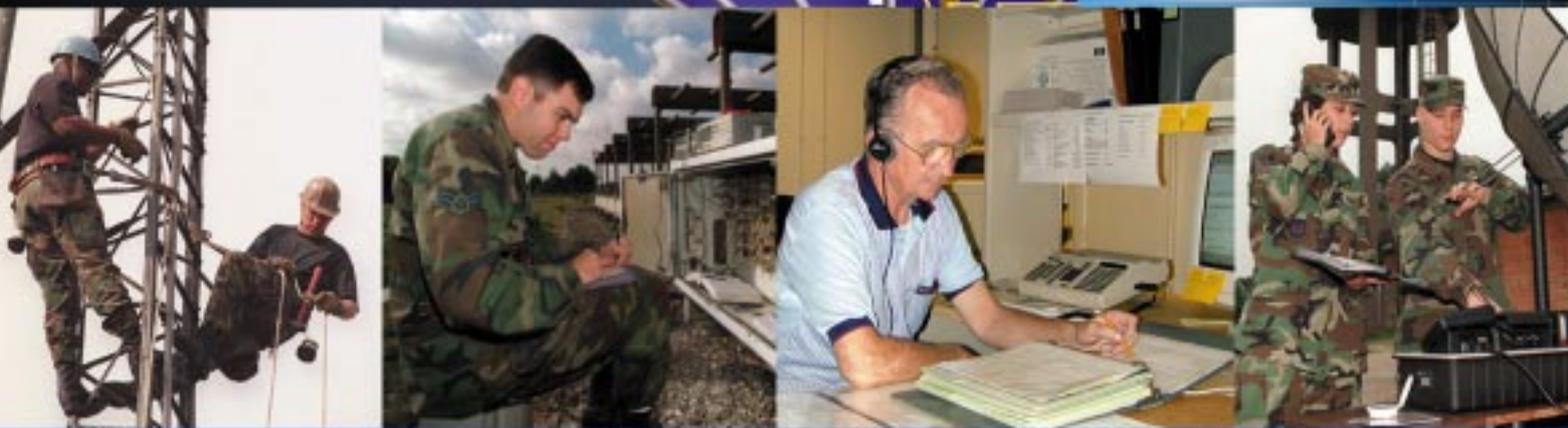


intercom

November 2001

*Journal of the Air Force
Communications and Information Community*

USAFE Communications and Information



intercom

Volume 42, No. 11

Headquarters U.S. Air Force
Deputy Chief of Staff for
Communications and Information
Lt. Gen. John L. Woodward Jr.

Commander,
Air Force
Communications Agency
Col. Thomas J. Verbeck

Editorial Staff

AFCA Chief of Public Affairs
Lori Manske

Executive Editor
Len Barry

Editor
Tech. Sgt. Michael C. Leonard

Contributing Editor
Chief Master Sgt. John Snead
U.S. Air Forces in Europe/SCXF

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/XPPA, *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.

Check out
our Web site at:

<http://public.afca.scott.af.mil/>



USAFE comm and info

4 RAF Croughton marks 50 years of support to global Information Superiority

6 39th Wing, Comm Squadron partner with DODDS for Cisco training



7

7 RAFs Croughton, Mildenhall become 'heartbeat' of U.K. telephone switchboard ops

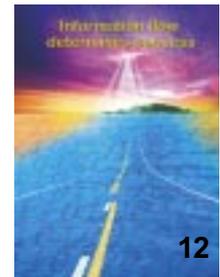
9 Server consolidation boosts effectiveness, security

10 Fiber optics bringing Incirlik into 21st century

12 EUCOM geared to win network wars

14 Air Force Portal provides single point of access to information, applications

16 Aviano tests SAN solution for server consolidation



12

IA Awareness Campaign 2001



17

17 Information Assurance more relevant than ever (We can't afford to be the weakest link)

19 Are all these passwords really necessary?

21 OPSEC: How much is too much?

22 Anything is possible ... with a computer

in other news

23 Information managers keep pace with technology

24 Air Force Virtual Private Network: big score for information operations

27 Counsel's Corner: IMPAC users need to know the rules



24

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

About the cover

This month's cover focuses on communications and information in USAFE.



Cover by Tech. Sgt. Mike Leonard

USAFE works to make *One Air Force ... One Network* a reality

By Gen. Gregory S. Martin
USAFE Commander
Ramstein AB, Germany

In 1969, the Department of Defense envisioned how to network incompatible computers to exchange information. The result has been an explosion of technology giving rise to the Internet and a wide variety of digital applications. Last year, former Secretary of the Air Force Whit Peters and Chief of Staff of the Air Force General Mike Ryan unveiled the vision that continues to guide us: *One Air Force ... One Network*. This vision prepares us for making tremendous advances in our

network systems, enhancing the delivery of information to everyone who needs it.

In USAFE we are working hard to turn *One Air Force ... One Network* into reality. From our “First Look” portal initiative to our efforts at centralizing server and network functions, we’re exploiting the value of quantum leaps in storage capacity and network technologies. This visionary approach will provide major progress in inter-office, inter-organization and inter-personal connectivity, which will allow us to leverage the value of our people in new and exciting ways. Of course with this great enhancement



Gen. Gregory S. Martin

comes the need for each of us to become much more sensitive to network security and Information Assurance across the full spectrum of our aerospace operations.

IT at the heart of Information Superiority

By Col. John W. Maluda
Communications and Information Director
Headquarters USAFE
Ramstein AB, Germany

Information Superiority continues to be a decisive factor in our ability to defend, secure and maintain democracy throughout the world. Ensuring the right person has the right information at the right time is vital to today’s warfighter. Nowhere in our Air Force is this need more apparent than in USAFE. With 91 countries in our area of responsibility, we need only look as far as Macedonia, Skopje or Africa to see how critical “information” is for our contingency forces.

At the heart of Information Superiority is information technology—the “guts,” the “machinery” that makes information flow. It has forever changed the way we perform, educate and operate from a global perspective. IT enables us to better leverage information to support contingency and humanitarian efforts, retrieving near real-time information from globally distributed networks and placing it at the fingertips of the warfighter within seconds. The

resulting impact on air campaign planning and execution demands we manage our IT infrastructure as a weapon system and effectively arm our comm and info warriors to operate, maintain and safeguard that weapon system.

As the USAFE/SC, I am responsible for a myriad of things, but I can tell you that I spend most of my time on Information Superiority/IT issues. We in USAFE endeavor to sustain steady-state in-garrison and deployed missions, while fortifying our readiness posture to respond to real-world EUCOM and NATO contingency scenarios. It is my responsibility to ensure USAFE’s comm and info professionals are at the forefront of all efforts to manage information like we would a weapons system. Accordingly, we’re implementing rigorous training and stan-eval programs in our Network Control Centers to ensure our comm and info professionals achieve and maintain crew position certification levels commensurate with operating and maintaining our IT weapon systems. USAFE comm and info professionals are using IT to help the Air Force refine and reengineer core processes—and no one comes close!



RAF Croughton marks 50 years of support to global Information Superiority

Helping to change the face of worldwide communications

By Capt. Tony Davis
*422nd Air Base Squadron/SCM
RAF Croughton, England*

“Croughton? Where the heck is RAF Croughton?” These questions are often heard when a U.S. Air Force communicator is informed of an assignment to the 422nd Air Base Squadron, Royal Air Force Croughton, England. However, anyone who’s been to the installation – or who’s familiar with communications and information in the United Kingdom – knows the vital role the 422nd ABS plays in the United States European Command’s theater of operations.

The “Cougars” of the 422nd ABS extend premier communications service to the National Command Authority, as well as Department of Defense and North Atlantic Treaty Organization warfighters across the globe. They maintain 23 major strategic communications and information systems, directly supporting forces deployed in CONUS, Europe, Africa and Southwest Asia. The squadron also maintains stations at other locations throughout the United Kingdom, including RAF Uxbridge, RAF Barford-St. John and RAF Daws Hill, in addition to 17 Digital European Backbone radio relay sites throughout southern and central England.

The maintenance and operations team ensures \$250 million in assets are working at peak efficiency. The 422nd carries one-third of all EUCOM communications bridging Europe and the CONUS, and anchors Europe’s largest HF-entry facility, the U.K.’s largest Systems Control Facility, the U.K.’s only Standard Tactical Entry Point and 3rd Air Force’s wideband special maintenance team for superior intra-theater support.

The unit has undertaken an extensive series of initiatives to revitalize its portion of the European communications infrastructure and expand the range of services it offers the tactical warfighter. These include



Staff Sgt. Clarence Russell fans and forms cables on the back of the new FCC-100s.

significant expansion of the STEP capabilities, complete reconstitution of the Systems Control Facility, and a key role in Defense Message System implementation and network consolidation for the United Kingdom and the theater.

They began expansion of STEP capabilities with partnerships to share access to other satellite capabilities. With partnerships in place, Croughton now offers access to three X-band Defense Satellite Communications Systems satellites: East Atlantic, Indian Ocean and Indian Ocean Reserve. This has more than doubled military satellite coverage, to include more than 60 percent of the globe. They’ve added access to commercial satellite capability with dedicated assets for Ku-band connectivity, and plan to add C-band connectivity by mid-2002. They even managed to work in testing with the RAF SkyNet constellation, to assess its stability and availability for possible U.S. military use.

The Cougars quickly realized they needed more capacity on the ground to fully use new satellite capabilities, and began a program to expand FCC-100 multi-

plexer suite to support more simultaneous warfighting customers. They reused three FCC-100s left over from a U.S. Navy system retirement, and moved two from another location.

Their self-help installation team used 3,000 feet of cabling to make 99 new cables, with 182 connectors, for equipment and patch panel connectivity in two separate locations. This upgrade more than doubled their ability to provide voice, video and data to deployed customers from three simultaneous deployed locations to eight, and gave them near the capacity of the two European dual-STEP sites at a fraction of the cost.

The 422nd ABS has taken steps to modernize the Systems Control Facility – the largest in the United Kingdom – with more than 1,200 circuits, more than 4,000 customers, and Facility Control Office responsibility for 17 terrestrial links and 67 Defense Information Infrastructure sites valued at more than \$110 million. Despite the immense responsibilities levied on Systems Control, the facility and equipment were aging, and the state of both was nearly to the point of affecting mission accomplishment. In late 2000, they began an aggressive program, combining self-help, funded CE and contractor projects, and replacement of furniture and equipment to transform the SCF into a clean, safe, state-of-the-art facility that better meets mission needs. Tech controllers put in hundreds of self-help hours removing eight obsolete equipment racks and more than 6,000 feet of communications and power cables from the floor and ceiling, and dismantling and removing two huge overhead cable troughs.

Right behind the self-help project, the base civil engineers swept in with a \$450,000 project to refurbish and paint the facility, install new suspended ceiling and office-grade lighting, and abate the asbestos problem. The last step was to purchase and install ergonomic workstations throughout the facility, greatly enhancing the efficiency and effectiveness of the work force. They continued to expand their role this year as key provider of network services in the United Kingdom. The 422nd ABS is home for United Kingdom DMS regional nodes, and provides single point of entry for all DII services to and from the region.



Airman 1st Class Melissa Covington changes a back-up tape on RAF Croughton's Regional Defense Messaging System nodes.

They teamed with Defense Information Systems Agency and 1st Combat Communications Squadron to provide the first virtual extension of a base network to the tactical warfighter in the field. In Operations Agile Lion and Med Flag '01, they used a combination of innovative network engineering, careful coordination, and thorough security review to reduce the field footprint by one pallet and two maintainers, while increasing service to customers. DISA has begun evaluating possible use of this concept throughout the STEP community.

If that wasn't enough, Oct. 20 marked the 50th Anniversary of RAF Croughton as a premier global communications hub. The installation was established prior to World War II, but began its communications role with establishment of a U.S. Air Force Global Airways Station in 1951. Numerous events were held this year to observe the anniversary, culminating with a banquet on the evening of the 20th.

By the way, in case you were wondering, RAF Croughton is near Brackley, about 70 miles northwest of London. So if you've read this far, you've not only gained an appreciation of the communications mission, but you've joined the ranks of distinguished Air Force communicators who can answer the questions: "Croughton? Where the heck is RAF Croughton?"

39th Wing, Comm Squadron partner with DODDS for Cisco training

By Capt. Tracy Burge

39th Communications Squadron
Incirlik AB, Turkey

The 39th Communications Squadron and Incirlik High School, a Department of Defense Dependents School, have teamed up to develop computer training to benefit both military personnel and students at Incirlik.

Incirlik High School is upgrading its computer science curriculum with a certified "Cisco Academy" to provide students an opportunity to learn and apply computer networking principles, from basic terminology to building professional networks.

To jumpstart the program, the communications squadron will provide \$16,000 in equipment, networking and computer equipment to use as visual aids, and an internship program for the academy's students.

Additionally, the wing benefits because the school's Cisco instructor provides hands-on training to communications squadron people at no additional cost.

To codify relationships and contributions to the program, the DODDS and 39th Wing built a memorandum of agreement outlining both parties' responsibilities.

Provisioning visual aids was the first step, as obsolete and non-functional communications equipment was transferred to the Cisco laboratory. The equipment included everything from old network cables to hubs and routers.

Many students don't understand the full concept of networks until they see the equipment in front of them, and these visual aids give them an opportunity to see the equipment first-hand.

Because the academy is highly technical, it has a rigid curriculum that builds upon itself from simple to complex. To complete the program each student must participate in an internship accumulating 125 hours hands-on work, a responsibility gladly accepted by the communications squadron. Students are assigned tasks such as making and pulling network cables and shadowing network technicians to troubleshoot real-world problems.

To round out their network exposure, students experience other areas of computer operations, such as help desk, systems administration and small computer maintenance.



Photo by Senior Airman Matthew Hannen, 39th CS, Incirlik AB, Turkey

Jessica Sigle, Incirlik High School student (center), talks with Greg Gerenza, Cisco instructor, while making an adjustment to a data port on a catalyst switch. (From left) students Nick Answine, Senior Airman Keya McLaughlin, and Senior Airman Eric McCorey look on.

Strict adherence to Cisco specifications is a requirement to establish a Cisco Academy lab. Getting communications equipment in Turkey is challenging because it requires a host nation agreement. Additionally, the market search for equipment is made more difficult by the language barrier.

Required equipment includes routers, wide area network interface cards and SMARTnet switches.

The initiative gives the communications squadron a local source of expert training in a Cisco certified laboratory. Without the laboratory traditional training is expensive, with only a few local providers in Turkey.

Without a laboratory the squadron's only options are expensive temporary duty assignments to Germany, England, Italy or the United States. Even if the Air Force eventually provides the resources for a network laboratory, the Incirlik High School Cisco Academy will provide a fully qualified Cisco instructor.

"The Incirlik High School and the communications squadron each benefit from a creative partnership, in which both realize much more than would be achievable going it alone," according to Lt. Col. Charles Dunn II, 39th CS commander.

Students participate in an advanced curriculum and even earn college credit, while the 39th CS receives continuing education and training at a fraction of the cost available through commercial vendors.

RAFs Croughton, Mildenhall become 'heartbeat' of U.K. telephone switchboard ops

By Tech. Sgt. Theresa McCullough
100th ARW Public Affairs
RAF Mildenhall, United Kingdom

The results of what began as a telephone operations study, later being converted to a reengineering project, are now coming to fruition with the consolidation of the telephone switchboards of U.S. air bases throughout the United Kingdom.

RAF Mildenhall and RAF Croughton are the heartbeat of the telephone switchboard operations for the U.K. The consolidation began in May, with RAF Molesworth combining with Mildenhall and RAF Fairford with Croughton. It was completed Sept. 30, with RAF Lakenheath combining with Mildenhall.

"The change was transparent for our customers," said Paul Franz, 100th Communications Squadron telephone switch network manager. "They receive the same excellent, if not better, service they have been receiving, just from a different location."

The 10 operators working at RAF Mildenhall, which increased to 18, are working three shifts.

"Overall the consolidations reduced the total number of operator requirements from 44 to 23, accomplishing the Air Staff directed reduction of civilian slots in 3rd Air Force," Franz said.

The initiative is expected to save an estimated \$1.9 million over five years.

Phone numbers for the installation switchboards did not change. Calls are transferred to the servicing switchboard automatically.

"The only glitch we experienced was when operators answered with a different base name than what you were calling when they answered a line," said James Bailey, telephone switchboard supervisor.

The Mildenhall switchboard operates 24 hours a day, 365 days a year primarily supporting Mildenhall, Molesworth and Lakenheath. The Croughton switchboard supports itself and Fairford from 7 a.m. to 9 p.m. Monday to Friday. However, due to limited workload for these two bases during non-peak hours (Monday to Friday from 9 p.m. to 7 a.m., weekends and holidays), the consolidated switchboard at Mildenhall handles all Fairford and Croughton calls during these times.

Previously, Mildenhall operators were answering about 1,700 calls per day, for Mildenhall and Molesworth. Addition of Lakenheath was expected to double the number of calls.

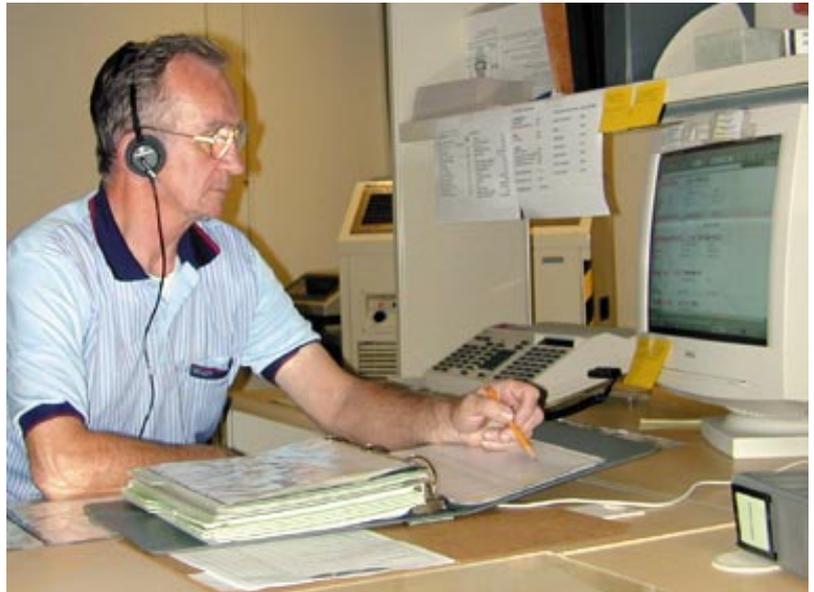


Photo by Senior Airman Rasheen Douglas

Raymond Prouty answers calls at RAF Mildenhall's consolidated switchboard facility.

"With an additional 20 to 25 percent for the other three bases on nights and weekends, the total number of calls per day can be around 4,000 to 4,500," Franz said.

With the significant increase in calls, the 100th CS is making plans to upgrade the operator positions with new computer assisted consoles to increase speed and accuracy of placing calls.

According to Franz, a multifunctional reengineering team was formed last year to determine how to increase the efficiency of telephone switchboard operations.

The team visited each site and gathered detailed data on workload, manning, operations and processes; reviewed reports on other telephone operation studies; and conducted benchmarking visits to several commercial call centers, looking for ways to improve telephone operator service.

The team's analysis of workload data revealed having decentralized switchboards at each of the five sites was inefficient and not cost effective. This was especially true at the smaller sites, where the number of assigned operators far exceeded that required by the volume of call traffic being handled.

Although the team found it feasible to consolidate all operations into a single site, it took into account the expressed desire of the communications community to have a switchboard at a minimum of two sites to allow for backup capability should the primary site become inoperative.

USAFE, EUCOM team to improve command and control, save costs

By Lt. Col. Mark Rydell
HQ European Command
and Master Sgts. Frank McClain
and Edward Zawoysky
HQ U.S. Air Forces in Europe

Even though the Cold War's over, it hasn't been easy reducing communications costs associated with that era. The transition from legacy to new systems presented difficult challenges to EUCOM and USAFE due to program delays, funding shortfalls, and reliance on legacy systems. The result was an infrastructure that kept growing even though we were drawing down our forces in Europe.

That has finally started to change with the recent decommissioning of the most labor-intensive hold-over command and control systems in use: Regency Net and Flaming Arrow Net-Europe.

Regency Net, commissioned in early 1993, was a high-frequency survivable communications network used to provide error-free data connectivity to many U.S. military locations throughout Europe. Developed in the late '80s, it was designed to provide message traffic to more than 300 terminals, either fixed or mobile, at these locations.

Flaming Arrow Net-Europe, commissioned in 1981, consisted of UHF satellite communications terminals



A terminal is removed from the 852nd Munitions Support Squadron at Buechel AB, Germany.

operating over the Air Force Satellite Communications packages located on (Navy) fleet satellites.

RN was decommissioned in April and FAN-E in September. Closing Regency Net and Flaming Arrow Net-Europe within USAFE saved \$239,000 annually in operations and maintenance and training costs, eliminated more than 1,000 man-hours, and released 23 manning authorizations for other use.

It took a joint European Command, J6, J3, U.S. Air Forces in Europe and U.S. Army Europe effort, along with the personal involvement of Gen. Joseph W. Ralston, commander-in-chief U.S. European Command and Supreme Allied Commander Europe, as well as Gen. Hugh Shelton, former chairman of the Joint Chiefs of Staff, to re-look requirements and bring the communications infrastructure in line with today's command and control needs. This teamwork provided a one-time cost avoidance of \$15 million.

"Shutting this system down and changing the 'more is always better' Cold War mind set was a major accomplishment," said Brig. Gen. Gary L. Salisbury, USEUCOM director of Command, Control and Communication Systems. "Not only have we increased the operational capability of our theater forces, but we saved taxpayer dollars."



A GSC-40 Flaming Arrow Net-Europe terminal is among older command and control systems being decommissioned.

Server consolidation boosts effectiveness, security

By Staff Sgt. Chris Norman
HQ USAFE/SCNOE
Ramstein AB, Germany

When Internet technology, notably the World Wide Web, moved into the computing mainstream in the mid-1990's, the model for Air Force computing changed dramatically. The Web model is characterized by loosely connected tiers of diverse collections of information and applications that reside on a broad mix of hardware platforms. Many people think of the Web and associate it with commercial sites such as Yahoo or Hotmail. Our vision is to use the Web as a tool for day-to-day business.

"We see the future of Air Force computing as a common Web-interface being the layer on top of file, e-mail, and application services," said Tech. Sgt. Craig Eckenrode, NCO in charge of Web operations. "In fact we work closely with those teams to keep in step with that vision."

The Enterprise Systems Branch at the USAFE NOSC, composed of primarily 3C0X1 and supported by several 3C0X2 and civilian contractors, serves as a focal point on Internet technology for USAFE. Following proven techniques from the commercial sector, they have designed and implemented an architecture to pro-



Photo by Tech. Sgt. Craig Eckenrode, Ramstein AB, Germany

Staff Sgt. Chris Norman logs onto the console to check performance metrics on one of the servers.

vide a common information-delivery platform that is scalable, extensible and highly available to support that vision.

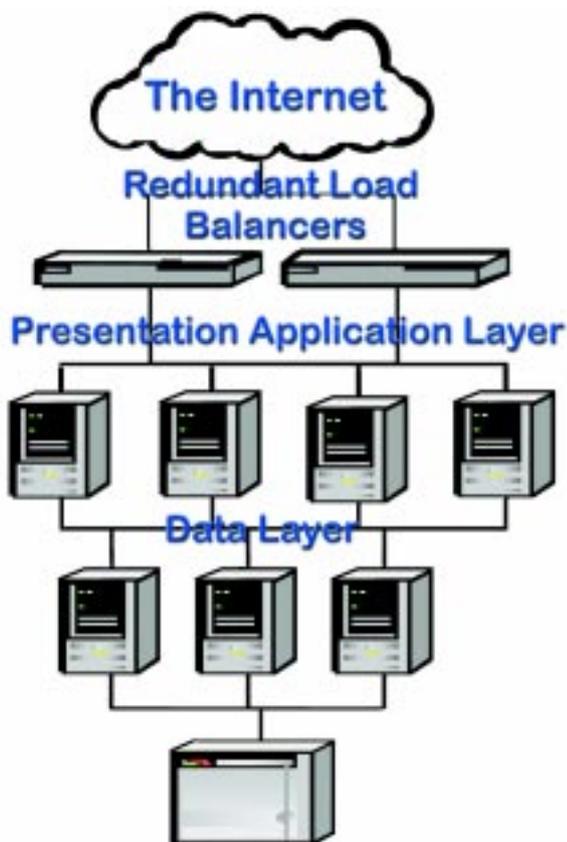
The consolidated architecture is built using n-tier methodology. Services are separated and located on different servers making them more robust and reliable. This model's ability to scale up or scale out provides a rich environment for developing Web-enabled applications such as the USAFE First Look Portal.

"We've gone from multiple unstable servers running different operating systems to one consolidated and very sturdy platform in less than two months," said Lt. Jay Crossler, lead developer for First Look. "The solid hardware foundation has allowed our productivity to soar."

Consolidating the command's Web sites to one redundant and load-balanced platform is a major step towards professionalizing the command's Web presence. This new architecture addresses issues such as duplication of effort among bases, non-compliance with Air Force Barrier Reef concept, and inexperienced technicians trying to protect a vulnerable system.

"The fewer servers there are in the command, the less chance a security patch will be missed leaving a system open to attack," said Staff Sgt. Greg Drake, in charge of security.

In the first year since consolidation began, they have reduced the command's public Web servers by 90 percent, effectively improving the command's Web security and Information Assurance.



USAFE's Web servers

See ISP Page 11



Photo by Senior Airman Matthew Hannen, 39th CS, Incirlik AB, Turkey

Staff Sgt. Dan Morris, 39th Communications Squadron, Incirlik AB, Turkey, reports the status of a damaged cable to the base cable shop.

Fiber optics bringing Incirlik into 21st century

By 2nd Lt. Brenda Kell
39th Communications Squadron
Incirlik AB, Turkey

After years of diplomatic and legal discussions, the U.S. Air Force's 39th Wing and the Turkish Air Force's 10th Tanker Base Command broke ground in July on a base cable infrastructure upgrade, or combat information transfer system, at Incirlik.

The upgrade will replace outdated 1950s paper-wrapped copper cabling with modern fiber optic cables, bringing Incirlik networks into the 21st century.

"Why is cable installation such a big deal?" The answer to anyone ever stationed at Incirlik is simple.

Turkish law and customs strictly govern communications installations. Strategic planning has a different meaning when communications installations are fully dependent on host nation support.

Though most installations are eventually approved, seemingly simple tasks can quickly overcome even the most experienced planner. Familiar acquisition and installation processes must be integrated into an entirely foreign process.

The 39th Wing overcame a number of obstacles be-

fore host nation approval was granted. The challenges were many and varied, including requirements to only field systems of direct benefit to the host nation, or to provide it an equivalent service or product.

Additionally, the base had to attempt to produce equipment and supplies in country before looking to the States.

Next the wing had to look within Turkey for a contractor. The result was General Dynamics with a Turkish subcontractor.

Turkish construction laws further compounded the challenge, with restrictions on breaking ground and installing manholes.

A major milestone was met when the Turkish General Staff began deliberations with the Turkish Air Force at Incirlik. The staff conferred with the Turkish Air Force, who in turn bartered with U.S. Air Force personnel for an acceptable win-win solution.

The U.S. Air Force and Turkish Air Force met several times before reaching a mutually acceptable solution. A successful package was approved in January. ESC selected General Dynamics, of Oklahoma City, as

See **FIBER** next page

FIBER

From previous page

the prime contractor with condition that labor in non-secure areas be provided by Turkish nationals, and equipment be procured on the Turkish market or through Turkish vendors.

General Dynamics had one on-site manager, one quality assurance person, and one logistics support person at Incirlik for the installation. The site managers subcontracted the majority of the work to local vendors selected during the survey and design phase.

General Dynamics encountered some unique obstacles. First they had to learn to integrate different Turkish customs into the work schedule, while overcoming a language barrier. Second, they had to teach contractor personnel to build within American specifications. The subcontractors learned quickly implementing the techniques in construction, while using new supplies, knowledge and skills.

Turkish subcontractors are installing fiber cabling to 85 U.S. Air Force buildings and 30 Turkish buildings, and copper to 22 other Turkish facilities.

Additionally, fiber optic cable is being installed in Turkish guard towers as a part of enhanced force protection around the base's perimeter, a condition of TGS and HNA approval.

The approximately \$15 million project increases bandwidth and data transfer speed of the network, improves command and control, and allows Incirlik to operate several U.S. Air Force standard systems previously limited by bandwidth.

Besides the many mission enhancements, fiber cabling is difficult to tap or electronically jam, and enables maintainers to track cable cuts and faults to within feet, allowing faster problem isolation and repair. Additionally, the fiber optic cabling may lead to voice transmissions over fiber, a more secure voice communications method.

The 39th Communications Squadron commander Lt. Col. Charles Dunn II, noted the upgrade meets a

multitude of community needs.

Though some are obvious, such as the increased data transmission rates and service to network customers, other benefits have yet to be realized as fiber optic technologies bring about new and improved capabilities.

The redundant and flexible nature of the system's design permits long-term cost effective upgrades as the base's mission requirements change.

In the short-term the upgrade will permit expansion of the wing's telephone network through redistribution of copper wire.

For the long term, the wing envisions a high-speed data fiber backbone to carry the data and voice communications load. Future telephone switch upgrades, already planned, will help make this a reality.

Beyond obvious enhanced capabilities, the cement encased conduit infrastructure could potentially support a much improved cable television infrastructure, further telephone upgrades, or any unforeseen communications project.

Fiber cabling will bring communications at Incirlik up to modern standards and enhance its force protection and combat support capabilities. World-class communications will support Operation Northern Watch and other contingency operations. The Turkish Air Force benefits primarily with much enhanced perimeter security and network communications base-wide.

The communications improvements and upgrades symbolize the wing's "can do" attitude and good working relationship with the Turkish Air Force and people.

The cooperative spirit between Turkish and American Air Forces, bilaterally and as NATO allies will continue to serve both countries well into the future, building on more than 50 years of partnership.

Though Incirlik residents can expect to see continuous excavation activity and some inconvenience over the next year, the wing expects smooth implementation with active daily program management and oversight. The 39th CS estimates the project will be completed in July.

ISP

From Page 9

Why consolidate Web servers?

"Aside from the obvious gains with only having to manage one suite of equipment, our biggest reason for consolidating Web servers is network security," said Maj. Paul Welch, chief USAFE NOSC. "Web pages are popular targets. There are hundreds of automated scripts out there that look for Web pages and post some message we'd just as soon

not have on U.S. government sites. Case in point, during the recent "script kitty" war, roughly 80 percent of USAFE Web pages were consolidated on common hardware suites in the USAFE NOSC. This includes 100 percent of the publicly accessible Web pages," he said. "This allowed us to apply single security policy changes to two hardware suites and protect the vast majority of USAFE Web pages. This standard operating procedure allowed us to combat the attempted

Web-page defacements through our normal operations without having to isolate ourselves, thus denying Web access to our own customers. Even though we were constantly probed, we never had to drop service or block access. The information was available, assured and secure the entire time."

Next on the list for these pioneers is to finish migrating the last 20 percent of the command's Web servers and prepare for the Air Force Portal.

EUCOM geared to win network wars

By Lt. Col. Court Allen
*European Command's Theater
C4ISR Coordination Center Director
Stuttgart-Vaihingen, Germany*

It is late Monday afternoon after an already busy day in the European Command's Theater C4ISR Coordination Center. Unexpectedly an urgent call comes from the European Theater Command Center indicating they had just received notification of a new worm detected on the network.

Initial indications of a routine virus quickly evolve into a rapidly propagating, worldwide worm virus over the Internet and the NIPRNET. Through command channels U.S. Space Command notifies the CINCs, while simultaneously the DOD Computer Emergency Response Team notifies the European CERT with the urgent information.

The ETCC quickly notifies the EUCOM Computer Network Defense Information Operations Response Cell and the TCCC. Immediately the TCCC posts the event on its significant network event conference chat to notify all of the theater's network operations facilities. Within moments of confirming the Code Red virus, the TCCC and the theater's Network Operations and Security Centers are monitoring the global situation and coordinating the theater's CND response.

One year ago EUCOM could not have orchestrated this rapid, synchronized crisis response. Previous reaction to significant network events such as the *I Love You* virus were more cumbersome and slow, with information flowing in and flooding the EURCERT and EUCOM staff.

Joint terminology defines network operations as the organizations, procedures and technologies required to monitor, manage, coordinate and control the Global Information Grid. Visibility into the Global Information Grid provides operators the situational awareness necessary to determine network status, recognize anomalies, detect and respond to intrusions, initiate corrective actions, redistribute information flow, and reallocate bandwidth to support higher priority functions across the theater.

Given this visibility and understanding, technical experts and senior leaders are able to identify and execute aggressive improvements, to include judicious planning for the introduction of new systems, and transitioning existing capabilities to provide higher levels of warfighter support.

Recent studies suggest asymmetric enemy tactics and network-centric warfare demand a new look at command and control. Information now is a weapon of

choice, with commanders challenged in this new battlespace environment with command and control of "infostructure."

Before improving overall theater network operations and establishing a TCCC, EUCOM lacked a fusion point for the plethora of daily network operations and security issues. Established late last summer, the TCCC quickly evolved into the go-to center for building theater network situational awareness, as well as supporting CINCEUR's needs to respond to theater-wide network anomalies and attacks. To help with these missions, DISA and NSA personnel were integrated into EUCOM's TCCC.

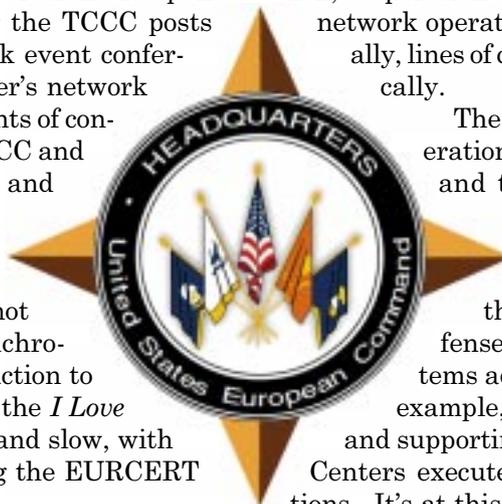
The TCCC's prime mission is to coordinate and deconflict NetOps activity across the theater. Ultimately, the TCCC provides network status visibility and operational impact assessment to the CINC, as well as orchestrating theater-wide responses to network threats and actual attacks. Through consultation, collaboration, cooperation and coordination with the numerous network operations facilities in theater and nationally, lines of communication have opened dramatically.

The heartbeat of EUCOM network operations is found at the lowest operational and tactical levels run by components, agencies, and allies. Where the theater view provides increased senior leader situational awareness, the day-to-day management and defense of the networks occurs at the systems administrator and operator level. For example, USAFE's Network Control Centers and supporting Network Operations and Security Centers execute minute-by-minute network operations. It's at this level that configuration control and security operations are managed and most critical.

The EUCOM TCCC provides the commander essential battlespace situational awareness of "Infospace." By synchronizing NetOps with the operational battle rhythm of the command, the TCCC proactively aligns the shifting operational priorities to prerequisite information dissemination requirements.

To best deal with network events occurring daily, the TCCC's scope of concern is focused on the most vital aspects of the network required for mission execution. By determining critical customers, the critical information they require to perform their mission, and critical aspects of the network supporting its dissemination, the TCCC can tailor the resulting Infospace situational awareness.

At a moment's notice, the steady state of NetOps can turn on a significant network event such as a major communications node outage, a virus in the wild, or worse yet a sophisticated network attack. In these



modes the nature of NetOps shifts into a more aggressive, crisis action response. Assessment, analysis, course of action development, "battle damage assessment" and "mop up" actions must now occur.

A top goal of one of the EUCOM J-6s, Brig. Gen. Gary Salisbury, is to improve and modernize Joint Task Force command and control by optimizing the supporting C4 capabilities. In EUCOM's JTF HQ training exercise, Sharp Eagle 2001, integration of NetOps concepts was a prime C4 objective.

At issue is recognition that each of the services is moving out with a similar, but not necessarily compatible, NetOps approach. When the JTF is established, a JCCC and supporting Joint NOSC assume responsibility for JTF NetOps. The challenge is to integrate service and component approaches to NetOps into a synchronized team that effectively supports the JTF operation. Our challenge is to balance needs of the JTF commander with the JCCC and the capabilities that the services and DISA bring to the fight from their fixed and deployable network management systems. General Salisbury strongly believes that ultimately the JTF commander's NetOps capabilities can be provided by the service component that's been assigned responsibility to activate the JTF. Thus, one of EUCOM's driving NetOps requirements is to have common tactics, techniques and procedures among DISA and the EUCOM service components.

During the Sharp Eagle exercise, special emphasis was placed on the NetOps relationship with the Components, JTF operations and information operations. Our reliance on information and network resources, and the growing capabilities and declining cost of these technologies, make network warfare an attractive option

for adversaries that don't have resources to attack U.S. interests in conventional ways.

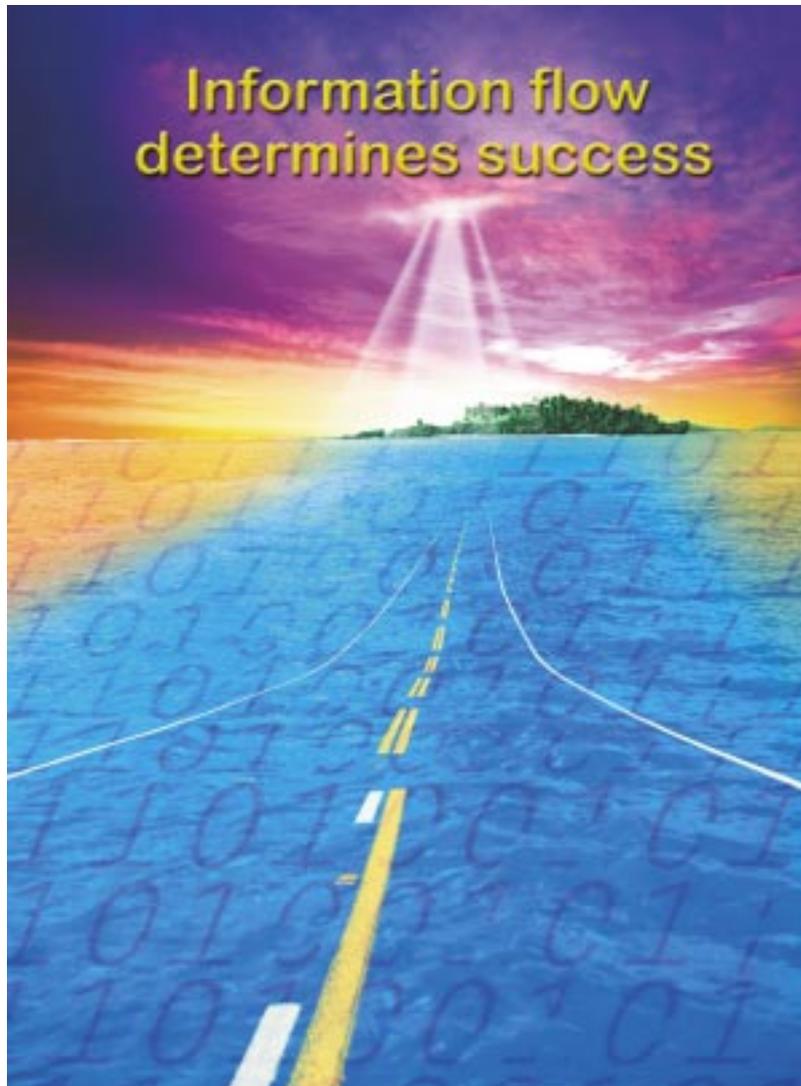
The nimbleness of this approach was quickly demonstrated in an exercise scenario that compromised the Sharp Eagle Joint Task Force classified network. Through vigilant monitoring by Joint NOSC network managers and threat analysts, the attack was quickly revealed. Immediately the JTF IO working group was convened and courses of action evaluated. Within no time, the threat was quarantined and JTF operations persevered through the event.

First steps toward a seamless, responsive and powerful network warfare capability include providing network managers complete network visibility, implementing Information Assurance, and establishing an ability to rapidly direct network managers to take all actions necessary to defend against network attacks.

Throughout the year EUCOM worked hard to operationalize network operations at the theater level. With this, the theater is more nimble in its ability to deal with daily network operations and inevitable crises. By synchronizing network and information operations roles and responsibilities with DISA, our components, JTF CNO, and theater agencies, EUCOM is aggressively posturing

to achieve Information Superiority over our adversaries.

In the coming year EUCOM will aggressively mature theater NetOps. The primary objective is to expand on current partnerships and establish the operational concept for providing an integrated information operations, network operations, and intelligence operations capability in the EUCOM Command Center. Through this vision EUCOM will prevail in future network warfare.



Air Force Portal provides single point of access to information, applications

By Dave McDonnald
HQ USAFE/SCYI
Ramstein AB, Germany



Log on to the vMPF NOW!
(Through the AFPC Secure Server)
Note: You will not be able to use
your AMS/AFAS password.



To learn more about the vMPF,
go to the Knowledge Management Web site.

Air Force employees worldwide have found a new tool on their computer desktop: the Air Force Portal. The portal provides users a convenient single point of access to information and applications on the Internet or Intranet.

Millions of military members have used the Web to access various commercial, government, military and educational sites on the Internet or Intranet. Many have Web e-mail accounts, a comprehensive list of favorite Web links and a host of news, weather and information sources. For those with the highest level of organizational skills, this information is neatly categorized and accessible on their Web browser or desktop shortcuts and links on their computer. For the rest of us, this information is stored on sticky notes, desktop icons or buried within our favorites located on two or more Web browsers.

When we need information, we know we've seen it,

... consider what our work life would be like if we had a tool to organize all of our information. And no matter where we went in the world we could access that information so long as we had access to the Internet.

but just where often eludes us for moment. Sometimes the search can take longer than to re-compile the information from scratch. Re-

gardless of our organizational abilities, there's one common denominator. All the information packed onto our desktops is only available from one place—our computer back at work. Now consider what our work life would be like if we had a tool to organize all of our information. And no matter where we went in the world we could access that information so long as we had access to the Internet. We would no longer be tied to our desktops. We would no longer be at the mercy of our organizational abilities. These are the ideas that have resulted

in the development of portal technology and have led to the Air Force Portal.

What is the Air Force Portal?

The Air Force Portal is a Web-based tool developed to add functionality to your desktop computer and designed for presentation, organization and management of various types of information. The information available to the typical user of the Air Force Portal is a collection of useful Web links, both military and commercial, and the Air Force White Pages. As the Air Force Portal matures, users will be able to access various applications as well.

The **Air Force White Pages**, as the name implies, is much like the telephone directories provided by phone companies. However, White Pages are much wider in scope as it includes all Air Force employees assigned worldwide. If you're looking for someone who works for the Air Force (military or civilian), you should be able to find this individual using the Air Force White Pages. The Air Force Portal is user customizable. You will be





able to add, delete and rearrange your portal view so that it looks and feels the way you want it. Eventually the Portal will provide single logon access to all of the resources an employee needs to perform their mission and provide access to information necessary to the individual in managing their career.

When will people have access?

Within USAFE 16,450 portal accounts have been created. Of these, 117 are administrator accounts. The bulk of the accounts, 15,000, are assigned to the Logistics community. USAFE is now in phase two of the implementation with an additional 12,000 accounts to be distributed between now and December. Our efforts are aimed at putting in place a well-trained and fully-staffed support community. This will ensure problems can be addressed promptly and users will have the best possible support available.

What can the portal do now and what will make it so great?

Currently, the portal has limited capabilities and users should not initially expect a wide range of capabilities. The following are examples of some of the services that are currently available:

Virtual Military Personnel Flight: The vMPF is a secure, Web-based link to each Air Force member's personnel records. Once an account has been established, members are able to access their personal records and conduct their personnel transactions via the Web on a self-service basis from any computer with Internet capability.

My Money: The Air Force Portal is also the gateway to 24x7 pay information. This module provides one-stop shopping for financial questions that Air Force military members and civilian employees are likely to have. The site has four major areas: military pay, civilian pay, travel, and personal finance. Users can see pay charts, calculate the pay impact of a raise or promotion, check on retirement funds and gather a wealth of



information on pay issues. The site will soon provide secure access to a personal LES and the ability to change allotments, tax withholding, etc.

The travel link can take users to per-diem rates, phone numbers of all DOD billeting, availability of lodging and meals, and travel regulations. Other useful travel data such as government airline ticket prices, hotel exemption forms, and even a link to government travel cards. The personal finance section contains an even wider range of useful financial information such as loan calculators, personal financial planning tips, mortgages, auto loans, taxes, or even savings bond purchases.

New functionality for the portal will be added over the next one to two years. The long-term vision is the portal's ability to centralize a user's access to information. The plan is to Web-enable as many Air Force processes as possible and then integrate e-mail, Air Force applications, Air Force information Web sites, local workflow processes (in-processing, EPRs, etc.), searches, and many other utilities into this single interface. Eventually the portal will provide single log on access to Web-enabled information systems for all Air Force users. So for all of us not-so-organized individuals out there looking for a fix to our informational needs, help is on the way.

Air Force

Portal

Aviano tests SAN solution for server consolidation

By Lt. Josederic Scott
and Tech. Sgt. Veronica Nicolay
31st Communications Squadron NCC
Aviano AB, Italy

One Air Force ... One Network, a term coined by Air Force leaders, outlines strategies designed to more effectively and efficiently manage our information systems. Centralized management and administration of network servers provides a single point of operations and support. Professionals who have been trained and who are responsible for network services manage these resources. The Aviano Network Control Center has begun its move to consolidate and centrally manage its services. As the Air Force leaders shifted towards network centric warfare and strategies, the U.S. Air Forces in Europe Command scanned its bases to select a pilot base. Since Aviano had already acquisitioned a Storage Area Network solution for server consolidation they were chosen to lead the way for USAFE.

The Aviano NCC was poised and ready to meet the challenge. They had two four-Terabyte Storage Area Network appliances and 10 servers on the way. The two SAN appliances would be located in two physically separate locations with real time mirroring. The 10 servers would be configured into five cluster servers using Windows 2000 Advanced Server. Complete redundancy at local and alternate sites was incorporated into the planning to ensure network services were not unavailable for extended periods of time. The overall objective was to migrate more than 50-plus file and print servers to the SAN. This would centralize management, increase reliability, and improve support for Aviano's 4,000 network customers. Planning includes the possibility of migrating e-mail services to the SAN. Feasibility is being reviewed and coordinated with USAFE.

Installation of the Aviano SAN was completed in June. Vendor contractors were in place with both USAFE CSS and base level representatives overseeing the project. With the SAN installed there was a need to form business practices to support the migration of all base units to the SAN. A USAFE CSS representative facilitated the process to ensure the standards set forth would be a model for all USAFE installations. Our job as an NCC is to provide our network customers with the services needed to successfully complete their mission. The directory structure and business practice had to accommodate the customers' needs. Base workgroup managers as well as Base Records Managers were incorporated into the planning. We had to ensure the challenges of E-File management and electronic records management was tackled from all angles. The results of the model provide users with a storage area for personal data, restricted office data, shared organizational data, as well as an electronic file plan. The ERM con-



Senior Airman Lyanna Pena manages the storage area network servers.

cept and official file plan location on the SAN ensures the integrity of electronic records is maintained throughout their life cycle. The interim solution to ERM provides a repository to effectively manage electronic records.

The new practices implemented here were geared towards maintaining the integrity of the SAN and working towards proactive management of file and print services. Tools were purchased and incorporated to restrict possible malicious logic from being placed on and executed from the SAN. File types of .exe, .com, .bat, .js, .shs, and .vbs are restricted, they are not authorized to be located on the SAN. A centralized location for executable code is strictly controlled by network administrators. A standard quota on storage allocation is in place to help network users in proper file management. There is also a tool employed providing active reporting of file use. The reports generated help identify unofficial, duplicate and unused files. These administrative tools will exponentially help network administrators do their jobs.

Initial business practices for ERM uses the same principles as those applied to paper files, to include end of year close out and transferring records to the inactive area. It also incorporated a base-wide ERM awareness campaign with training in records custodian and workgroup manager classes.

Today, the migration of file servers to the SAN is well underway. An overview briefing on the SAN/ERM was presented to Lt. Gen. John L. Woodward Jr., Headquarters Air Force deputy chief of staff for communications and information, Sept. 10. He said he was impressed with the efforts at Aviano in meeting the challenge and fully embracing the *One Air Force ... One Network* philosophy.



Information Assurance more relevant than ever *(We can't afford to be the weakest link)*

By Maj. Gen. Dale W. Meyerrose

Director of command control systems, Headquarters U.S. Space Command and North American Aerospace Defense Command, and director of communications and information, HQ Air Force Space Command, Peterson AFB, Colo.

Sept. 11, 2001, changed the United States, and our responsibilities within the Department of Defense. I am not qualified to interpret these events, and many, more articulate than I, are adding meaning to the sacrifices and extolling the heroism of our fellow citizens. Instead, I am following our leadership's direction to maximize my contribution by focusing on responsibilities central to my position. Nothing is more central to the communications community's contributions to our Air Force and country than Information Assurance. For that reason, we must ensure our people concentrate on the right issues for the right reasons.

Our first and most fundamental Information Assurance responsibility is to link our peoples' work inextricably with our Air Force's values, six core competencies, and the Expeditionary Aerospace Force. Other agendas are secondary in importance. Our people must understand the purpose and objectives of Joint Strike Task Force, Information Operations, Space Control, Predictive Battle Space Awareness, Integrated Missile Defense, and Homeland Defense and Security, and their contributions in operating communications systems and command and control processes supporting these critical mission areas.

Availability is the most crucial of the five tenets embedded in the jointly accepted Information Assurance definition. If we deprive operators and users access to their data and information, then the other Information Assurance tenets of integrity, authenticity, confidentiality, and non-repudiation diminish in significance. While no one wants to be the next "poster child" for not protecting a network, we must resist the temptation to transform every threat into a successful de-

nial of service attack by blocking services, or worse, shutting ourselves down. We build enterprise networks to provide vital services to our Air Force. Thus, our primary goal is to operate Air Force networks throughout the spectrum of conflict. We need to learn how to balance risk with mission needs so our commanders always have the information with which to make decisions, and the means to command and control their forces.

In light of recent events, protecting network enterprises, and in turn, information and systems, is high on the Department of Defense agenda and often analyzed in the national media. Modern technology provides an asymmetrical threat status to nations, factions, terrorists, and non-state actors as we've recently seen all too clearly. If we're not careful, this discussion can be dominated by side issues by those who don't live the business of Information Assurance day in and day out. As our Air Force's enterprise network operators we need to keep the discussions focused on the most relevant and important aspects of Information Assurance. We should write our system concepts of operations and not let that responsibility default to others. We must find the root cause of every network failure and fix it, irrespec-

tive of source and intent. We have to prevent "half starts" in our security analyses and implementations. Further, we cannot "build in failure" by installing systems without the upfront requisite training, command and control concepts, and investment, marketing, and sustainment strategies.

Information Assurance at the local level is very detailed and narrow—not so across an enterprise network. At the more macro level we need to map the enterprise in three architectural contexts: operational, systems, and technical. We need to identify critical nodes and paths and figure out repeatable courses of action to apply at a network's critical pressure points—and many of those pressure points are process vice technical. As



See LINK Page 19

Education key to protecting computer information

By Staff Sgt. Robert Root
Wing Information Assurance Manager
F. E. Warren AFB, Wyo.

A New York businessman is sitting in the airport, going over some sensitive e-mails on his palm pilot (or personal digital assistant). This is something that happens hundreds of thousands of times a day, all over the world. Unfortunately, he's so into his e-mail, that he doesn't notice the man sitting across from him, smiling and chuckling to himself.

In another minute, the man across the aisle stands up and walks away. The businessman doesn't even notice he has a palm pilot which now contains all the businessman's sensitive information: names, phone numbers, bank account information, stock account information.

A great scenario for a movie. But, it happens more and more every day. Downloading information in a matter of seconds and stealing have a lot in common. The largest problem the computer world faces is the ability to steal large amounts of information in minutes, if not seconds. But worse yet, many people don't even know that it's happened.

This scenario is possible because of a built-in feature in the palm pilot: an infrared port. It's like a television remote when you point it in the right direction, it can communicate with other computer equipment with infrared ports—just another example of wireless technology.

A teenager sits in her room surfing the Web and, if her parents ask, that's exactly what she's doing. However, she doesn't know that the programs she downloaded have "Trojan code" in them. This invisible pro-

gramming code will allow a hacker to take over the computer in the blink of an eye.

Once the hacker has control of the computer, they can use that computer to hack into other computers. How about a bank to steal money? Government computers to steal sensitive information? Or to send off the next world-affecting computer virus?

Does this scare you a little bit, a lot? Well, it should. Computer theft is becoming common place in the world, because we are putting more and more information into the World Wide Web.

The Computer Security Institute polled 538 corporations for the first half of 2001. They found that 85 percent of the companies had detected computer security breaches. Approximately 186 companies acknowledged financial losses, totaling \$377,828,700. The combined loss over the previous three years (1998-2000) was \$120,240,180.

Okay, but how do we fix the problem?

Education is the key! Everyone needs to learn the vulnerabilities of the equipment they use. When we find weaknesses, we can effectively protect equipment we rely on to accomplish our mission. The Air Force Computer Emergency Response Team forwards security bulletins to all agencies as soon as security vulnerabilities are acknowledged.

These bulletins include the nature of the vulnerability and the steps to be taken to fix it. For example, ports on the Palm Pilot can be disabled. Problem solved ... but, what about passwords? Viruses? Lapses in encryption? The list goes on and on, and you can find the help you need by contacting your local Information Assurance Office.



Are all these passwords really necessary?

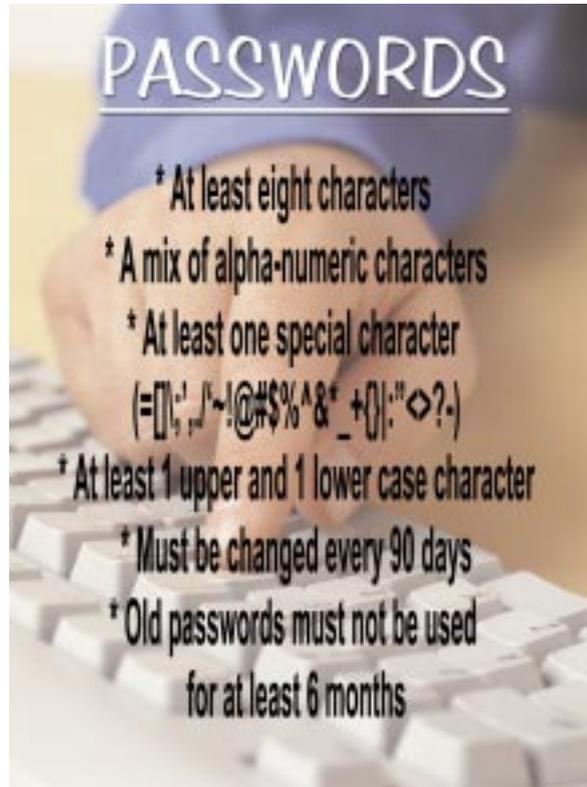
By Airman 1st Class
Joseph C.
Lionbarger
21st Communications
Squadron
Peterson AFB, Colo.

In an age where computers control nearly every facet of our lives, we find there's more need than ever to protect information in these systems. In the Air Force, we rely on the integrity of our information systems for everything from daily reports to missile and weapon control. That is why passwords are increasingly our last line of defense against those who want to exploit our secrets.

Although you may not think you have anything on your computer of intelligence value, you have a responsibility to protect information it contains just the same. While the information on your machine alone may not be of much use to anyone, if it's combined with the information on other computers it can be valuable.

For example, you may have information on your computer about an order of 200 mobility bags. Alone, this information probably wouldn't give away too much about the operational status of our forces. However, add the fact that someone across base had information stored on arranging for the transportation of 200 personnel to the desert, and then add with current news reports of growing tension between the U.S. and Country X.

Thanks to those unrelated pieces of information, I have just discovered that you will be sending 200 military members to the desert for



a possible offensive/defensive strike.

Accidental release of this type of information may be prevented by the proper use of passwords. Passwords must be used every time you login to your computer, and every time you leave your computer system unattended. Reference Air Force Manual 33-223, your passwords must meet the following criteria:

- * At least eight characters
- * A mix of alpha-numeric characters
- * At least one special character (=[\;',./~!@#\$\$%^&*_{}|:~<>?~)
- * At least one upper and one lower case character
- * Must be changed every 90 days
- * Old passwords must not be used for at least six months

By using these guidelines for password management, we can minimize or eliminate risk of inadvertent disclosure of information, and penetration of our networks.

LINK

From Page 17

we build our effects/outcome-based capability, and rule-based security policies, we need to remember that analysis inside the firewall is more important and difficult than responding to "alerts" outside the firewall.

Much of what we knew about Information Assurance in the context of enterprise networks has changed in the past couple of years in terms of capability, scalability, and "do ability." However, we need to recognize some fundamental building blocks have not. The first Information Assurance axiom of information superiority is a skilled, trained, and operationally-focused workforce. We need to nurture our people's thought process to not be satisfied with status quo. Our folks must personify our Air Force warrior culture and have an operational outlook. Our Information Assurance culture should not be to wait for an error, mistake, or user report to prompt action on our part. Our aim is to prevent and detect problems, and correct them before the users' service feels the impact.

By any measure, we've greatly matured our understanding and performance with respect to Information Assurance over the past few years. Our networks are among the most sophisticated and complex in the world—and our superb people, civilian, enlisted, and officer, don't take a "back seat" to anyone in delivering quality, world-class services. But, we must continue to invest in our people and improve our capability, or we will lose our credibility and superiority, and the trust placed on our community by our Air Force. However, I'm confident that Air Force communicators will remain "leading edge" and won't become the weakest link with respect to Information Assurance.

Avoid classified security incidents on the Net

By Senior Airman Owen Freeland

21st Space Wing Information Assurance Office
Peterson AFB, Colo.

Have you ever tried to send or read e-mail only to find your server is down? If you wondered why or think it's the network folks, you should be aware it might have been you, the user, who was responsible.

The majority of server down time is associated with classified information being passed over the unclassified network. You may think that this is a rare occurrence but, unfortunately, it is rather common. When a confirmed classified e-mail is found on the network it sets an exhausting chain of events in motion. This not only affects each person associated with the contamination but all other users on the server are affected as well.

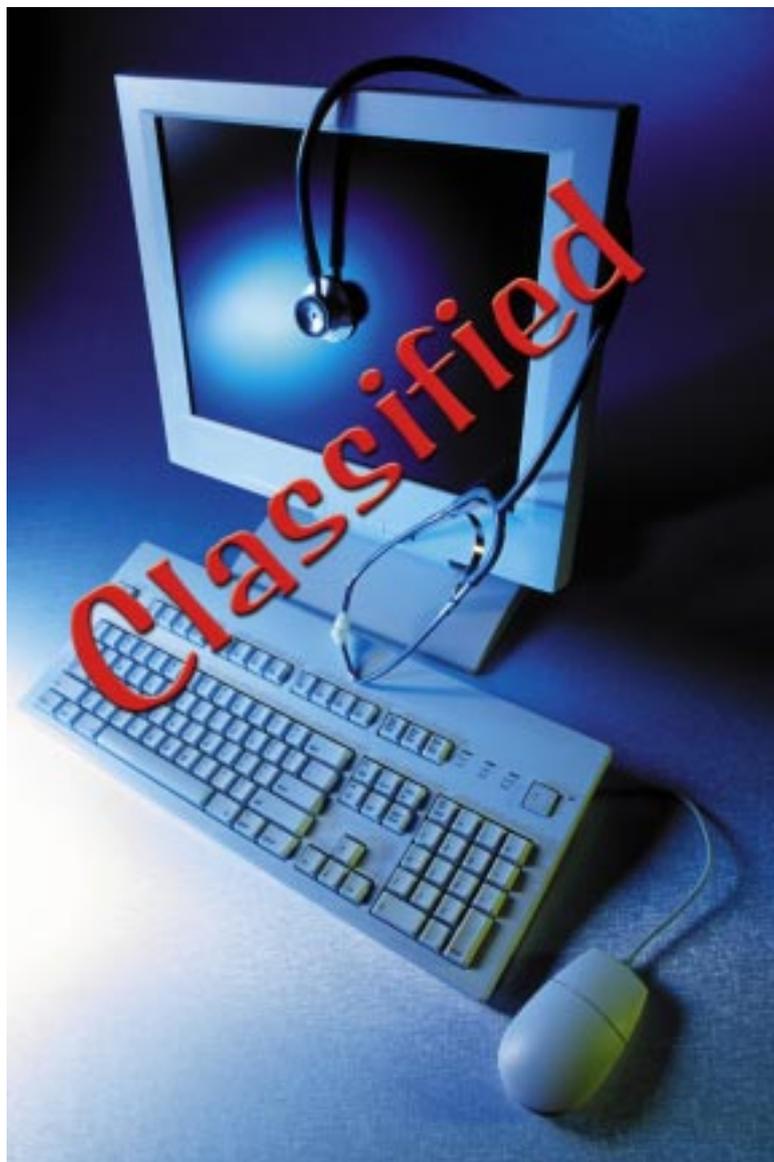
The discovery of a verified classified message on the NIPRNET will prompt the shutdown of the infected server so the NCC can find out who sent it and identify any other servers and users that were affected by the contamination. Once the total scope of the contamination is known the NCC can then isolate the information, clean the servers and restore services.

The amount of time service is down depends on the scale of corruption. If any other bases are involved, notification is also sent to them. Contamination is considered classified until all personnel, organizations, and bases have cleaned their computers, so the help desk cannot disclose any information concerning the outage until the incident is closed. Each incident requires a notification process up the chain of command to the wing commander and the Network Operation Security Center. Each and every incident is briefed in detail to the wing commander during the operations briefing. It's not a good thing to have your name listed as the cause of a computer security incident.

To prevent your name being briefed to wing leadership, you should always know the classification of the information you send out. There are a few easy steps to ensure you're not causing a classified security incident.

1. Unclassified information can become classified when combined with other classified information. The cut and paste option that we all know and love is the major reason an unclassified e-mail quickly becomes classified.

2. The key to preventing an unintentional classified e-mail is to understand the nature of the information you send and ask questions before you send the



message. A security classification guide will tell you if the information is classified. For more information and where to review a classification guide, see AFI 31-401, *Information Security Program Management*.

3. If you suspect you've received a classified message, don't send or forward it to anyone until you have verified its classification.

4. In the event that you have received or caused a security incident, immediately disconnect and secure your computer, notify your UCM or ISSO and call your help desk.

Security incidents can affect each of us and can easily be prevented through vigilance and knowing the sensitivity of the information you send. Always ask if you're unsure whether information you're working with is classified, and never send information you think may be classified.

OPSEC: How much is too much?

By Staff Sgt. Kathryn O'Neil
341st OSS Combat Crew Comm
Malmstrom AFB, Mont.

You are so excited. It's been three years since you last traveled home. You can't wait to get on that plane and spend the next few weeks relaxing and hanging out with friends and family. You board your plane and take your seat. As the plane takes off, a friendly gentleman next to you strikes up a conversation. He asks where you are going, who you will see, you know, the normal airline chit chat. Then the conversation takes a turn. He wants to know about your job and the military. What do you tell him? How many details can you give him? The Air Force created a program called OPSEC for just this reason.

OPSEC, or operations security, is defined as: The process to deny potential adversaries information about capabilities, and/or intentions *by identifying, controlling, and protecting* generally unclassified evidence of the planning and execution of military operations and sensitive activities. In other words, the OPSEC program was designed to identify critical information that could create a vulnerability to the Air Force if put into the wrong hands. When this nice gentleman next to you starts asking questions regarding things such as

the status of the missiles, or how we launch a missile, think again before answering. You can create a vulnerability by providing information that an adversary can interpret in time to provide effective decision making for their actions. For example, you know that big inspection you just went through? OPSEC dictates information pertaining to a failure during that inspection is critical and cannot be made public, because it can reveal weaknesses of a unit or base. This sort of information can give adversaries the upper hand should a conflict arise and it can aid terrorists. How do you know what information about your job is critical? Just ask your unit security manager. Every unit should have a list of critical information that pertains specifically to it. By knowing what information is critical to your unit and being aware of OPSEC, you can help prevent compromises.

So, the next time you are on a plane talking to someone about your job, remember:

- * Be aware of your organization's critical information
- * Understand how an adversary might try to obtain that critical information
- * Stay OPSEC minded. Each base has an OPSEC manager who can answer any questions you may have.

Only you can prevent computer viruses

By Staff Sgt. Robert Root
Information Assurance Manager
F. E. Warren AFB, Wyo.

"Only you can prevent forest fires!" Throughout the years it's been a popular slogan to assist with fire prevention. But, what if we change it around a little bit? "Only you can prevent computer viruses!"

Still true, but a little closer to you as a computer user. Every day, hundreds of thousands of e-mails are sent around the world—a portion of these being DOD or Air Force related material. Every day, every hour, we send e-mails to our supervisors, flight commanders, squadron commanders and countless other places on and off base.

How many of these e-mails are free from every computer virus ever made? All? Some? None? Surpris-

ingly enough, a large number of these viruses are caught and deleted as they come on and off Air Force bases. Where then do all the problems come from? The culprits are easy to tell you about, but a bit harder to stop. How about starting with floppy disks.

We pass them around with decorations, presentations and many other forms of information. We take work home on them, and we use them for hundreds of little things every day. In many ways, floppy disks have made our jobs much easier.

Wait! Stop! They are as much a problem a help. It is estimated that around 50 percent of all viruses that you encounter at work will be passed by our friend the floppy disk. And once they infect your computer, they're on the network, and can

spread like wild fire.

"Only you can prevent forest fires!"

How then, can we ensure that we don't infect our computers and computer networks? Anti-virus software is the key. Use this Air Force provided tool to scan everything on your computer, every day. Have a stack of floppy disks? Check them too! Did you know DOD employees may take a copy of the anti-virus software home to use? It's just another step to ensure the work you take home stays virus free.

In just minutes, we can prevent disaster from striking and causing chaos on our computers.

So, yes it's true: "**Only you can prevent computer viruses!**" And your local Information Assurance office can provide any information and assistance you may need.

Anything is possible ... with a computer

By Staff Sgt. Robert Root
Information Assurance Manager
F. E. Warren AFB, Wyo.

Build a better mousetrap and you will catch a better mouse. Make something foolproof, and you will create a better fool. Today, the impossible can be attained with just a click of the mouse, and the push of a key. Anything is possible with a computer.

The 1990s were the years of the Internet. It went past baby steps to a full-stride run, and looked as though it would never slow down. Almost overnight, fortunes were being made, and people were making a place for themselves. In the background, almost like in the plot of children's cartoons, the bad guy was waiting in the background.

From pickpockets to spies, the face of the "bad guy" has changed through the years, but the crimes are about the same. Theft, bribery, extortion, espionage—the sneakier the crime, the better the chance it will work. Now, with the ability to cruise around the world in mere seconds, a new level of threat has come into the hands of the "bad guys." For sake of argument let's call them hackers, or as the computer industry calls them, black hats.

Look in the news today and you'll see headlines about some kind of crime committed using computers. Hackers are breaking into corporations and stealing business secrets, new software and even large sums of money. Viruses are flying across the Internet at break-neck speeds, causing hundreds of millions of dollars of damage every year.

Yet, if you look deeper into the headlines, you will

find that less and less of the headline-making hackers are in their 30s and 40s. You must look at generation 'X,' now well into their 20s, and even to the teenagers. Anything was possible when you were young, and you were encouraged to dream. Yet dream with a computer within reach and more possibilities are born.

More and more every day I hear people around me saying, "That's impossible. You can't do this" or "Don't do that." People laugh when I say anything is possible.

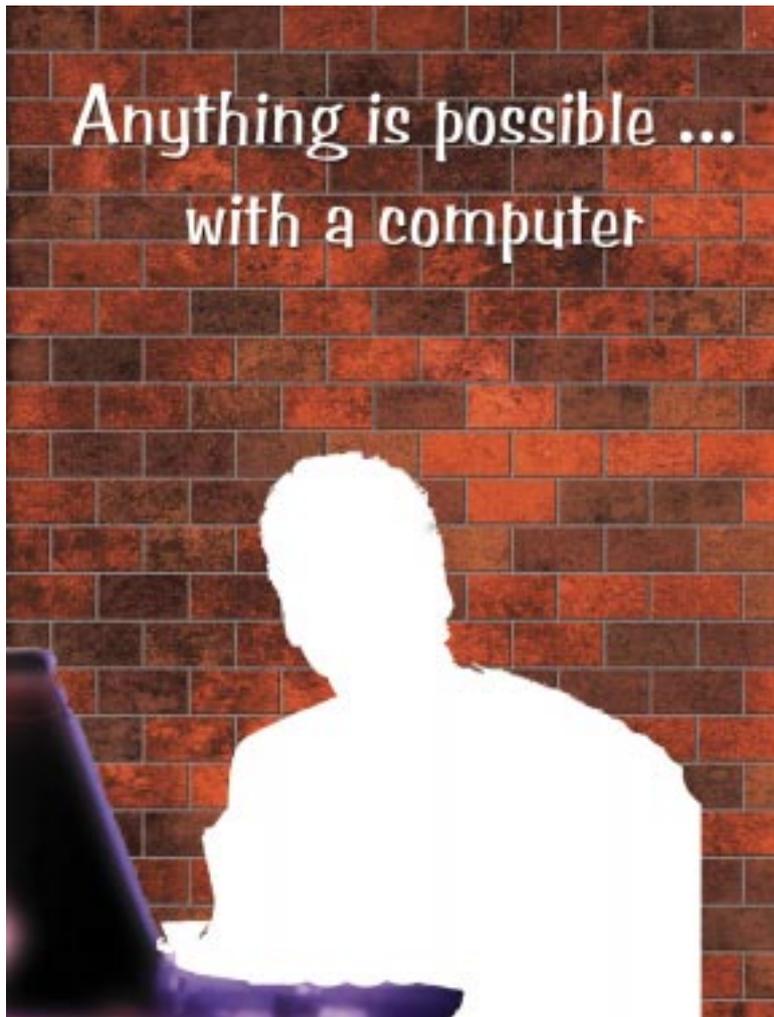
Case in point: DVD encryption. It was said encryption wouldn't be broken. Yet two individuals from MIT wrote a sic line program to decode the encryption. It can't be done, or you can't do it, and the younger generation not only says you can, but here is how you do it. To them, it's a challenge.

An even better example: A year ago, a hacker attacked two dozen computer networks and denied all activity in and out of the networks for three days, costing approximately \$30 million in damages and lost revenue. The hacker in question had just turned 16, and he just wanted to see if he could do it.

Why do I tell you all of this? It gets harder every day to predict the next bad thing that might happen, but if we don't take off our blinders

and realize that anything is possible, we're setting ourselves up for failure.

For someone that understands that *anything can be done*, it only takes seconds to exploit everything we are working to protect. Yet, for every security procedure that is followed, it's that much more difficult to gain unauthorized access. In the end, our goal should be to make our computer systems and networks as secure as possible.



Information managers keep pace with technology

WASHINGTON, D.C. — The Air Force of the 21st century is powered by information, its associated technologies and the knowledge and experience to master both. This critical relationship is nowhere more readily apparent than in Air Force Vision 2020, which acknowledges Information Superiority as a core Air Force competency. People in Air Force Specialty Code 3A0X1, more commonly known as information managers, are responsible for the effective and efficient management of information.

“At the dawning of the 21st century, it’s critical that we move swiftly to keep this career field in stride with the explosive growth in technology which has completely altered the information management landscape,” said Lt. Gen. John L. Woodward Jr., Air Force deputy chief of staff for communications and information. While some may see this as a radical change to the information manager’s role it’s actually a logical evolution which started more than a decade ago, according to Chief Master Sgt. Todd Small, career field manager of Air Force information managers.

“Changing the career field title from administration to information management in the late 1980s was an indicator of sweeping changes,” said Chief Small.

Another important milestone in this transition was in 1996 when the Air Staff directed the integration of communications-computer systems and information management to form a single communications and information functional community.

“Air Force senior leaders clearly recognized that information systems technology was central to the effective management of information,” said Chief Small.

That change resulted in information managers adding workgroup management as a central responsibility. Workgroup management includes tasks such as Web development and management, personal computer software and hardware installation, configuration and control.

In the past, information managers used typewriters, stand-alone word processors, manual mail systems and filing, storage and retrieval systems.

“Computers are simply a new tool or, better yet, a new weapon system in the arsenal of the information manager,” said Chief Small.

The Air Force still needs information managers who possess knowledge of records, administrative communications, publications and forms.

“Knowledge of these functions is fundamental to the management of information, be it paper- or electron-based, throughout its life cycle,” said Chief Small. He

added, “It’s not as though we’re starting with a clean slate ... we’re simply going to leverage the good from the past with the good from today. We’re going to create an Air Force specialty code skilled at managing a broad range of information resources, by coupling the structure and discipline long associated with information management processes to the tremendous computing power of today’s information systems.”

Another battle faced by information managers is to keep pace with changing technology used to manage information. Unfortunately, status quo will never be good enough, because technology continues to create better methods of managing information, according to Chief Small.

“The Air Force Portal, electronic records management, and electronic workflow and staffing significantly change how information is controlled. This evolution will continue as these new emerging technologies are developed and adopted,” the chief said.

During the past several years, training for information managers has changed dramatically to keep up with technology.

“For example, our 3-level course migrated from a 19-day self-paced course to 37 days of instructor-led instruction focused on the information life cycle and the technologically based tools used to manage that life cycle,” Chief Small said.

Keeping training current isn’t easy because of the speed of technological advances.

“Despite this training challenge, I’m convinced today’s information managers are better prepared and more qualified than in the past to provide our customers the expertise and guidance to organize, integrate, and handle information as a critical national resource to achieve the Air Force mission,” said Chief Small.

The key to the success of this effort is correct use of information managers.

“Commanders and supervisors must exploit the expanded capability of the information management career field and use these people to improve and streamline the management and processing of information and control of information resources,” said General Woodward.

Both General Woodward and Chief Small emphasized the need for commanders and supervisors to maintain close contact with the information management functional managers at their base or headquarters to stay abreast of the rapid changes facing the career field.

Air Force Virtual Private Network: big score for information operations

By Craig Boke

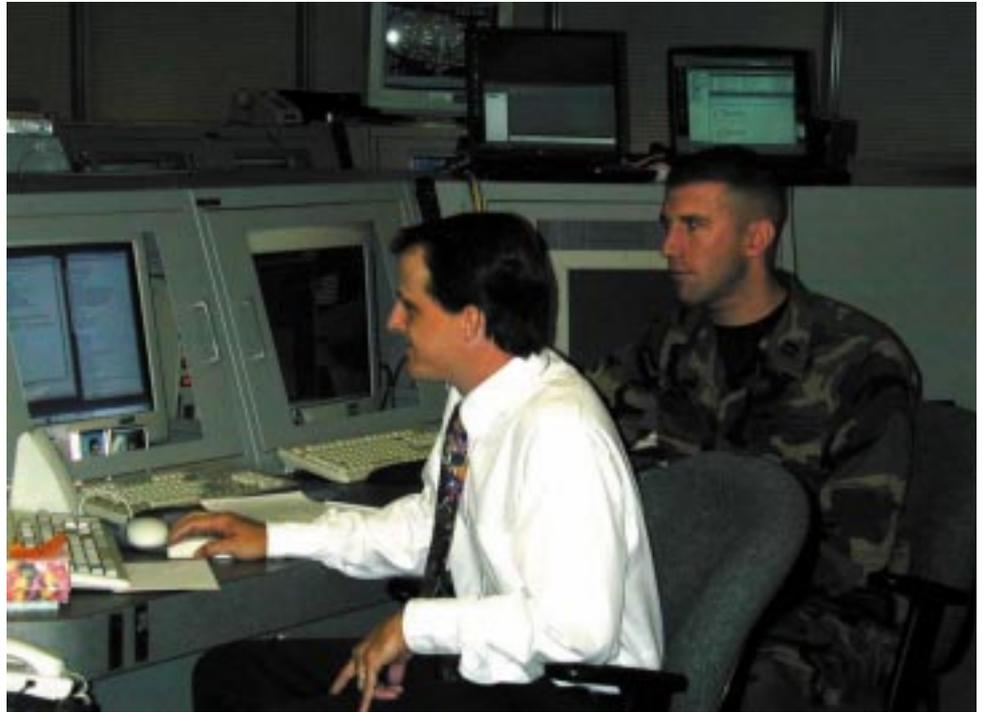
Chief, Wide Area Networks
Office of the Air Force
Deputy Chief of Staff
for Communications and
Information
Washington

A new plateau was reached this summer in the *One Air Force ...One Network* vision with implementation of the Air Force Virtual Private Network. AF VPN encrypts all traffic flowing between Air Force bases, increases bandwidth by 600 percent, makes networks much more reliable, secure and powerful with top notch Cisco routers at all main operating bases. We avoid millions of dollars in costs by precluding the need to implement other methods of protecting sensitive data for each system.

Air Force VPN represents the most significant contribution to information operations in years. But the true significance of this “big score” is not just technical. The VPN story is a powerful demonstration of communications warrior teamwork in action. Never in networking history has the Air Force established such a robust capability in so short a time.

We’re a network-centric Air Force. Networks are critical to combat effectiveness. Evolution of these networks to keep pace with expanding user populations and Web-based applications is an art as much as a science. The art involves anticipating growth and timing network enhancements so the right capability is delivered on time. We have to spend our precious time and resources on efforts that bring the most significant benefits. The science involves staying current with technology without being on the “bleeding edge.” To serve the network-centric Air Force, we have to be innovative, and to understand our operational context and limitations.

What is a VPN? Private networks use dedicated long-haul routers and switches to form a closed network, which can only be accessed by users who are



Ron Volnoff (left) and Capt. Matt Camacho, Air Force Network Operations Center, Maxwell AFB-Gunter Annex, Ala., coordinate with major command network operations security center and NCC individuals as they remotely configure another base into the Air Force VPN.

physically connected to one of these links. VPN technology uses encrypted “tunnels” within an open network to create a “virtual private network” without having to own the infrastructure and interconnecting links. Users can access the VPN only if they are specifically added to the configuration. When communicating between these “private” endpoints, traffic can’t be intercepted, viewed or altered. Authenticity can be verified because it has to be encrypted using a special key. This prevents hackers from “hijacking” a session and “spoofing”—or inserting their own traffic. Traffic that’s not properly encrypted is discarded, foiling any spoofing attempt. The Air Force VPN employs the same process over NIPRNET.

Why is VPN important? Never before in the history of Air Force networking have we been able to implement such a significant increase in capability and security. By protecting all traffic, we precluded the need for every function to individually implement costly solutions to meet DOD security mandates.

Refreshing the all-service delivery point routers gave the Air Force a robust, standardized foundation to keep pace with networking needs. By providing the same look and same feel, management and logistical support was simplified. Standardization of the top-notch Cisco 7206VXR platform gave the Air Force greater security, reliability, scalability and performance capabilities. AFCERT and JTF CND advisories could be more easily implemented. Every member of the VPN reaped these benefits. Another important consideration was implementation method. We harnessed the strength and cooperation of major command and base communicators to complete installations in record time.

The Air Force began the effort to add VPNs to our defense-in-depth strategy to protect sensitive unclassified data and prevent spoofing. Our networks faced risks from information warfare threats and hackers. One of the major concerns is protecting sensitive information flowing over our networks. Remote management of network components and computer systems required the transmission of system passwords. A hacker intercepting one of these sessions could gain enough knowledge to access our systems. Other sensitive military information was vulnerable to intercept across unprotected wide area networks. We had to come up with a way to mitigate these threats. Additionally, the majority of Air Force systems transmitted some form of sensitive data, and therefore faced the high cost of implementing individual methods of securing data. Proliferation of individual solutions would have severely hampered the base Network Control Center's ability to support network users and significantly increased cost. A VPN solution would protect all traffic flowing across the wide area network, and all systems with a standard solution, while providing NCCs visibility to diagnose problems within the base enclave.

Communications and information warrior teamwork began as an architecture working group established and co-chaired by Headquarters Air Force and Air Force Communications Agency. The group included members from major commands, field operating agencies and various functional communities concerned about protecting sensitive data. The group defined requirements, architecture and issues related to implementing and managing a solution.

Product evaluation was initially performed by the Combat Information Transport System program management office, at Hanscom AFB, Mass., which helped narrow the field to two candidate solutions. One solution involved a separate device and the other made use of an internal feature in Cisco routers. It became evident that NOSC's and NCC's would find it difficult to maintain the VPN because of wide area network protocols involved with either solution. The expertise of NOSC's and NCC's was correctly focused on maintain-

ing our base networks, rather than the WAN. At this point, the MAJCOM CIO's voted to have AFNOC centrally manage the VPN, due to its expertise in WAN protocols.

The final evaluation effort was transferred to the Air Force Systems Networking program management office at Maxwell AFB-Gunter Annex, Ala., which is responsible for engineering classified and unclassified WAN service delivery points, and supporting the AFNOC. After extensive testing, AFSN determined the Cisco solution was better for the Air Force, since it better leveraged the existing knowledge base of AFNOC personnel, and freed funding to buy external equipment and accelerate replacement of Service Delivery Point routers.

Before the VPN could be rolled out Air Force-wide, operational test and evaluation was performed with 16 bases. Testing revealed a major showstopper. Most of Air Force systems had communications settings hard-coded into the software. Specifically, the "do not fragment" and "maximum packet size" settings created problems when encryption was added, causing packets to exceed maximum size, forcing fragmentation, and preventing proper operation of software. This was a serious problem, since it potentially required modification of thousands of programs. AFSN and AFNOC sprang into action. Working with Cisco, they modified the router's integrated operating system to ignore software settings, and made other improvements to optimize VPN performance. Fortunately, this fixed the problem and the deployment decision was made by AF/SCMN after testing validated the final configuration.

Implementation

What really made this project such an achievement is how it was implemented. For a number of years, we'd been treating some of our infostructure projects like we were building airplanes or missiles. Development and implementation often took too long, and by the time we finished, the solution was sometimes obsolete. We couldn't afford long lead times, because technology was evolving too quickly. We needed to get commercial off-the-shelf equipment implemented in one year, use it for a couple of years, and then upgrade to the next level. Our existing acquisition approach lacked the immediate responsiveness we must have. On this project we tried something new – which paradoxically was something old. We leveraged comm warriors at bases to help do the work.

The old Defense Data Network PMO, which brought us the DDN concentrator and the Air Force Internet, was famous for blitzkrieg-style implementations. They bought equipment, configured it, and sent it to bases for installation by the "node site coordinators," or PMO

See **VPN** Page 26

VPN

From Page 25

gurus. This enabled simultaneous multiple installations by local comm squadron personnel. The AFSN PMO was created from the old DDN PMO and still had some of the original crew from AFIN days. There was no reason we couldn't still employ these assets to expedite implementation. In jest, I instructed my lead engineer, "This isn't an airplane we have years to build – think like Silicon Valley. Get it done in six months or you're fired!" What followed was nothing short of amazing. By May, every base had a brand new router and by August the world's largest, fully meshed IPSEC VPN (103 bases) was fully operational.

The coalition of PMOs, MAJCOM staffs, NOSCs, NCCs and Cisco deserve major recognition for making this quantum leap a reality. This project showed what the comm and info community can accomplish when it sets its mind to it. This was a real team effort. AFSN shipped the new routers out to the bases with instructions, then AFNOC arranged cutover schedules with NOSCs and walked NCCs through the steps. NCC personnel did the hands-on work. This project gave everyone a chance to exercise important skills. New routers were installed and powered up in advance, and then connection cables were simply swapped over to the new router. Once new routers were on-line, AFNOC remotely configured them. We had a few router failures, but those problems were quickly resolved. Next we deployed an additional card for the router, which off-loaded encryption work from the main processor. The hardest part was getting permission to take the WAN off-line long enough to switch over.

An early benefactor of VPN was Air Force/DP. MILMOD required protection of its data to meet certificate of worthiness. AFPC faced either having the VPN in place or investing \$700,000 in an alternate solution. To meet the May operational deadline, we first implemented the VPN between all bases and Randolph AFB, Texas. To decrease risk, we needed to get new routers in place, because improved processors would better support increased load. During this time, rising international tensions in the Far East, and general concern about the Red Worm virus, made some units reluctant to transition to the new routers. After weighing the options, we decided to put our best equipment in place before conditions deteriorated. Major military action was averted, and when the virus did appear in July, our routers continued to function effectively. Using the new routers and the VPN feature in the software, MILMOD support was achieved on time.

Complementing the new routers were multi-megabit NIPRNET upgrades for main operating bases, which were raised from 1.544MB connections to between 9-21MB. This represented at least a 600 percent increase

in NIPRNET bandwidth for every base. AFSN, AFNOC and DISA worked hard to get additional bandwidth to the bases.

Key Capabilities

VPN afforded a number of key capabilities. Since it created better trust relationships between Air Force bases, we were able to modify security rules, allowing better functionality for internal applications and improving firewall performance. Remote management of key routers and servers could be done with much less risk. VPN precluded transitioning everyone to Secret-high networks for protection from hackers.

The next step is to build on our success. Air National Guard and Air Reserve bases are being added. Expansion to include the Defense Enterprise Computer Centers is next on the agenda. The AFSN PMO and DISA are finalizing plans to host additional AFNOC managed SDPs at those facilities to encrypt sensitive data. With VPN in place to each Defense Enterprise Computing Center, the Air Force will protect the majority of traffic other than Web surfing. Another near-term objective is to revise architecture for remote access. AFSN is developing a VPN client based solution. With VPN client software installed, authorized users will access VPN remotely, using an Internet service provider or dialup. This will improve security for temporary duty personnel, partners, remote locations and personnel working from home.

The Air Force network weapon system is more secure than ever. Homogenizing every base with top of the line equipment increased overall reliability. Bandwidth upgrades helped us stay ahead of demand. VPN technology proved to be an effective way to protect the authenticity and integrity of WAN traffic and improve firewall performance. Turning on a feature in the router's software and adding an accelerator card to our base gateways was relatively easy. These simple but substantial steps equaled big improvements. The most noteworthy accomplishment was the way our Air Force communications and information warriors teamed to implement the project. Having local personnel do the touch labor saved thousands of travel dollars and accelerated implementation by 18 months. More importantly, the entire community shared in the pride of making this event happen. It provided a model for implementing future projects using the team approach.

This story needs to be shared throughout the Air Force, DOD and other federal agencies, so they too can economically comply with mandates to protect sensitive information.

For more information, contact Capt. Matt Camacho at AFNOC (DSN 596-5771 opt 2219) or Capt. Kenneth Morris at AFSN PMO (DSN 596-6116).



By Joseph Brown

Legal Office

Air Force Communications Agency

Scott AFB, Ill.

A new AFI 64-117 provides updated rules and instructions for IMPAC card use. Now you can take that plastic card and buy more government required stuff with fewer restrictions. However, there are some important basics users need to know. There are a number of rules regarding IMPAC card spending limits:

- * There's a limit of \$2500 for purchase of supplies, equipment and non-personal services. These purchases are exempt from laws and clauses requiring competition.

- * The card may be used to purchase from the Army and Air Force Exchange Service and all other DOD Nonappropriated Fund Activities. The limit is \$25,000 for Federal Prison Industries (UNICOR). Purchases up to \$100,000 are authorized with the Defense Automated Printing Service. Education personnel may pay for training and education up to \$25,000 for an individual event, or series of the same training event, activity, service or course material.

- * Up to \$25,000 may be used for Federal Supply Schedule, Blanket Purchase Agreement and Indefinite Delivery-Indefinite Quantity contracts.

- * Overseas cardholders may make commercial purchases up to \$25,000 from vendors located outside the U.S.

However, don't forget the old rules governing IMPAC use. You still need approval from the controlling and servicing organization to purchase the following supplies, equipment or non-personnel services:

- * Books, periodicals and manuals
- * Business card purchases from Lighthouse for the Blind, Inc.
- * Civil engineer material and real property
- * Communications and computer equipment and software
- * Express Next Business Day Small Package Delivery Service

IMPAC users need to know the rules

- * Paid advertisements
- * Rental or lease of material handling equipment and fleet motor vehicles
- * Telephone instruments, cell phones and expansion plug-in cards
- * Visual information, electronic digital imaging, and video equipment and services

Basically you need to follow these steps in using your IMPAC card:

- * Identify the purchase needed
- * Verify the dollar amount is within approved limits
- * Contract the supplier (Will the vendor accept the card?)
- * Give the card number and tax exempt status
- * Give your name and shipping address
- * Always request a receipt
- * File the receipt(s)
- * Match receipts with monthly statements
- * Provide receipts to the certification authority
- * Once the statement is sent to the billing office and payment is remitted, the process is complete for that month

Finally, remember the IMPAC card is not authorized for the following uses:

- * Cash advances
- * Travel related expenses
- * Construction services exceeding \$2000
- * Controlled cryptographic items
- * Gifts (for example, for retirements or farewells)
- * Major telecommunications systems
- * Ratification actions
- * Renting or leasing buildings or land
- * Repairing leased vehicles
- * Utility services

To keep up to speed, you must complete annual refresher training. Further, if you don't use the IMPAC card when available, you must justify the reason in writing to your local contracting officer.

The Air Force has a goal of greater than 90 percent use for small purchases.

Last, remember if you can't legally use appropriated funds for purchase by another contracting process, you probably can't use your IMPAC card as a way around the restriction. If you do have questions, contact your local IMPAC card advisor, or call Joseph Brown, AFCA Judge Advocate's Office, at DSN 779-6060.



U.S. AIR FORCES IN EUROPE