NATIONAL AIR INTELLIGENCE CENTER

Headquartered at Wright-Patterson Air Force Base, Ohio, the National Air Intelligence Center, a component of the Air Intelligence Agency, is the Air Force's single, integrated intelligence production center and is the primary Department of Defense producer of foreign aerospace intelligence.

The NAIC assesses current and projected foreign forces, threat and weapon system capabilities and employment, develops targeting and mission planning intelligence materials and evaluates evolving technologies of potential adversaries.

NAIC products and services play a key role in assuring that American forces avoid technological surprise and can counter the foreign air and space threat. NAIC and constituent units provide center customers a broad range of integrated, tailored assessments and information operations products and services.

These services and products directly support Air Force operational units, national decision makers, as well as the research and development sustaining the acquisition of United States air and space weapons systems. The combat effectiveness and survivability of advanced weapons and support systems, both in the field and in development, depends on the accuracy of NAIC intelligence.

The National Air Intelligence Center develops its products by analyzing all data available to the U.S. intelligence community on foreign air and space forces and weapon systems to determine performance characteristics, capabilities, vulnerabilities and employment.

NAIC assessments are also an important factor in shaping our national security and defense policies. As the Department of Defense experts on foreign aerospace system capabilities, center members have historically been involved in supporting U.S. weapons treaty negotiations and verification.

Center responsibilites cover the full range of air and space systems and technologies including:

- **aircraft**
- **missiles**
- **space systems**
- **radars**
- **electronic and electro-optic countermeasures**
- **integrated air defense systems**
- **command, control and communication systems**

Sophisticated data processing, en-

The National Air Intelligence Center's Electronic Warfare Signals Laboratory.

National Air Intelligence Center

gineering and modeling techniques enable NAIC analysts, technicians, scientists and engineers to fulfill the center's mission.

Another core NAIC mission area is the processing and exploitation of Measurement and Signature Intelligence. NAIC serves as the National and Department of Defense executive agent for processing, exploitation, integration, reporting and dissemination of MASINT data collected from radar, electro-optical and infra-red technical sensors.

NAIC prepares spectral, spatial and temporal signatures of threat targets in support of air and space forces, develops analytical tools for technical analysis and provides technology transfer of these techniques for fusion of MASINT data in the operational environment.

NAIC is the nation's only exploitation organization for imagery collected under the Open Skies Treaty. It serves as the exploitation agency for Signals Intelligence collected for the RC-135 Rivet Joint and Combat Sent missions and is the Department of Defense organization for the development of machine translation tools.

HQ NAIC traces its roots back to the Foreign Data Section of the Airplane Engineering Department, formed in 1917, at McCook Field in Dayton, Ohio. The section studied foreign aircraft, translated foreign language aerospace publications and maintained a technical library.

Ray Austerman, NAIC, removes large prints from an IRIS printer.

During World War II, the Army designated the unit the Technical Data Laboratory and depended upon it for information on enemy aircraft technology. By the end of 1945, nearly 750 people were at work at the unit, then known as "T-2 Intelligence," evaluating captured foreign aircraft and translating, indexing and microfilming technical documents.

In 1951, the S&TI mission fell upon the Air Technical Intelligence Center, its primary focus Soviet technology. In July 1961, the Air Force deactivated ATIC, yet activated another unit to take over its manpower, mission and facilities.

The National Air Intelligence Center's 24-hour Watch Area.

The Air Force Systems Command's Foreign Technology Division was the organizational beginning of today's National Air Intelligence Center. Since the beginning of its organizational lineage in 1961, the units mission and resources have expanded to meet the challenges of worldwide technological developments and the accompanying national need for aerospace intelligence.

In recent years, the emphasis has increasingly shifted toward evaluation of worldwide aerospace systems and the production of "tailored," customer-specific products.

NAIC was formed Oct. 1, 1993, with the integration of the Foreign Aerospace Science and Technology Center and the 480th Intelligence Group.

Headquarters NAIC employs more than 1,600 people. Subordinate units at Langley Air Force Base, Va., and Offutt Air Force Base, Neb., form the 480th IG, and provide support to NAIC operational customers.

The five divisions of the Directorate of Intelligence Analysis, located at the Pentagon and Washington, D.C., area, provide tailored, substantive military intelligence to the Air Force Chief of Staff, the Secretary of the Air Force, Air Staff and other Department of Defense and national customers.

Besides their commitment to the mission, the 2,059 people that work for NAIC are actively involved in many community projects helping people. Tutoring children at a local school, coaching youth sports teams, working with Habitat for Humanity in building houses for the less-fortunate, working with kids that have mental and physical challenges, adopting a highway, organizing local food and blood drives and sponsoring the Wright-Patterson Air Force Base Annual Sports Day.

NAIC people are leading the way, making the community better.

As our nation enters the information age of the 21st century, the need for tailored air and space intelligence and information operations products and services will continually increase.

As information operators on the AIA team, NAIC will continue to provide the nation's military forces the tailored intelligence products essential to precision employment and information-based warfare, expanding the Air Force's capability to conduct information operations and achieve information superiority.

480TH INTELLIGENCE GROUP

Supporting the operational forces by providing timely intelligence information

With headquarters located at Langley Air Force Base, Va., the 480th Intelligence Group is a component of NAIC.

Langley is a long standing establishment on the lower peninsula of Virginia. It is a major contributor to the entire community known as the Tidewater area, which is located within minutes of several major cities including Norfolk, Hampton, Newport News and Colonial Williamsburg. The capital, Richmond, is only an hour away.

The 480th, formerly an Air Combat Command organization, provides conventional mission planning support and target materials, multi-source intelligence analysis and operational intelligence required to train, prepare and support in-garrison and deployed combat air forces.

MISSION

The 480th's specific mission is to process and apply intelligence and other information using state-of-the-art capabilities to provide timely, relevant and accurate products and services for the operational air forces.

VISION

The unit's vision is "Center of Excellence," providing imagery-focused multidisciplined intelligence for global information superiority, committed to vigilance.

Through sophisticated communications and computer systems, the 480th provides the deployed war fighter direct access to the comprehensive assets of the NAIC.

The unit is organized into three subordinate squadrons:

- **20th Intelligence Squadron**
  Located at Offutt Air Force Base, Neb., was assigned in 1992.
- **27th Intelligence Squadron**
  Located at Langley Air Force Base, Va., was assigned in 1990.
- **36th Intelligence Squadron**
  Located at Langley Air Force Base, Va., was assigned in 1990.

Also, the 123rd Intelligence Squadron, an Arkansas Air National Guard Unit, located at Little Rock Air Force Base, is gained during wartime.

Subordinated squadrons provide both scheduled and ad hoc intelligence tailored to the unique, immediate needs of air warfighters. They employ the concepts and processes of virtual production, application utilizing a myriad of state-of-the-art information processing and production systems and on-line databases.

The unit has committed itself to being ever vigilant of the constant advances in information processing, storage and dissemination technologies. It is also recognized throughout the intelligence and operational community as a leader in the testing, evaluation and application of new technologies to meet the needs of current and emerging weapons systems and their employed munitions.

The unit has been instrumental in recent innovative programs and projects that included the development of digital target materials, production of digital materials for Air Force Mission Support Systems, virtual production and providing air combat units with near-real-time imagery information for mission planning and execution.

Since its origination in 1969, the 480th has been awarded five Air Force Outstanding Unit Awards.

20TH INTELLIGENCE SQUADRON

EMBLEM

The patch was approved in 1958. The cloud and sky are symbolic of the squadron's historic flying mission.

"Yosemite Sam" represents

National Air Intelligence Center

Staff Sgts. Anthony Turner and Abigail Figueroa, both with the 20th IS, research statistics and trend analysis.

squadron personnel carrying on the activities of the unit, map reading, target location and visual reconnaissance. Sam's gun is symbolic of target-making weapons and devices, and the camera system indicates photographic reconnaissance.

The lightning bolt represents direct destruction from the air, artillery adjustment and fighter strikes.

The 20th IS provides mission planning support primarily to bomber units in support of U.S. Strategic Command. It maintains liaison between NAIC and U.S. Strategic Command on nuclear targeting, weaponeering and battle damage assessment issues.

MISSION

The mission of the 20th is to provide prompt, precise intelligence enabling warfighters to safely engage and achieve global objectives.

The 20th processes and analyzes raw electronic intelligence data, and prepares both operational and technical ELINT reports and studies.

The 20th is organized into three flights:

- **Target Materials**
- **Combat Applications**
- **Operations**

The Target Material Flight produces precise coordinated measurements and mission-support materials for Air Force bomber, fighter and other airborne platforms engaged in exercise, training or actual combat operations.

It provides graphics, coordinated measurements and aim point selection assistance supporting nuclear, conventional and humanitarian relief operations. It also performs distribution of maps and charts supporting short-notice mission planning and flying requirements Air Force wide.

The Combat Applications Flight activities entail providing direct application support for specified combat customers. This includes an AIA node for operational dissemination of near-real time imagery to Air Force and Department of Defense users worldwide; and is Air Combat Command's point of contact for pre-mission survivability and threat assessments, target analysis, weaponeering support and post-mission combat assessments for the Conventional Air Launched Cruise Missile program.

Additionally, it performs modeling and simulation survivability analysis studies for requesting customers and is the executive manager for the Integrated Air Defense systems efforts.

The Operations Flight provides the day-to-day operating support to the other flights within the 20th. These activities are dispersed through branches who perform the activities of planning, requirements management, systems maintenance, logistics support and resource management.

The 20th IS began its origins as the 20th Photographic Mapping Squadron in 1942. In these early years, the unit worked under many different names and was stationed all over the world from Sydney, Australia, to Newark, N.J., to Yokota, Japan. They participated in the Pacific air offensive and the occupation of Japan until inactivation in 1946.

The 20th was back in service for the Korean War as the 20th Tactical Reconnaissance Squadron until 1967. In 1992, it was reactivated and designated the 20th Air Intelligence Squadron under the newly formed Air Com-

Senior Airman Kerry Crossley with the 20th IS, uses NIMA's Dewdrop workstation to mensurate coordinates.

bat Command, operating out of Offutt Air Force Base, Neb.

A year later, it was redesignated as the 20th Intelligence Squadron under the Air Intelligence Agency.

Offutt Air Force Base, Neb. was established in 1896 as Fort Cook, and is currently the oldest "fort" west of the Mississippi River.

Fort Cook was named after Gen. George Cook, who was famous for more than 20 years of service during the Indian Wars.

In 1924, they added a runway and the base became Offutt Air Field after Lt. Jarvis Offutt, Omaha's first air casualty. It became Offutt Air Force Base, Neb., in 1948 when the Army and Air Force became separate services.

Senior Airman Jermaine Jones, with the 27th IS, removes a print from the printer.

Offices of the 20th IS are located in the Martin Bomber Building, the same building that manufactured B-26 Marauders and B-29 Superfortressess.

Both the "Enola Gay" and "Bock's Car," the B-29s which dropped atomic bombs on Hiroshima and Nagasaki were built here. The Martin Bomber Building, or Building D, is one-third the size of the Pentagon.

27th Intelligence Squadron

The 27th Intelligence Squadron's mission is to expertly serve the 480th IG and other Department of Defense organizations using skilled professionals and leading edge technologies and to develop, provide and manage systems and production infrastructures and services.

The 27th IS is responsible for sustaining the 480th's daily operations. It operates and maintains automated production support systems, a secondary imagery dissemination system and photographic and lithographic facilities for the group.

Their vision is to become an unrivaled source of information warfare support and achieve a virtual based infrastructure to fuse multimedia applications and products through emerging technologies and state-of-the-art facilities in anticipation of customer needs for information dominance and operational supremacy.

The 27th provides the communication, photographic, dissemination and facility, security and logistics management necessary for the 480th to deliver high-quality, time-sensitive, imagery based intelligence for dissemination to U.S. and allied warfighters around the globe.

The 27th Intelligence Squadron is comprised of two flights:

- **Production Services**
- **Systems/Data Base Management**

The Systems and Database Management Flight provides state-of-the-art communications and computing and the Production Services provides a broad range of essential services.

The Visual Information Branch provides digital and wet imagery processing, still photography and 35mm slide production, high-speed, large-volume reproduction and graphic design.

The Dissemination Branch distributes and tracks all outgoing products, maintains a chart library with worldwide coverage and the basic target and training graphic repository.

Also, the Security Branch manages the group's programs and maintains unit and visitor security clearances and facility security devices. The Facility Branch manages the entire facility and grounds including upgrades and construction. The Logistics Branch manages the group's supply and equipment accounts.

The unit was active during World War II when it won seven campaign streamers, a Distinguished Unit Citation and the French Croix de Guerre with Palm. The 27th was inactivated in December 1945 then reactivated in September 1990.

EMBLEM

Bat outa hell: red cloaked batman with oxygen mask and headset

Aerial Cameras: model K-17, 18, 22, 24 in various formats

Map Section: connecting the twin fuselage

White cloud formation: highlighting the batman and representing the sky

P-38 Lightning: unique twin-boom airframe, fastest long-range fighter

National Air Intelligence Center

Lightning Bolts: Representing the aircraft's name, and the crew's flying style

Bare metal: flying without paint shaved an extra 300-4000 pounds, given it more speed

Blue: as camouflage to hide form gunners as they made high speed runs over defended targets

Normandy stripes: often left to keep our gunners from shooting down single or small groups of P-38s

Nose art: Like most WWII flyers, F-4 and F-5 crew often personalized their aircraft. They often painted small swastikas on the nose for each mission over enemy territory.

36th Intelligence Squadron

The 36th IS provides tactical target materials, special targeting and weaponeering analysis, and tailored digital data bases to support U.S. Air Force weapons systems, mission planning and aircrew training.

The squadron also provides focused and tailored intelligence to meet the specific requirements of Air Force units preparing for deployment, while they are deploying, and during the time they are deployed.

The 36th is organized into four flights:

- **Digital Materials**
- **Intelligence Applications**
- **Targeting/Recognition Materials**
- **Requirements Management**

The Digital Materials Flight provides accurate digital maps, charts, elevation data, detailed geocoded imagery and other digital products supporting automated mission planning needs and unique requirements for advanced weapon systems.

It serves as the Air Force's sole producer of multi-spectral imagery.

The Intelligence Applications Flight supports combat air forces, training units, the NAIC and AIA staffs by producing materials, targeting analysis and specialized target studies.

The Targeting/Recognition Materials Flight produces ad hoc and scheduled general military intelligence to support exercise, training and combat operations of the Air Force and other Department of Defense aircrew members the same type of target materials they will be using in operational conditions as well as producing prototype target materials for future and developmental weapon systems.

The Requirements Management Flight assigns and tracks all ad hoc and scheduled production requirements. They also submit, track and monitor associated all-source intelligence collections.

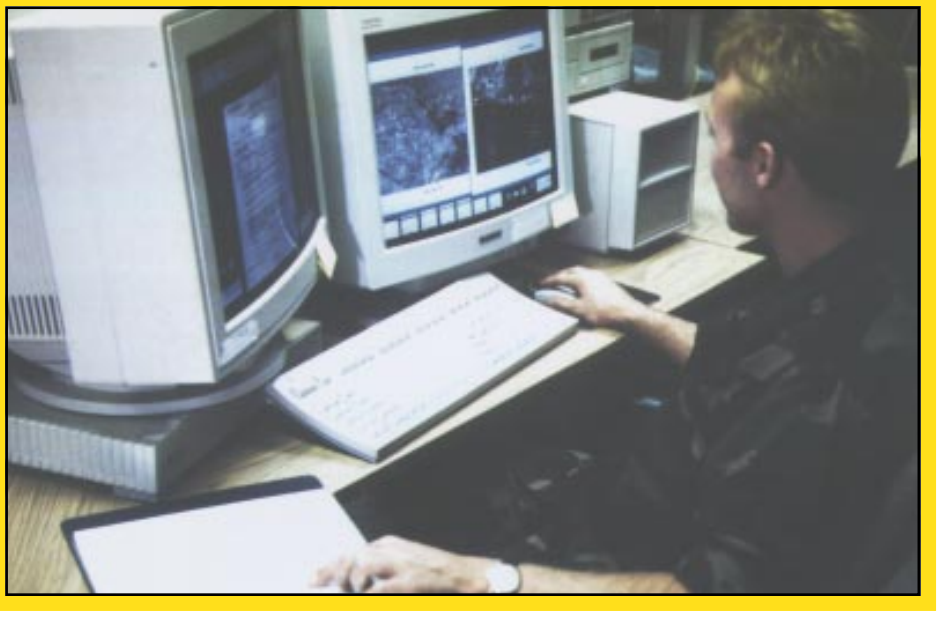
The 36th was originally called the 28th Observation Squadron July 1942 and activated at Goodman Field, Ky.

The 28th held many different designations including the 28th Reconnaissance Squadron, April 2, 1943; the 28th Tactical Reconnaissance Squadron in August; the 36th Photographic Mapping Squadron in October; and the 36th Photographic Reconnaissance Squadron, March 1944.

In those early years, the unit served in the United States, New Guinea, Philippines, Okinawa and Chofu, Japan.

The 36th PRS was inactivated in February 1946. In September 1990, the unit was redesignated as the 36th Tactical Intelligence Squadron at Langley Air Force Base, Va., and assigned to the 480th.

In November 1991, the 36th TIS was redesignated as the 36th Air Intelligence Squadron and in October 1993, it was redesignated as the 36th Intelligence Squadron.



Senior Airman Dwayne Russler, 36th Intelligence Squadron's Target Materials Flight, conducts a test to quality control an operating instruction.

AIR FORCE INFORMATION WARFARE CENTER

The Air Force Information Warfare Center, collocated with the Air Intelligence Agency, was created to be an information superiority center of excellence, dedicated to offensive and defensive counter information and information operations.

AFIWC was originally activated as the 6901st Special Communication Center in July 1953. The following month the 6901st was redesignated as the Air Force Special Communications Center. It was then redesignated as the Air Force Electronic Warfare Center in 1975.

Air Force successes in exploiting enemy information systems during Desert Storm led to the realization that the strategies and tactics of command and control warfare could be expanded to the entire information spectrum and be implemented as information warfare.

In response, the AFIWC was activated Sept. 10, 1993, combining technical skills from the former AFEWC, the Air Force Cryptologic Support Center's Securities Directorate and intelligence skills from the former Air Force Intelligence Command.

AFIWC's team of 1,000 military and civilian personnel are skilled in the areas of operations, engineering, operations research, intelligence, radar technology, communications and computer applications.

The members are dedicated to providing improved C2W/IW capabilities to the warfighting U.S. Air Force major commands.

Photo by Boyd Belcher

Air Force Chief of Staff, Gen. Ronald Fogleman (right), discusses the mission of the Information Warfare Battlelab with Col. James Massaro, AFIWC commander.

MISSION

The mission of AFIWC is to explore, apply and migrate offensive and defensive information warfare capabilities for operations, acquisition and testing; and provide advanced IW training for the Air Force.

The AFIWC provides IW services to the warfighter in contingencies and exercises through quantitative analysis, modeling and simulation, database and technical expertise in communication and computer security.

The AFIWC is divided into eight directorates:

- **Advanced Programs**
- **Communications-Computer Systems**
- **C2W Information**
- **Engineering Analysis**
- **Mission Support**
- **Systems Analysis**
- **Operations Support**
- **Information Warfare Battlelab**

The newest directorate, the Information Warfare Battlelab, supports the full spectrum of Air Force operations by rapidly identifying innovative and superior ways to plan and employ IW capabilities; organize,

Air Force Information Warfare Center

train, and equip Air Force IW forces; and influence development of IW doctrine and tactics.

Advanced Programs foster the development and employment of advanced IW capabilities using a multi-disciplined approach. They explore and advance technologies, techniques, talents and tactics for IW applications. Developing multi-disciplined (scientific, technical, intelligence and operation) solutions, they provide support for emerging warfare techniques.

Communications-Computer Systems provides the command, control, communication, computer and information systems infrastructure to support all AFIWC mission areas. SC develops C4I systems architecture and initiates programs for their implementation or acquisition.

Using all-source data, C2W Information develops, builds, extracts and integrates standardized C2W data into the Air Force Extended Integrated Data Base architecture. DB addresses the issues of control, quality assurance planning, training, development, deployment, technical support and implementation of new databases.

Engineering Analysis provides technical guidance in the areas of computer security during the development of information, sensor and weapon systems including in-depth analysis and electromagnetic measurements of aircraft.

The Air Force Computer Emergency Response Team is the Air Force's global command center for handling worldwide networked computer system security issues. The AFCERT is the single point in the Air Force for reporting networked computer intrusions and problems. AFCERT responded to 47 computer security incidents in 1996 and expanded its internal security database

Photo by Boyd Belcher

Left, Maj. Byron Thatcher, chief of AFCERT Operations, discusses an Automated Security Incident Measurement incident with Tech. Sgt. Kenneth Taylor, ASIM analyst.

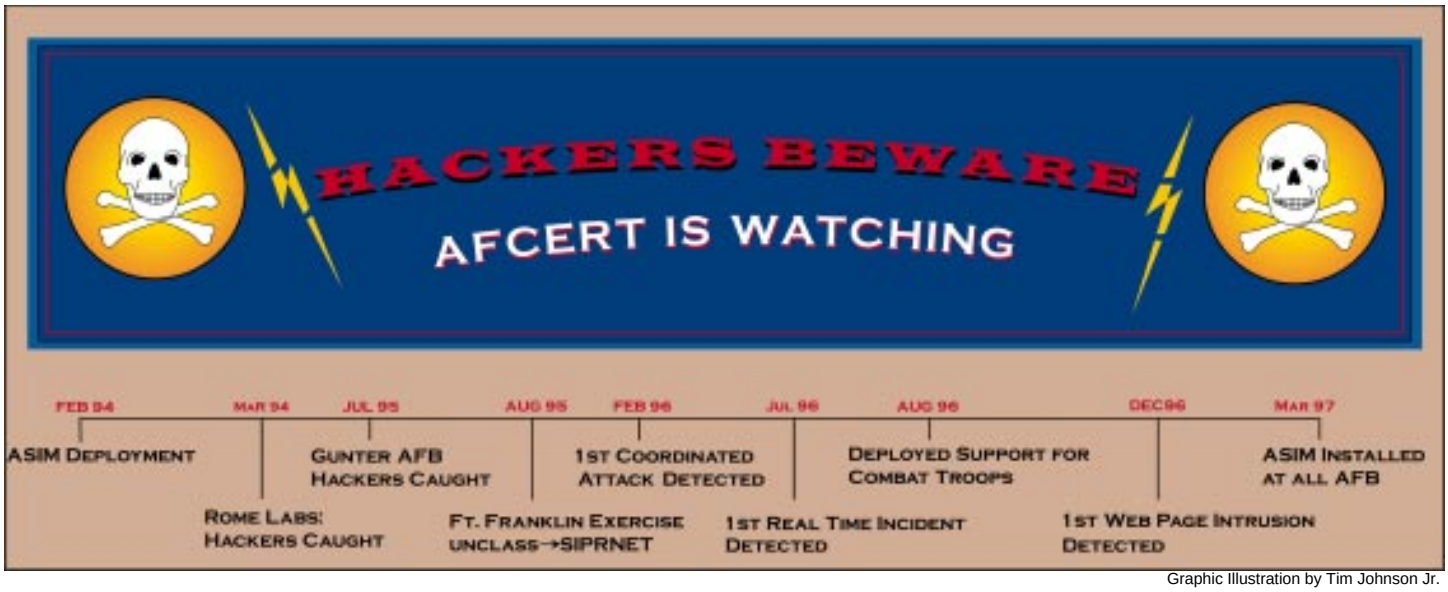
connectivity and capabilities. They educated worldwide Air Force and Department of Defense customers on computer security topics and provided assistance to other computer security organizations.

Mission Support maintains the research library that provides analysts, engineers and scientists with vital information for projects and studies. They also promote awareness of AFIWC capabilities through marketing and business development and provide a centralized education and training activity for the center. Additionally, they manage AFIWC safety, security, facilities and contracting functions.

The scientists and engineers of Systems Analysis provide quantitative analysis through modeling and simulation of offensive and defensive IW systems capabilities and vulnerabilities. SA develops and operates engineering, platform, mission, and campaign models for analysis of information, sensor and weapon systems. Evaluating vulnerabilities of US Air Force radar, communications, navigation, and IW systems; SA helps the warfighter to understand the potential vulnerabilities of friendly weapon systems, C2W systems and space systems. This understanding allows the warfighter to develop tactics and procedures to counter current, future and reactive threats.

Operations Support trains, equips and deploys personnel to provide IW and intelligence to the warfighter during contingencies, special operations and exercises. Deployable information warfare support teams provide planning support for operations security, military deception, command and other operations to Air Operations Centers and Joint Force Air Component Commanders.

In addition to these directorates are staff support. Intelligence Requirements, Management Support and Technology Management Support complete the infrastructure, allowing AFIWC to strive for information dominance and supply the warfighter with the services needed in contingencies and exercises.



Graphic Illustration by Tim Johnson Jr.

AIR FORCE COMPUTER EMERGENCY RESPONSE TEAM

The Air Force Computer Emergency Response Team is the Air Force's global command center for handling worldwide networked computer system security issues.

The AFCERT is the single point in the Air Force for reporting networked computer intrusions and problems.

It performs three broad missions; remote security assessments, automated intrusion detection and security incident response.

The AFCERT's accomplishments in 1996 include:

- improved worldwide Air Force automated intrusion detection coverage and capabilities
- remote security assessments
- responding to 47 computer security incidents
- expanding its internal security database connectivity and capabilities
- educating worldwide Air Force and Department of Defense customers on computer security topics and providing assistance to other computer security organizations

The AFCERT uses an automated computer intrusion detection system called the Automated Security Incident Measurement.

The ASIM is a hardware and software system that sits on Air Force networks "listening" for "suspicious activity" that is characteristic of intruder techniques.

It processes what it deems suspicious and reports once every 24 hours to the AFCERT.

The ASIM is the workhorse of the AFCERT and is extremely effective at detecting and reporting intruder activity, the first two steps necessary to mount an effective response.

At the beginning of 1996, the Air Force had only 26 bases covered by an ASIM. By the end of 1996, the ASIM covered 52 bases and three joint sites. Now the AFCERT monitors 107 Air Force and three joint ASIM sites. The AFCERT estimates the ASIM now detects over 100 million suspicious Internet connections a month.

Plans were in the works at the end of 1996 to enhance ASIM software to provide the AFCERT with near real-time intrusion detection alerts and a "connection denial" capability.

NRT alerts give the AFCERT timely notification of an attempted or actual intrusion so it can work with the affected base's computer security

personnel to reduce or prevent damage to Air Force computer systems.

The AFCERT established formal ASIM training and conducted courses toward certification for computer security personnel in 1996. The AFCERT teamed up with the Air Force Communications Agency to quickly provide this training to Air Force and Department of Defense personnel through contract courses.

The AFCERT wrote "rules of engagement" for the use of ASIMs. They were accepted by Air Staff who applied them Air Force wide. These rules were also added to the draft Air Force Instruction 33-208, Information Protection Operations.

The AFCERT performs remote security assessments on worldwide networked Air Force computer systems through its On-Line Survey program. Through the OLS, the AFCERT employs intruder techniques, tools and capabilities to "attack" unsuspecting Air Force computer systems.

The OLS's goals are to measure the Air Force's networked computer security posture (by seeing if systems can be penetrated using well-known, simple vulnerabilities and checking to see if anyone noticed and reported the attack on their system), to show the Air Force what an attack looks like and to operationally exercise the Air Force's ability to protect its computer resources.

The AFCERT conducted 62 OLSs at 52 different bases in 1996, surveying 4,309 systems. Of these, only 433 (10 percent) resulted in successful limited intrusions and 48 (one percent) resulted in full access intrusions, or root access.

These values showed continued improvement from 1995, when the AFCERT penetrated 15 percent of the tested systems at the user level and three percent at root.

The continued downward trend in the AFCERT's ability to penetrate systems shows a satisfactory improvement on the part of Air Force computer systems to repel unauthorized intruders and demonstrates the worth of the Computer Security Assistance Program, the AFIWC's program to help the Air Force defend its computer resources.

The AFCERT would like to see detecting and reporting at 95 percent or higher, however, only 14 percent of the attacked systems detected and reported the OLS activity to the AFCERT, down from 16 percent in 1995.

The Air Force's poor performance in adequately reporting attacks is thought to be the result of inadequate training and the high workload of system administrators.

Despite the AFCERT's many attempts to raise human detection and reporting levels, it continues to languish in the sub-20 percent level, adding increased credence for investing in more ASIMs, other intrusion detection tools, and continued research and development to help balance the odds against intruders.

The remote computer assessments capability was expanded in 1996 by the AFCERT training and certifying some major commands' computer security personnel and providing them with the OLS tools and "rules of engagement" for their use.

The AFCERT opened 47 intrusion detection incidents in 1996. The AFCERT worked with base personnel, major commands, the Air Force Office of Special Investigations and Air Force leadership to resolve each of those incidents. When needed, AFCERT personnel deployed along with CSAP deployable personnel to assist bases in recovering and reconfiguring computer systems in a secure manner.

Out of the 47 incidents, the AFOSI launched 21 substantive investigations

Graphic Illustration by Tim Johnson Jr.

Air Force Information Warfare Center

Photo by Boyd Belcher

Master Sgt. John Volk, noncommissioned officer in charge of AFCERT Operations, reviews a slide show presentation.

during 1996. The investigations identified 10 suspects, including three foreign individuals. Five cases were considered serious enough to pursue prosecution and three are pending. Prosecutions usually take a long time to bring to trial and the punishments are usually light because the laws in this area are nonexistent or have not adequately kept up with technological advances.

The AFCERT plans to continue working with law enforcement and the legal community to bring about changes in the law that adequately address computer intrusions.

The AFCERT uses the CSAP Database System to track and correlate Air Force vulnerability and intrusion data. In 1996, the CDS was improved to incorporate historical OLS and ASIM data.

This action provided a more comprehensive database to search for related intrusion detection activities and base vulnerabilities, resulting in dramatic support information improvements for OLSs, hacker incidents, vulnerabilities, malicious logic, and other AFCERT activities.

The AFCERT continues to educate the world on Air Force computer security operations, techniques, tools and procedures.

The AFCERT plans to grow from an 8-hour, five-day a week function to a 24-hour, seven-day a week function. The plan was to go from approximately 25 personnel at the beginning of 1996 to approximately 65 personnel, starting 24-hour operations on Oct. 1, 1997. This required new billets, personnel and the training program to ready them for duty.

The AFCERT also provides computer security education and awareness through AFCERT advisories. AFCERT advisories are issued anytime the AFCERT recognizes a security situation that could apply to users across the Air Force and provides a convenient way to easily disseminate the word.

In 1996, the AFCERT published 15 advisories. They ranged from making IP personnel aware of common poor security practices to providing information on known vulnerabilities and recommended preventive measures.

The AFCERT's home page was created in 1996 to provide Air Force and other customers with voluminous information on computer security. From the AFCERT web page, Air Force organizations can download a computer security tool kit or gain information on a wide variety of IP topics (e.g. viruses, hoaxes, anti-viral software, etc.) There is a security solutions section which organizes links to other web sites by operating systems, network types, tools, checklists, encryptions and many other IP related topics.

The AFCERT Daily Operations Report, the AFCERT's defensive picture of Air Force network activity requested by the Air Staff, was created in 1996 and made available on the Intelink, a classified intelligence network.

The AFCERT has worked with other organizations to assist them in establishing computer security operations of the same high caliber. The AFCERT assisted the AIA Information Operations Center with defining risk conditions and information conditions.

They assisted the Air Mobility Command and AETC in beginning to set up Regional Information Protection Centers. The AFCERT worked with the Pacific Air Forces in 1995 to establish the prototype for the regional centers and has extended that in 1996. AFCERT personnel also assisted the 609th Information Warfare Squadron in defining, and implementing deployable computer security operations.

The AFCERT has assumed a major leadership role within the Depart-

ment of Defense and federal government in helping other organizations stand up CERT operations; determining community computer security standards, terms, definitions, tools and operational procedures; bringing in legal authorities to deal with antiquated laws governing computer security; and providing technology insertions and concepts to quickly advance capabilities and responses.

The U.S. Army hired consultants to build its Army CERT and define its operational procedures. These consultants were tasked to build a facility modeled after the AFCERT, and the AFCERT was tasked to provide the consultants with advice, copies of its concepts of operation, and to host numerous visits, with which they gladly complied.

The key to the future of Department of Defense CERT operations is to fight jointly, share the same standards and cooperate. The AFCERT supports this notion and is a full partner with its sister service and Department of Defense CERTs, hosting the first Joint Information Assurance Operations Working Group meeting and keeping it going through leadership and support.

The AFCERT plans to improve Air Force computer security operations by expanding the RIPC concept of moving more responsibilities and capabilities to the major command and base levels; and improving the ASIM's near-real-time capabilities; and later implementing a connection denial capability.

The ability to electronically inventory Air Force networked computer assets and tie them to a database filled with critical information about them, a concept known as virtual battlespace, is a priority for 1997 as well.

Having this information when Air Force systems are attacked is vital to decision makers, allowing them to make the correct decisions in times of crisis. The AFCERT could advise a commander on what warfighting capabilities are lost if certain attacked systems cease functioning.

The AFCERT will continue to support AFIWC efforts to build a conceptual system known as "CSAP21." The CSAP21 concept embodies the AFCERT of the future by automating its functions and displaying worldwide computer security information on large wall screen displays for decision makers. The CSAP21 system would feature command center hardware and courses-of-action-determining software powered by modules incorporating risk management, intelligence, and modeling.

Air Force computer security is global in nature, yet defies geographical limitations. Implementation of computer security tools crosses traditional organizational boundaries. Policies and procedures are needed to define roles and responsibilities between AFCERT, major commands, bases and the information warfare squadrons.

The ASIM works. Hackers have been caught and prosecuted. ASIM continues to identify poor security practices, as well as real intrusions. Research must continue to identify ways for eradicating both, with the result being fewer or no intrusions. With each report or advisory issued, someone in the Air Force community is educated on how to implement better computer security practices.

Although analyzing ASIM data daily reveals possible intrusion activity, fielding a reliable NRT ASIM is critical to providing alert notifications in a timely manner. Improvements to the NRT ASIM, in particular the connection denial capability, will enhance this capability. Once NRT ASIM alerts a possible or actual intrusion, the AFCERT needs to provide the commander the option of denying that connection to prevent damage to Air Force computer systems.

Graphic Illustration by Tim Johnson Jr.

AFIWC TOOLS OF THE TRADE

C2W Analysis & Targeting Tool

The mission of the Systems Analysis Directorate is to provide analysis through modeling and simulation of offensive and defensive U.S. Air Force command and control warfare/information warfare systems capabilities and vulnerabilities.

This requires automated tools which can be used by analysts, operations personnel and combat commanders to train for exercises, and assess the impact of various C2W actions that may be used. They must provide a computer environment in which the modern warfighter can quickly apply real-time intelligence to decision making.

The C2W Analysis Division which is the C2W Analysis and Targeting Tool can provide commanders with the ability to more effectively select the correct mix of C2W techniques to expand and corrupt his adversary's decision cycle. It provides accurate simulation capability of adversary systems and the capability for analysts to do what-if analyses.

CATT is a computer model of an operational Integrated Air Defense System. CATT uses UNIX-based graphical user interfaces and high-resolution map displays to make the model user-friendly. It includes end-to-end modeling of IADS processes such as detection, tracking, communication, decision making and engagement.

An understanding of the enemy's IADS can be achieved by examining the processes in detail and how they function together.

The CATT model has a control screen and at least one IADS command screen. The control screen shows the ground truth for the IADS scenario with the flight paths overlaid. The IADS command screens depict what a red (hostile) operator would see in the IADS structure.

CATT is currently a prototype model and is being expanded to model the IADS of several countries. Analysts will be able to examine any country of interest by incorporating the country's tracking algorithms and IADS structure. Another upgrade will allow current intelligence data to be fed directly into the database, so the model will use the latest intelligence data from a variety of sources.

The CATT point of contact is Lt. Col. Ross Ziegenhorn, AFIWC/SAA, 102 Hall Blvd, Suite 338, San Antonio, TX 78243-7020. DSN: 969-2427, Commercial: (210) 977-2427.

"PATHFINDERS" Foster Technology Exchange

U.S. military forces now operate in an information age where the need for precise and instantaneous intelligence is increasing and expanding across the entire spectrum of military operations.

One of the Air Force Information Warfare Center's primary missions remains that of channeling all electronic battlefield information toward the objective of gaining information dominance over any adversary. The AFIWC's Office of Technology is actively pushing forward to put into place the processes, measurement criteria and programs necessary to ensure that the AFIWC has the technological lead necessary to maintain mission effectiveness into the 21st century.

Their recently instituted "Pathfinder" effort attempts to do two things:

1) Assist in linking the technology requirements of the various directorates to potential solutions

2) Foster cross-fertilization of technology among the various directorates within the AFIWC

The Office of Technology is the AFIWC's designated focal point for information warfare technology. The "Pathfinder" effort assigns specific OT personnel to each directorate within the AFIWC to assist in researching potential technological solutions for their mission requirements.

This program investigates promising commercial and government technology research and development efforts for application to missions within the AFIWC. The pathfinders then facilitate the introduction or dissemination of these promising technologies.

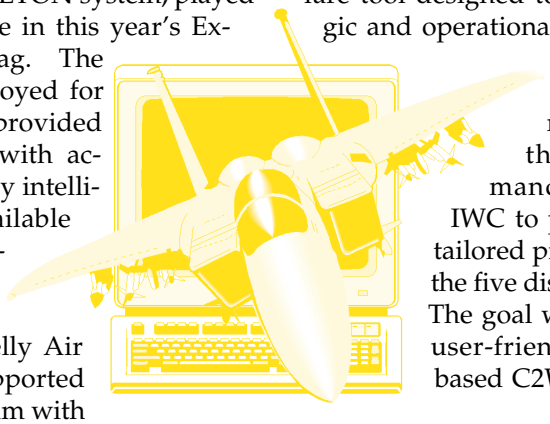
OT provided the necessary tools and software support to information warfare support teams deployed to support military exercises and real world contingencies in an effort to fill the role of pathfinder. This assistance allowed the IWSTs to provide real-time intelligence information to the warfighter. It became imperative that the IWSTs maintain their proficiency in the use of this tool to provide information to decision makers during exercises and real world contingencies.

OT provided planning, technical support and coordination for space-

related applications within AFIWC, and also operated, maintained and adapted S-band satellite systems to support reach-back and in-garrison information operations.

The TETON system used existing national satellites for high-speed data communications which supported national contingencies and exercises throughout the year. The OT staff also integrated the joint service Miniature Data Acquisition System into the AFIWC architecture.

This prototype Mini-DAS system, along with the TETON system, played a significant role in this year's Exercise Green Flag. The Mini-DAS, deployed for the first time, provided the warfighter with accurate and timely intelligence data available for use at all levels and in all commands. Personnel at Kelly Air Force Base supported the deployed team with the TETON system. The TETON provided critical imagery and intelligence data to the deployed team. This data was then processed by the Mini-DAS.



This program pulls shared resources from throughout AIA, as well as the AFIWC, to help develop an advanced concept on IW Planning. This effort will result in refined requirements that can be passed to Air Combat Command for inclusion in their mission planning process.

SENSOR HARVEST

The new world order has changed the way we plan to fight future wars and conflicts. The bipolar threat environment has essentially disappeared and a multi-regional threat environment has emerged.

The current and future battles will not necessarily be fought physically, but may occur electronically or through information systems. Intelligence support to the warfighters will be even greater in the 21st century due to emerging technology and vast accessibility to information.

The Air Force Information Warfare Center has various products and services tailored to support the warfighters in obtaining information superiority.

Sensor Harvest is a command and control warfare and information warfare tool designed to support strategic and operational planners. Sensor Harvest got its start in February 1993, when the AIA commander tasked the IWC to produce a C2W-tailored product involving the five disciplines of C2W. The goal was to develop a user-friendly, computer-based C2W planning tool.

OILSTOCK is the geographical information system used when displaying information on maps and through web technology. The product is disseminated in various ways, based on customer requirements, however, it is primarily made available through a classified wide area network called INTELINK.

Some of the information found in the Sensor Harvest product include a country's military capability, economy, culture, geography, politics and information systems. The information provided in the product is critical in both deliberate and crisis action planning. The overall goal of the product is to support planners during the operational environment research stage of campaign planning.

Sensor Harvest serves as a foundation and starting point for planners to use in understanding an adversary's decision-making process. Planners can use this information to effect the enemy's observe, orient, decide and act loop to achieve the CINC's objectives.

A nodal analysis approach provides a unique aspect in targeting and enables a shift from conventional targeting to IW/C2W targeting. Assessments on possible vulnerabilities to the elements of C2W include: psychological operations, deception, physical destruction, electronic warfare and operation security. The product can be utilized throughout the range of military operations — from peacetime to conflict.

Sensor Harvest has been used by joint services in both operational and exercise environments. The product was key in the target nomination process during Operation DELIBERATE FORCE. Sensor Harvest also supports various joint and service-unique exercises, such as Unified Endeavor, Ulchi Focus Lens, Green Flag and Red Flag.

Today the program enjoys the success in making commanders and planners more aware of information warfare. The product has been exposed to many high-ranking Department of Defense officials, foreign military personnel and civilian officials. Sensor Harvest was also demonstrated to the Global Air Chiefs during the Air Force's 50th Anniversary celebration in Las Vegas, Nev.

It is essential to know your enemy prior to engagement on the battlefield; whether on a typical land battlefield or a digital battlefield. Information is knowledge and knowledge provides the necessary power to gain air, space and information superiority. Sensor Harvest enables our warfighters to come one step closer in achieving air, space and information superiority.