrity of the Air Force enterprise network. Network vulnerabilities can be minimized with an effective password policy, a continuous awareness program, and Air Force members' acceptance of responsibility for protecting their workstations.

Air Force Manual 33-223 states, "Inappropriate passwords create some of today's most common information systems vulnerabilities." Base network control centers have system configuration tools for detecting and negating unwanted visitors who might wish to harm the enterprise network, but what have you done lately to mitigate the risks

of infiltration? Does your password meet requirements of paragraph 2.4 of the manual? Specifically, are you using an eight alpha numeric password scheme with advanced special characters? Do you actively use password-protected screensavers, and remind co-workers to use them?

Recently, a government organization used a readily available cracking tool to test password strength. Some of those test results are in the graphic below. The information includes password types, lengths, examples and the estimated time to crack them.

These statistics reflect the dangers of using a weak password, since it's apparent a skillful individual can quickly crack it. It's imperative that you use good password construction and protection techniques to prevent intruders from gaining access not only to your system, but ultimately, to the entire Air Force enterprise network.

Password Strength Test Results

<u>Password Type</u>	<u>Length</u>	<u>Example</u>	<u>Estimated Time</u>
Dictionary A-Z	8	Exchange	<1 Sec
	9	ExchangeA	<1 Sec
	12	ExchangeUser	<1 hr 20 mins
	14	ExchangeUserAB	<3 hrs 10 mins
Alpha Numeric A-Z; 0-9	8	4Exchang	<23 hrs 50 mins
	9	4Exchange	<25 hrs 10 mins
	11	4Exchange2A	<34 hrs 50 mins
	14	4Exchange2User	<39 hrs 20 mins
Alpha Numeric Plus Special Characters	8	Exch@USA	<130 hrs 10 mins
Alpha Numeric Plus Advanced Special Characters	8	4Exch@t4	<2,365 hrs 10 mins
	10	4Exch@(4U]	<2,170 hrs 8 mins*

*Estimated time to find two characters



Photos by Boyd Belcher

Clockwise, from left: 1st Lt. Chet Wall, Carlos Garcia, Alva Veach, Juan Munoz, Harry Halladay, Robert Coursey, Dustin Childs, Chris Hernandez, Philip Soliz

and Wayne Rodriguez. Lieutenant Wall is countermeasures officer and technical project lead in the Information Operations Technology division.

AFIWC, AFCERT team up for common mission

By Capt. Tre Martin
*Air Force Information Warfare Center
Lackland AFB, Texas*

It's 8 a.m. Chet Wall walks through an endless maze of cables and computers, painstakingly evaluating latest and greatest technologies – virtual private networks, network traffic analyzers and intrusion detection sensors.

The success of his organization hinges on his ability to plan and arrange these technologies to serve and protect its information.

His modus operandi remains the same: Always stay one step ahead of the competition.

No, Wall isn't some company's highly-paid CIO.

It's 3 p.m. Chad Cooper gathers information on activities and locations the average person never hears about.

He carefully draws parallels between certain events and actions, linking them to corresponding people and organizations.

His bosses require him to master keen problem-solving skills to gather information their organization requires.

No, Cooper isn't a top-secret spy.

It's 2 a.m. April Ducote sits in front of her computer using various administrative network tools to analyze hundreds of Internet protocol addresses. She visits an assortment of hacker Web sites, gathering information on myriad system backdoors and vulnerabilities.

Ducote realizes success lies in minute details, and she knows all it takes is one carefully planned connection or one careless action by a system administrator to achieve root access.

She patiently awaits the inevitable.

No, Ducote isn't some foreign-based hacker.

The fact is Wall and Cooper are first lieutenants stationed at Lackland AFB, in the Air Force Information Warfare Center. Lieutenant Wall is a countermeasures officer and technical project lead in the Information Operations Technology division. Lieutenant Cooper is officer-in-charge of the Computer Threat section in the Information Operations Analysis division. They support AFIWC's mission to develop weapon systems and threat analysis products to support computer network defense operators such as 1st Lt. April Ducote, a crew commander on the Air Force Computer Emergency Response Team, in the 33rd Information Operations Squadron.

Their efforts illustrate finely-tuned synergy between AFIWC and AFCERT in support of a common mission: Detect and identify network intrusive activity to prevent adverse impacts on Air Force network operations – a mission far easier said than done.

AFIWC members perform this mission daily, ensuring the Air Force continues to play a leading role in waging America's relentless cyber war. Since Air Force information and information systems are vulnerable to attack, they require aggressive defensive counter-information programs and capabilities to deter and respond appropriately to both foreign and domestic threats.

Information dealt with by the AFIWC is often both a weapon and a target, and the center carries out its mission with this fact firmly in mind. While IOT creates technology solutions to address threats and vulnerabilities, IOA focuses on using these solutions and other methods to identify threats and prevent them from succeeding.

IOT provides a wide range of defensive information warfare technology solutions, and develops foremost safeguards for the Air Force worldwide network.

As one of the nation's early pioneers in Information Assurance, AFIWC began developing an intrusion detection system in 1991, and three years later, released its IDS prototype. "Many people don't understand that before AFIWC's collaboration with the University of California – Davis, and Lawrence Livermore National Labs, there was no intrusion detection on the network level," said Capt. Sam Birch, IOT's chief countermeasure architect. "There was practically no commercial industry before us."

Beneficial collaboration has grown over the years. AFIWC works and shares technical infor-



Photos by Boyd Belcher

1st Lt. Chad Cooper, officer-in-charge of the Computer Threat section, in the Information Operations Analysis division of the Air Force Information Warfare Center.

mation with a variety of organizations, including Joint Task Force-Computer Network Operations, the National Information Protection Center, and various law enforcement agencies, research institutions and academia.

IOT mastered the difficult art of staying on technology's cutting edge. Other successes include deploying a virtual private network to more than 150 locations, researching desktop firewalls, and defending telecommunications from attack.

Three key elements placed the Air Force at the head of the intrusion detection community and provided the heart and soul of the Department of Defense's premier IDS: the automated security incident measurement sensor, common intrusion detection director system, and computer security assistance program database system.

"One of AFIWC's highest priorities is to develop and deliver the absolute best IDS that we can," according to Col. John Wright, AFIWC's information operations director. "We must not underesti-

See **MISSION** Page 24



Christine Heikkinen, computer threat intelligence analyst, for AFIWC/IOA.

MISSION

From Page 23

mate the critical need for a robust intrusion detection system to meet Air Force warfighters' information needs."

You might wonder what an IDS is and how it works. While a firewall serves much like the lock on a door, IDS tools provide the security guard to watch the lock. IDS constantly scans network traffic and host audit logs, looking for anything unusual, which is normally defined as anything outside the parameters of an organization's security policy.

The AFIWC-developed ASIM sensor, CIDDS and CDS decision-support system comprise the operational network-based IDS used today. The ASIM sensor performs much like a network sniffer. Installed on the digital perimeter of a base's network, the sensor analyzes packets of information flowing into and out of the base, and calls attention to unusual activity such as unwarranted port scans or random connections from unidentified sources.

More than 150 sensors are now in operation across the Air Force.

Sensors forward real-time alerts to a CIDDS, commonly known as a director. Each major com-

mand has an operational director, which in turn reports real-time data to the main parent director at the AFCERT.

Directors correlate ASIM information into a database, and graphically portray and manipulate the data through a user-friendly interface.

"For analysis purposes, nothing matches the director's capabilities," according to Capt. Chuck Port, chief of AFCERT's incident response team. "Commercial products can give us alerts, but not the data to back up what's happening. I think commercial sectors are catching up, but the Air Force is still clearly at the forefront."

The third piece of the IDS puzzle is the decision-support system known as CDS. This centralized, Web-based repository gives Air Force cyber warriors access to virtually any element of information, ranging from past hacker incidents, to virus information, to Air Force-regulated policies and procedures.

It also gives analysts fingertip access to Air Force and MAJCOM numerical statistics for hacker incidents and virus attacks, as well as an abundance of other database queries. AFIWC's combination of sensor, director and decision-support system has afforded computer network defense units the most bang for their buck.

While IOT formulates technical solutions to provide evidence of malicious activity against the networks, IOA teams with AFCERT in a detective role to pinpoint the person or organization behind a particular activity.

"We identify hackers on a tactical basis," said David Lemmon, chief of IOA's computer network operations threat analysis section. "Identifying the who behind electronic attacks is like being Sherlock Holmes – every event is like a little mystery to be solved."

IOA's primary focus is investigating foreign threats on a non-structured, semi-structured or fully-structured basis, with the full spectrum of potential activity initiators ranging from beginning "script kiddies" up to government agents.

Investigating foreign threats is accomplished in two distinct phases. First, the computer threat team works with the joint threat incident database, or JTID, which compiles and correlates as much information as possible on all unidentified foreign network actions. Their analysis forms the basis of recommendations for AFCERT action, and is simultaneously sent to higher joint levels, such

as Joint Task Force - Computer Network Operations.

The second phase involves the computer threat analysis tool, or CTAT, which focuses on creating target profiles for active foreign hacker groups, Internet service providers and associated organizations. The profile is usually a one- to two-page summary on a particular group or organization regarded as posing a threat to Air Force or DOD information systems. The AFIWC/IOA CTAT crew correlates the most serious foreign technical activity to real-world events.

AFIWC analysts share information with organizations such as national agencies, the joint information operations center and the Air Force Office of Special Investigations.

The JTID tool's effectiveness led U.S. Space Command to adopt it as its standard for computer network intelligence production. Essentially, IOA's main goal on a daily basis is to gather target profile information and share it throughout the DOD network security community.

Collaborative efforts of AFIWC teams have



Photo by Boyd Belcher

1st Lt. April Ducote, crew commander on the Air Force Computer Emergency Response Team, a part of the 33rd Information Operations Squadron, works with members of the Air Force Information Warfare Center in support of a common mission. The agencies detect and identify network intrusive activity to prevent impact on Air Force network operations.

produced an unparalleled intrusion detection system and analysis process. However, technology can only accomplish so much.

Although AFIWC's ASIM, CIDDS and CDS tool suite can gather needed data, no physical IDS system is capable of analyzing the massive amounts of incessant, incoming information to ultimately provide a magic "silver bullet" to address all security concerns.

The fourth and most important "X factor" in the whole IDS equation is the human mind.

In the commercial sector, one of the most critically unsung problems in terms of computer security is the lack of talented individuals to protect information systems from attack.

Fortunately, the AFIWC possesses some of the most highly-skilled and technically-adept security minds in the country. And in the ultra-fast-paced computer security realm, having well trained analysts with the ability to learn and process information quickly is an absolute must.

Because IOA's JTID has become the standard for all joint databases of its kind, personnel come from every level and service to learn from AFIWC members, Lemmon said.

IOA analysts don't rely just on IDS tools and training to accomplish the mission – they often turn to each other.

At any given time, foreign threats could launch a merciless attack against Air Force electronic resources, such as the one waged by China shortly after last year's P-3 incident. Having a diverse staff of analysts provides a seasoned line of defense in these situations.

The IDS tool suite, used by trained analysts, has produced innumerable results that have greatly benefited the Air Force.

AFIWC's IOA, teaming with AFCERT, were first to identify the Lion Worm, a foreign virus designed to cause systems to send critical network information to a domain in China. Their teamwork resulted in eventual capture of the virus creator.

While the nation's cyber war may not produce visible bomb blasts like those often seen in network television news coverage of more conventional Air Force combat, this war is as intense as any kinetic activity.

Fortunately, with people like Lieutenants Wall, Cooper and Ducote leading the planning and analysis for our cyber fight, we can all take heart that the U.S. Air Force's computer network defense units will always stay one step ahead of the game.

AFCA conducts change of command ceremony

SCOTT AFB, Ill. – Col. David J. Kovach took command of the Air Force Communications Agency June 3 in a ceremony in the base theater officiated by Lt. Gen. Leslie F. Kenne, deputy chief of staff for Warfighting Integration, Headquarters U.S. Air Force.

Col. Jay R. Adsit relinquished command of AFCA, having served as its vice commander, then commander, since August 1999. He retires in July after serving more than 30 years in the Air Force.

Colonel Adsit succeeded Col. Thomas J. Verbeck, who moved to Langley AFB, Va., to become the director of staff for Air Combat Command. Colonel Verbeck had been AFCA commander since April 2000. Officiating at that ceremony was Lt. Gen. John L. “Jack” Woodward Jr., then Air Force deputy chief of staff for Communications and Information, Washington.

General Kenne said of Colonel Kovach, “He is eminently qualified and he knows what it takes to bring C4 (command and control, communications and computers) and ISR (intelligence, surveillance and reconnaissance) together for the warfighter. Like C4ISR, which brings the right information to the right decision-maker at the right time so that we can have a devastating effect on our enemy, (Colonel) Kovach is the right leader at the right time to lead the Air Force Communications Agency in delivering integrated C4ISR to our warfighters. I have the highest confidence that he will make tremendous progress in doing that.”

Colonel Kovach said, “I’ve seen first-hand some of the outstanding work AFCA people have done around the world, particularly in the Persian Gulf region, supporting Operations Southern Watch and Enduring Freedom and other critical missions there. Your professionalism is superb. Your people are energetic and smart. And I’m very excited by the opportunity to join you in what will be an exciting future, I’m certain, as we shoulder the Air Force’s toughest warfighting integration challenges.

“At another level,” Colonel Kovach said, “it’s wonderfully gratifying to return to Scott AFB, which was home to Air Force Communications Service and Air Force Communications Command.



Photo by Senior Airman Omayra Cortes

Lt. Gen. Leslie F. Kenne (left), deputy chief of staff for Warfighting Integration, Headquarters U.S. Air Force, passes the Air Force Communications Agency flag to incoming commander Col. David J. Kovach, as Master Sgt. Graham Smith, AFCA first sergeant, looks on.

“I’m humbled by the opportunity to become part of AFCA’s heritage.”

Colonel Kovach came to Scott from Shaw AFB, S.C., where he served as chief, Communications and Information, U.S. Central Command Air Forces, and commander, 609th Air Communications Squadron.

Colonel Kovach entered the Air Force in 1975, after graduating from the U.S. Air Force Academy. He has served in the communications-computer systems field for his entire career.

AFCA is the Air Force center of excellence for command and control, communications, and computers, and information technology. It leads the Air Force in information infrastructure optimization. It deploys C4 strike teams for assured Air Force network combat power. It drives innovation for information superiority, and exploits and certifies new information technologies and systems. The agency serves as Air Force communications force structure and policy expert, and retains the only Air Force specialists dedicated to information technology law and history. AFCA has been recognized by Headquarters U.S. Air Force with nine organizational excellence awards.

e-Publishing Web site has new address

BOLLING AFB, D.C. (AFPN) — Air Force Departmental Publishing Office officials announced the e-Publishing Web site has a new Web address.

Serving as the central Web locale for more than 7,000 Air Force forms and publications, the e-Publishing Web site is now maintained at the Defense Information Systems Agency in Oklahoma City, Okla.

“The changes are occurring behind the scenes,” said Carolyn Watkins-Taylor, AFDPO director. “Other than possibly having to type in a new URL, our customers will not have to do anything different. The Web site will be set up exactly as it was before and will continue to provide products to Air

Force personnel worldwide.”

Providing more bandwidth, DISA officials will be able to accommodate increasing traffic and provide faster service to customers. Additionally, the Web site itself will be more secure at DISA.

“Now more than ever, it is imperative that we take steps to secure our systems,” Watkins-Taylor said. “We are essentially ensuring our continuity by covering all of the necessary bases.”

The old address will remain intact and will provide redirection to the new address so customers can adjust any bookmarks or Internet browser links accordingly.

For more information, call the customer support desk at DSN 754-2438.

SSG hosts AF Information Technology Conference

MAXWELL AFB – GUNTER ANNEX, Ala. – Keynote speakers for the 2002 Air Force Information Technology Conference Aug. 26 – 29 at the Montgomery Civic Center, Montgomery, Ala., include Air Force Chief of Staff Gen. John Jumper, and Michael Dell and Michael Capellas, presidents and chief executive officers of Dell Computers and Compaq, respectively.

The 16th annual conference is geared toward users, buyers, developers and managers from across the Department of Defense who identify and define requirements for future IT capabilities. With the theme “Air Force IT for a Changed World,” the conference gives DOD personnel an update on latest technologies, and a preview of upcoming industry advances and offerings.

Government and industry leaders will present more than 260 seminar sessions, and the exhibit floor will showcase the latest in IT from Microsoft, GTSI, Dell and Micron, among others.

More than 5,000 people are expected to attend the conference, sponsored by Standard Systems Group. SSG acquires, develops and sustains standard systems, and provides data processing communications computer systems and capabilities to Air Force major commands and bases around the world.

Online registration for the conference is available at <https://web1.ssg.gunter.af.mil/afite/>.

For more information, call DSN 596-4319, or (334) 416-4319.

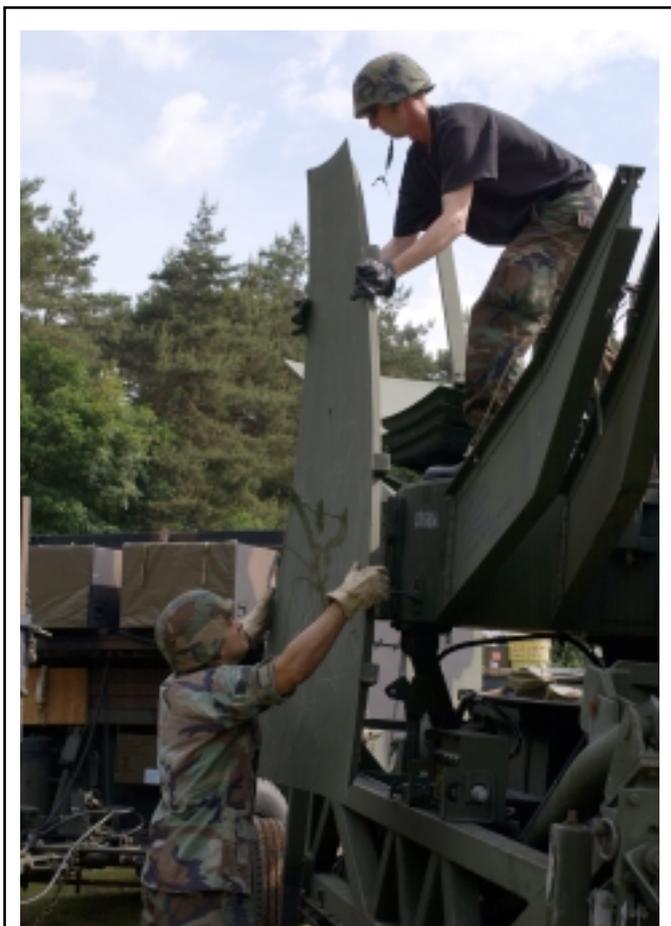


Photo by Senior Airman Marie Cassetty
LANDSTUHL, Germany (AFIE) – Airman 1st Class Paul Shyne and Senior Airman Hamlet Arutynovx, both satellite, wideband and telemetry systems apprentices from the 1st Combat Communications Squadron at Ramstein AB, Germany, move parts of a satellite antenna at the Landstuhl Army Training Site during exercise Golden Divide June 8. The exercise is used to evaluate mission readiness.

AFPCA keeps HQ AF connected

By Tech. Sgt.
Mona Ferrell
Public Affairs Office
Air Force Pentagon
Communications
Agency
Washington

Walk into any office in the Air Force these days and one of the first things you're likely to see is a desktop computer. In today's world of information technology, a computer with all of its peripherals has become a necessity, linking us to each other and the world. But what happens when your system is "down" or broken?

If you're one of more than 8,000 Headquarters Air Force members assigned in or around the Pentagon, you rely on personnel assigned to the Air Force Pentagon Communications Agency desktop maintenance branch to get you up and running.

Ensuring continuous and consistent IT operations for all of these customers isn't an easy task, said Capt. Rich Turner, officer-in-charge of desktop maintenance for AFPCA's HAF office automation directorate.

"We have a staff of 40, consisting of military, civilian employees and contractors, who work day-in and day-out to ensure all HAF customer computer problems are taken care of in a timely manner," Captain Turner said. "One day our maintenance technicians could be working on a desktop issue, like a printer, monitor or personal digital assistant connection problem – and the next day on the nuts and bolts of the computer, like installing video cards, hard drives or disc drives. Basically our technicians ensure any computer problem needing a hands-on approach is rectified as



Photo by Tech. Sgt. Mona Ferrell, AFPCA

Napoleon Stewart, HQ Air Force office automation network technician, places a fiber network interface card in a computer after troubleshooting the unit.

soon as possible."

Since the Pentagon client base is larger and different from most Air Force bases, there has to be a reliable and efficient means of working computer problems.

The customer's first step is to call HAF's office automation help desk. "If the problem can't be worked over the phone and a technician has to physically lay hands on a computer, it will be given to a desktop maintenance technician," said Master Sgt. Carl Peeples, HAF OA desktop maintenance superintendent. "We can have as many as 200 jobs open at one time, so we stay pretty busy."

But tracking the work order, or "ticket," doesn't stop there. As it's assigned to desktop maintenance, it goes into a queue. From there, a queue manager, who continually monitors all of the open tickets, assigns the job to one of four teams, depending on which office is having the problem, Sergeant Peeples said.

"It's important for our customers and technicians to build rapport, so our teams are broken

down by office symbols,” he said. “People have come to rely on their computer to get work done – they also need to be able to rely on their computer technician. Assigning jobs based on the originating office allows our customers to put a face with the job – confidence can be built.”

Confidence is also built through quick and reliable turnaround, Captain Turner said. Desktop maintenance personnel try to complete most work orders within 24 hours. For VIPs such as general officers and senior executive service employees, the goal is six hours or less.

“We generally don’t have a problem meeting our goals,” Captain Turner said. “Of course, there will always be one or two customers who have very difficult problems that push us beyond our goal, but that’s definitely not the norm.”

“Every computer problem is important to the people it affects,” Captain Turner added. “But at the Pentagon, we’re working with high-level senior Air Force officials with a real need to have their IT peripherals working at all times. There’s a ‘food chain’ of sorts, and for the most part, people realize this.”

If customer satisfaction is the HAF OA desktop maintenance section’s primary goal, they’re succeeding, according to Col. Phil Breedlove, senior military assistant to the Secretary of the Air Force.



Staff Sgt. Julius Williams, assistant NCOIC of desktop maintenance, configures software on a customer's new laptop computer.

Considering the nature of the business conducted by the Office of the Secretary of the Air Force, it’s imperative to keep the office’s two local area networks, and the blackberry personal digital assistants carried by the secretary and his staff, in top working order at all times. AFPCA’s desktop maintenance technicians make it happen.

“We do everything electronically here (in the SECAF’s office), and we’re totally dependent on the network,” said Colonel Breedlove, whose office calls for help a couple of days a week on average. “We’re outside the office quite a bit, so we continuously rely on our blackberries to stay in touch. We’ve gone through a painful learning experience with blackberries, since we’re such PDA power users. However anytime our IT services are down, AFPCA’s OA personnel are very responsive. In fact, they’re normally here within 20 minutes. They’re very punctual and professional.”

It’s this type of IT service and support HAF personnel rely on daily. “Just like aircraft maintainers are essential to a flying wing, we’re relied on to maintain all the Air Force IT resources at the Pentagon,” Captain Turner said. “Basic office communications couldn’t continue without us – or AFPCA’s OA directorate as a whole.”



Darren Clouden, HAF OA desktop maintenance queue manager, oversees and filters tickets coming in from the HAF help desk.

ECATS champions collaboration

By Rick Jolly

*Air Force Communications Agency
Scott AFB, Ill.*

Have you ever tried to work a problem by generating a bunch of e-mails requesting inputs from offices and people who might have pertinent information, and then piecing together all the disparate e-mail responses?

Have you spent endless time going through your inbox and folders to find and consolidate all that input?

Have you ever thought there has to be a better way than e-mail to collaborate with others on solutions?

Or even worse, have you ever jumped on a plane to attend a quick meeting to resolve some issues – only to return home with more tasks and no solutions?

If you answered yes to any of these questions, there's a tool that just might help end your frustrations: It's the Enterprise Collaborative Analysis for Technical Solutions concept. The Air Force Communications Agency's Enterprise Information Management Branch developed ECATS to support the Air Force mission and enterprise information management by providing an effective way to promote collaboration as a way to deal with the gamut of action items, concerns and problems.

ECATS Concept

On a daily basis, Air Force people search for answers and solutions. While they may have a lot of knowledge resources, including the World Wide Web and e-mail, they struggle to pull together the specific needed information in a limited amount of time. Unfortunately, no single office or organization has a "corner on the market" for information and knowledge. So they must turn to collaboration for help.

Collaboration is a term commonly used by vendors to describe their vision, culture, products and services. As former Oracle President Ray Lane said, "Collaboration is the most important word in business today."

According to the Gartner Group, 80 percent of a company's useful knowledge is unstructured information residing in e-mail, desktops, internally generated documents, pages pulled off the Web,

and human-readable reports generated by enterprise applications.

From the Air Force enterprise perspective, ECATS is the answer. Our goal for ECATS is to provide a Web-enabled knowledge exchange, or KE, to allow collaborative and comprehensive analyses of issues leading to viable solutions.

The ECATS vision is to empower users by channeling the information flood into a reservoir of renewed corporate decision power.

ECATS uses the power of the Web to gather information from all relevant sources, provides a central repository for feedback and updates for all interested users, and in doing so, reduces e-mail congestion. ECATS gives the Air Force community a central collaborative KE information source. KE components include: issues database, discussions and analyses, initiatives database, points of contact, and search capabilities.

ECATS Capabilities

Issues Database. The issues database, depicted in the illustration on Page 31, is the heart of the ECATS KE. It facilitates issues to be captured, understood, discussed and collaboratively resolved. Issues are problems, action items or concerns. Issue owners can upload all pertinent issue-specific and enterprise-related information. Issue-specific data might include description, office of primary responsibility, estimated completion date, and Web content links. Enterprise-related data could be related technology and technical standards, business area, and the ECATS category, or related focus area of the issue, such as architecture, policy, technology, standards or functional initiative. The enterprise information allows ECATS to find other related issues with similar characteristics that may bear on the issue resolution. A point to keep in mind: As necessary, issues can be privatized to restrict visibility and access.

Discussions and Analyses. The key component for each issue is the ability for two-way communication and collaboration through discussions and analyses areas. The issue process provides two-way exchange of information for gathering and sharing knowledge. Users simply login to a discussion and submit information and comments.

Then the issue owner and other editors upload their analysis feedback to the user and issue com-

munity to iteratively progress a resolution. As issue content is changed, ECATS provides the option of sending all linked individuals an automatic e-mail with the specific uniform resource locator, or URL, so users can link directly from the e-mail to the ECATS content. In this way, all interested parties are continuously updated on issue information and status.

This power of collaboration is what makes ECATS KE such a compelling capability for the Air Force.

Initiatives Database. The initiatives database is a repository for information such as ongoing Air Force projects, programs, studies and working groups. Similar to the issues database, the initiatives database contains initiative-specific and enterprise information, including related ECATS category, technology, standard and business areas. All related issues are also linked.

Points of Contact. ECATS maintains a database of registered users, and all their related issues and initiatives.

Search Capabilities. ECATS provides several powerful methods to search its issues and initiatives databases using on-screen drop-down menus – by title, related issue or initiative, business area, ECATS category, technology and standard. There’s also a text search for user provided key words. For example, a user looking for information on extensible markup language standards can search ECATS and find all related issues, initiatives and persons.

Value

ECATS is envisioned as a one-stop service for the corporate Air Force. ECATS users will drive the success of KE, because their inputs strengthen the collaborative nature of the system.

ECATS’ goal is to put the user in control. Similar to how e-mail has emancipated Air Force managers from the telephone as a means of collaboration, ECATS will emancipate us from the confusion of e-mail by relegating it to a *notification* status when ECATS content changes. All ECATS information is located in a central place, tied to Air Force corporate enterprise issues, rather than

in disparate e-mails with broken message trails. Everyone can have instant 24/7 access to the latest analysis and resolution of issues.

Successes

- Several Air Force groups have used ECATS to:
- Resolve Air Force Architecture Sub-Council issues and action items.
 - Gather Requirements Review Board inputs for a new system development.
 - Capture all AFCA technical studies.
 - Help AFCA representatives work problems for industry and standards groups; for example, Open Applications Group issues for the Global Combat Support System – Air Force program office.
 - Work World Wide Web Consortium XML query and Web services issues.
 - Administer enterprise information management Air Force Instructions, including a repository of information on software enterprise licenses.

Implementation

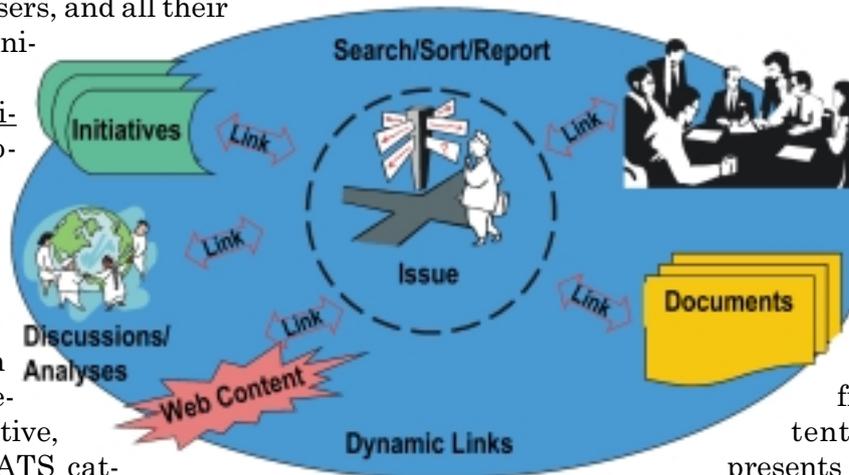
ECATS is being implemented incrementally. The April 2002 release allows users to privatize issues to limit visibility and access, and to provide automatic e-mail notification of issue content changes. It also

presents a new personalized “My ECATS” page; uses a new search feature for issues, initiatives and contacts; and provides for direct upload comments by registered users.

Future enhancements will include document upload and linkage to issues, expanded role-based access, and integration with other Air Force collaboration tools.

Air Force users are encouraged to visit the ECATS Web site at <https://www.afca.scott.af.mil/ecats>. Users wanting to add issues or initiatives, or enter discussions can register online and submit their information. With your help, ECATS will enhance its viability as the central interface for working issues and providing smart implementation of solutions throughout the Air Force.

For more information, contact Richard Jolly at DSN 779-6711, (618) 229-6711, or afca.itcm@scott.af.mil.



Issues database

