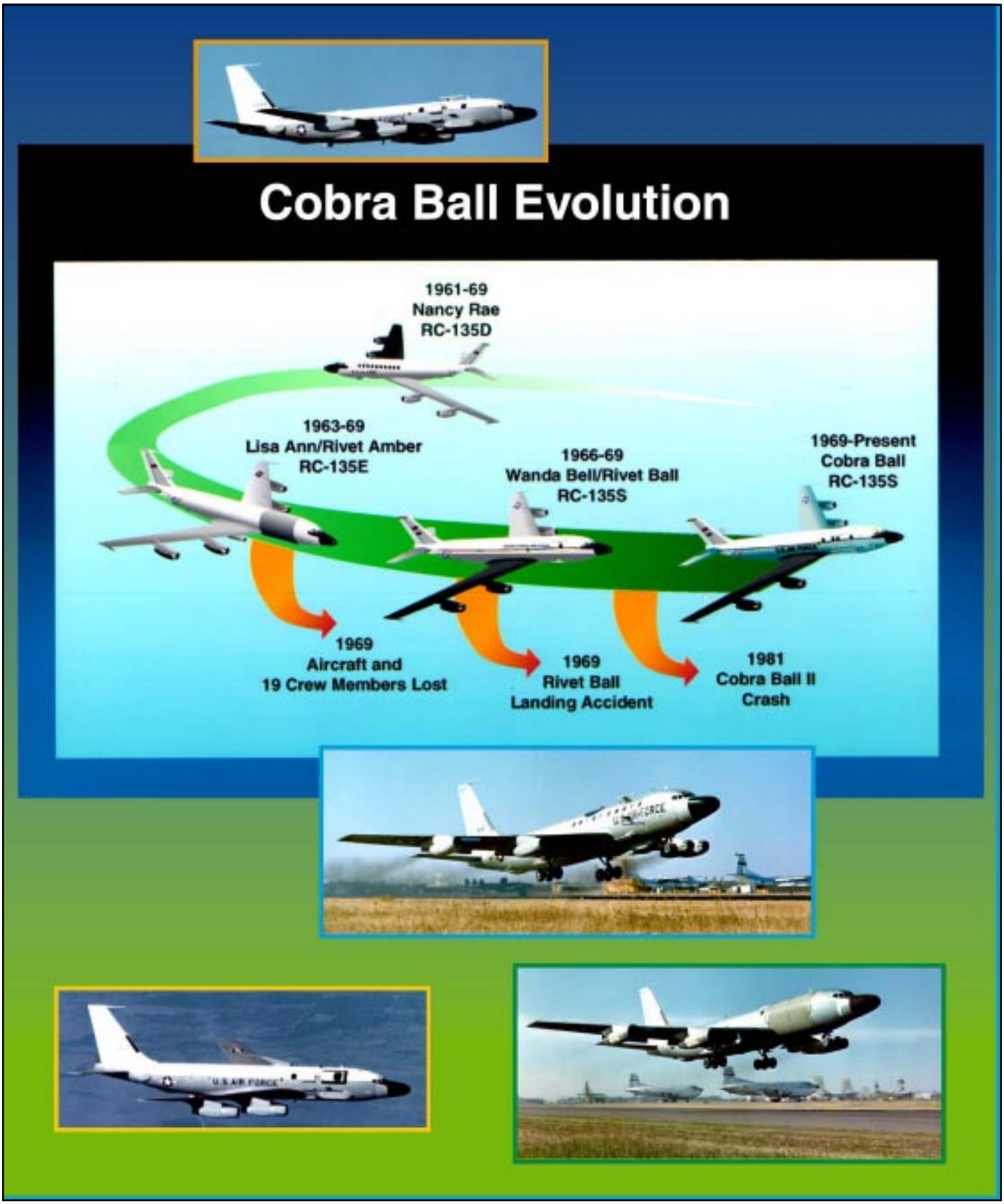
Cobra Ball



Graphic Illustration by Catherine Hammer

RC-135S Cobra Ball

Air Force's optical intelligence collection platform

For three years in a row, the Cobra Ball aircrew has earned the Air Force Association's O'Malley Award for being the best overall reconnaissance crew in the Air Force.

The 67th Intelligence Wing's own 97th Intelligence Squadron, is partnered with 45th Reconnaissance Squadron members at Offutt Air Force Base, Neb., where the 55th Wing has operational control over both squadrons.

✈ The RC-135S is an optical intelligence collection platform. Cobra Ball tracks missile systems for treaty verifications and has a growing role in theater missile defense.

✈ Cobra Ball's specialized crew employs sensitive telescopic monitoring devices, advanced optics and infrared sensors to provide national and theater command authorities with intercontinental ballistic missile treaty verification data and Theater Air Defense warning.

Cobra Ball was primarily used as a traditional mission in the past against Russia, but now the United States has no named enemy. This platform is evolving to meet new roles and missions, and now has linguists proficient in more than eight languages.

Out of the 18-member crew, the 97th has five slots for an airborne mission supervisor, manual Morse operator, cryptolinguist, air communications operator and one maintenance technician.

Graphic Illustration by Tim Johnson Jr.

The Cobra Ball crew distinguished itself by performing numerous aerial reconnaissance missions of national-level significance.

When the Joint Chiefs of Staff tasked Cobra Ball for joint Navy/Air Force Pony Express operations, they were mobilized and deployed on short notice to Kadena Air Base, Japan, in March.

While there, the Cobra Ball crew monitored tensions between two neighboring countries.

During the same deployment, the crew was also tasked to fly a never-attempted sortie to collect against a high-priority, strategic launch system from a different intelligence source.

The 97th IS's operations tempo is reaching the maximum capacity. Last year, 133 Cobra Ball sorties were flown, adding up to more than 1,097 flying hours.

Because the 97th also supports other RC-135 missions like Rivet Joint and Combat Sent, most of the airborne linguists are qualified for more than one platform.

To qualify an airborne linguist on Cobra Ball is difficult because they have to be qualified on a real sortie, with activity at their position. With three other operators on-board, training is slightly easier compared to getting a maintenance technician qualified. Experienced airborne technicians are in demand for Cobra Ball to ensure most equipment can be repaired.

Currently, the 97th supports two Cobra Ball RC-135S's. The addition of a third Cobra Ball may make things more difficult, said Lt. Col. Jim Glenn, commander of the 97th IS.

"The ops tempo would increase by 1.5. It would give us three on-station so we could keep one in depot maintenance and dedicate two crew to each aircraft. Both could deploy simultaneously and all three could actually depart if the situation got serious enough," said Glenn.

In the future, the 97th Collection Support Branch hopes to provide quick-look analysis of Cobra Ball data, decrease the turnaround time of data to national consumers and take advantage of the efficiencies created by the commonality between RC-135 programs.

RC-135V/W RIVET JOINT

Air Force's primary airborne reconnaissance platform

MISSION

Rivet Joint is the Air Force's primary airborne reconnaissance platform providing data to theater commanders and national command authorities. This data is essential for effective combat operations.

Rivet Joint crews also directly support combat operations through Information Warfare support.

They also perform direction-finding and range estimations in support of search and rescue operations.

FEATURES

The RC-135V/W is a four-engine, long-range, high-altitude, all-weather reconnaissance platform. It is a modified version of the C-135 aircraft.

The RC-135 has high, very high and ultra high frequency radios, radar and a doppler/GPS/stellar/INS navigation system.

Other equipment may include a variety of sensor types; receiver systems; probe; blade; and various fairlings used to smooth the outline of the aircraft and reduce drag. The Rivet Joint is continually being upgraded.

As the aircraft go through depot maintenance, they receive the latest system upgrades. This leads to ongoing training programs for crewmembers and maintainers alike.

BACKGROUND

Rivet Joint flew numerous missions in support of Operations Desert Storm and Desert Shield.

Additionally, Rivet Joint has participated in Operation Uphold Democracy in support of Haiti operations; Operations Provide Hope and Provide Comfort in support of relief for the Kurdish and Shiite peoples of Iraq; Operation El Dorado Canyon, the retaliatory strike against Libya by U.S. forces; and Operation Urgent Fury, the liberation of Grenada.

RC-135 General Characteristics

Primary Function:
Reconnaissance platform providing data to theater commanders and national command authorities.

Prime Contractors:
Boeing Aerospace Co.

Power Plant:
4 Pratt & Whitney TF33-P-9 or TF33-P-5 turbofans

Thrust per Engine:
16,050 pounds

Length:
140 feet, six inches

Height:
41 feet, 8 inches

Wingspan:
130 feet, 10 inches

Maximum Takeoff Weight:
299,000 pounds

Speed:
500 mph

Range:
Unlimited with aerial refueling

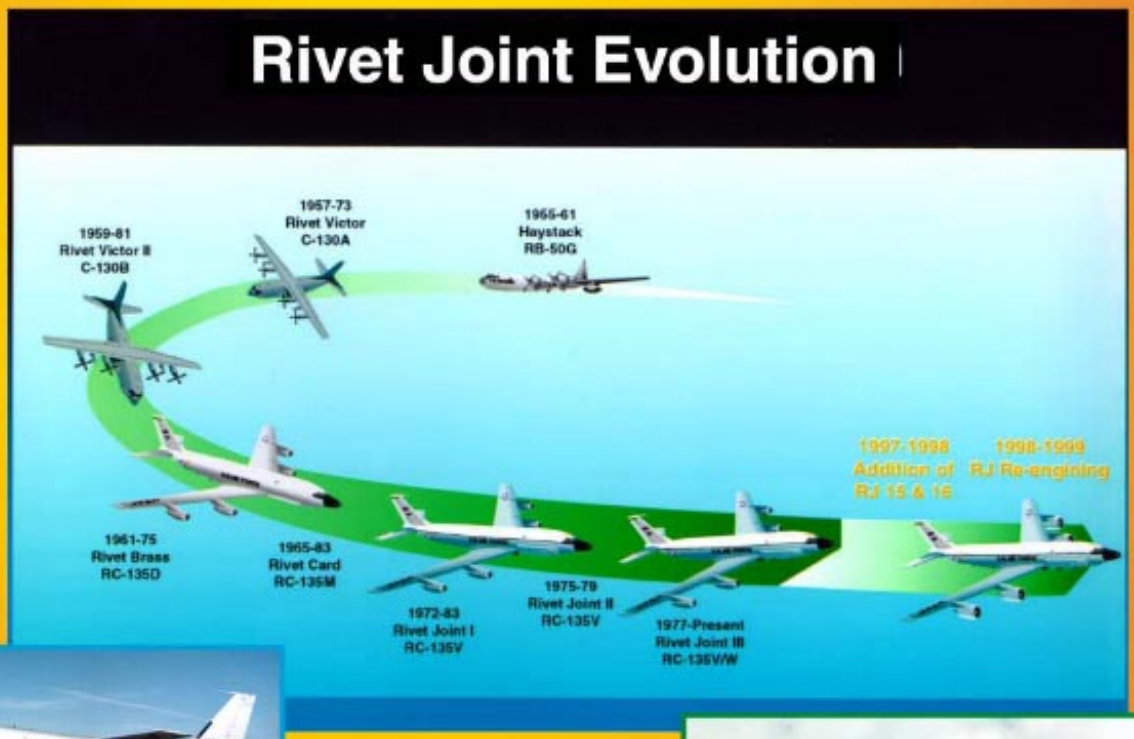
Ceiling:
Above 35,000 feet

Crew:
Minimum of 24; includes pilot and copilot, two navigators, three electronic warfare officers and a maintenance technician, all assigned to Air Combat Command; 15 enlisted operators and one maintenance technician, all assigned to Air Intelligence Agency

Date Deployed:
1973

Inventory:
14, with 2 more planned for production

Rivet Joint



Graphic Illustration by Catherine Hammer

Information Warfare Battlelab

MISSION

The Information Warfare Battlelab (IWBL) is a corps of Information Warfare (IW) experts linked with other Information Warfare organizations that support the full spectrum of Air Force operations by rapidly identifying innovative and superior ways to: employ IW capabilities; organize, train and equip Air Force IW forces; and influence development of IW doctrine and tactics in order to meet current and emerging Air Force missions.

FEATURES

The IWBL is composed of 24 personnel (15 Officers, 8 Enlisted, 1 Civilian). It draws from many career fields: the rated fields (a pilot and navigator), communications and computers, engineering, intelligence, space and administration. Other Air Force organizations will be tasked to temporarily provide members when their expertise is needed for a particular project. The Battlelab is housed in a 4,000-square-foot facility located within the Air Force Information Warfare Center at Kelly Air Force Base, San Antonio, Texas.

BACKGROUND

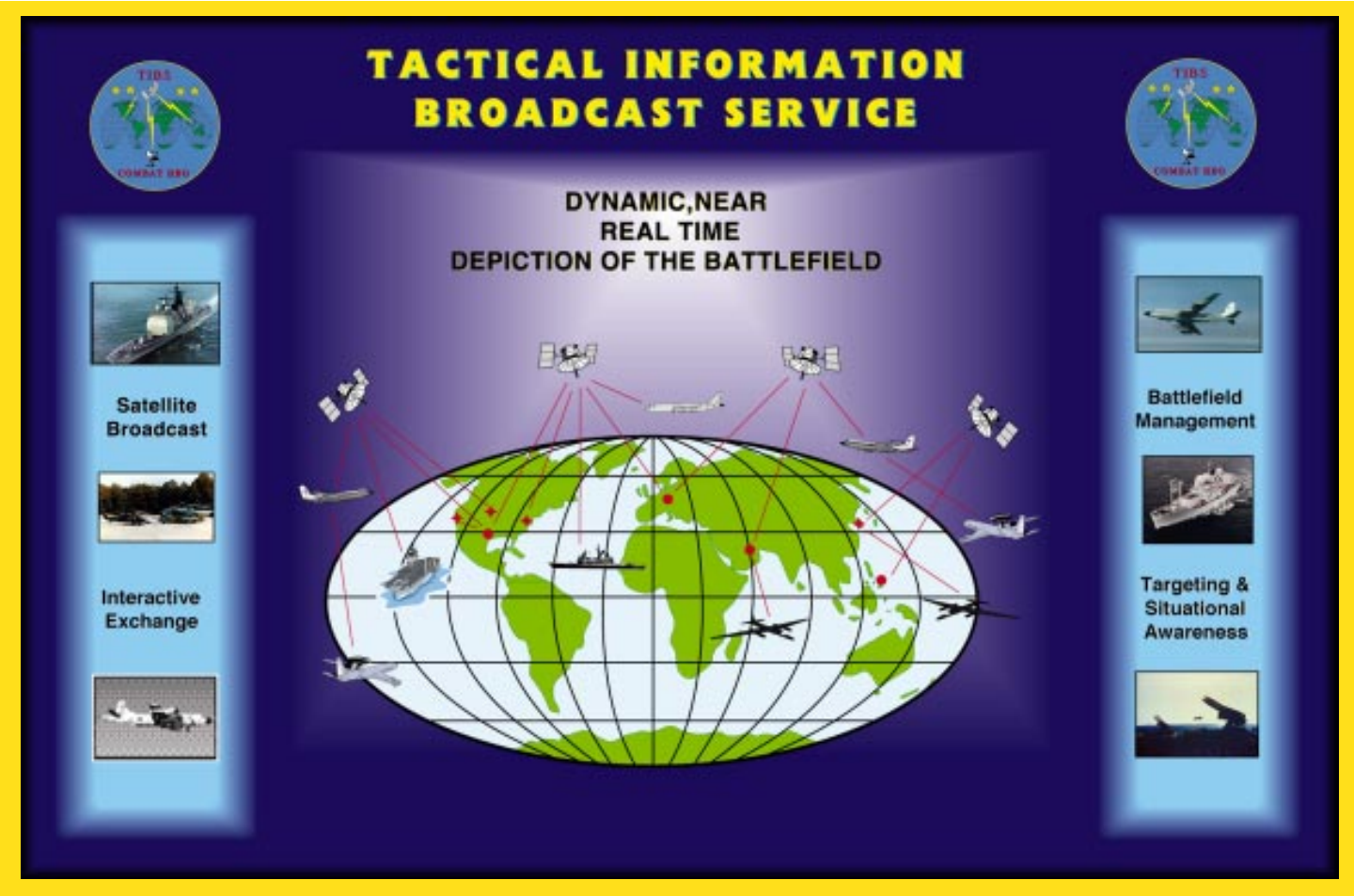
The IWBL is one of six Battlelabs located around the continental United States. Battlelabs were created to identify innovative operations and logistics concepts in order to advance the Air Force's core competencies: Air and Space Superiority, Information Superiority, Rapid Global Mobility, Precision Engagement, Agile Combat Support and Global Attack. They will draw on the best technology the private and public sector has to offer for the benefit of the Air Force. The IWBL began operations on March 17, 1997.

IWB GENERAL PROCEDURES

The IWBL will develop innovative solutions to IW needs in a five-step process:

- Solicit and prioritize IW needs and ideas from Air Force operators, industry, laboratories and academia.
- Organize and coordinate demonstrations of innovative IW tactics, techniques, procedures and/or technologies.
- Lead operational demonstrations within 18 months, with extensive warfighter interaction and operator feedback.
- Analyze results, focusing on operational impact.
- Publish results and make recommendations to the Air Force Board of Directors and Air Force Requirements Oversight Council

Tactical Information Broadcast Service



Graphic Illustration by Tim Johnson Jr.

TACTICAL INFORMATION BROADCAST SERVICE

MISSION

The Tactical Information Broadcast Service is a tactical intelligence dissemination network developed to provide direct support to military operations in the areas of battlefield management, targeting, and situational awareness as they relate to combat commanders, their supporting echelons, and other supporting organizations throughout the world.

FEATURES

TIBS produces a dynamic, near real-time, graphical depiction of the battlefield by utilizing information from a variety of intelligence disciplines and other sources. As a satellite broadcast, the data is available to all user commands, concurrently and immediately.

Unlike many information distribution systems, TIBS is designed to allow an interactive exchange among network participants which yields a rapid assembly of information to the user audience.

BACKGROUND

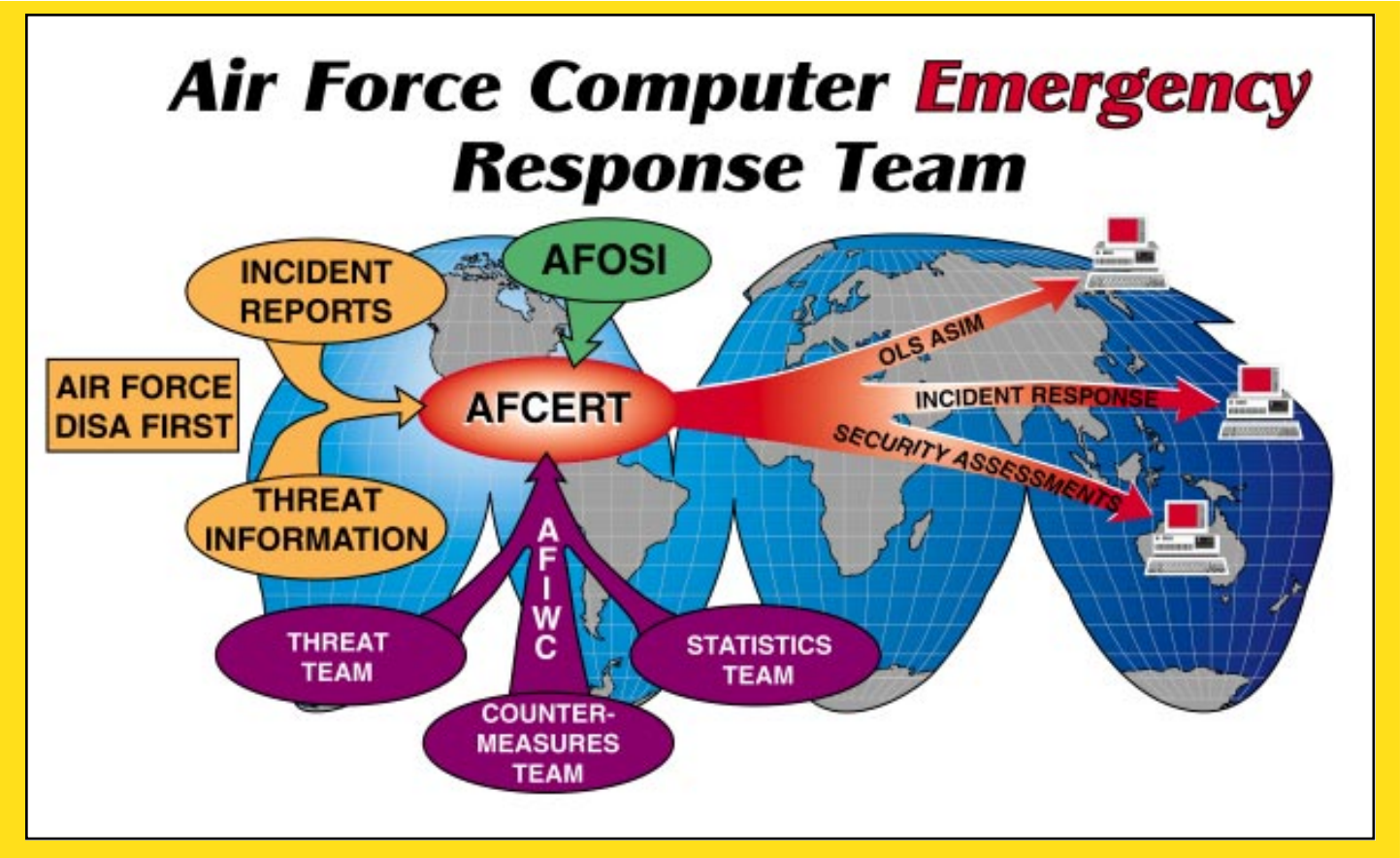
TIBS currently supports real-world operations as well as various exercises, operational concept demonstrations, and tests. The Assistant Secretary of Defense and the Air Staff designated the Air Intelligence Agency Directorate of Operations as the Department of Defense Executive Agent for TIBS. AIA created the TIBS Special Management Office to oversee the management of the program.

TIBS GENERAL CHARACTERISTICS

The TIBS network is a continuous, secure broadcast with data providers and data subscribers interconnected by a common radio channel in the UHF range (225-400 MHz). While UHF terrestrial line-of-sight networks are possible, typically the transmission medium is a United States Air Force satellite communications broadcast.

The current TIBS network architecture supports up to 10 data providers, 4 high-priority talkers, 50 active query subscribers and a number of receive-only terminals.

Air Force Computer Emergency Response Team



Graphic Illustration by Stan Doering

MISSION

The Air Force Computer Emergency Response Team is the single point of contact in the Air Force for the reporting and handling of all computer security incidents and vulnerabilities.

The AFCERT's primary responsibility is the coordination of Air Force Information Warfare Center technical resources to assess, analyze and assist in the handling of computer security incidents and vulnerabilities.

HISTORY

The AFCERT was created in 1993 in order to address known vulnerabilities inherent in computer networks.

The AFCERT was self-initiated by the Air Force Information Warfare Center, and has grown from three people to over 60.

The AFCERT has computer scientists, computer analysts, engineers, programmers, intelligence operators, database experts, displays experts and a representative from the Air Force Office of Special Investigations.

It is now at the forefront of information protection.

FUNCTIONS

The AFCERT has three major functions:

- On-Line Surveys
- Automated Security Incident Measurement
- Incident Response.

Air Force Computer Emergency Response Team

① ON-LINE SURVEYS

On-Line Surveys are both automated and manual tools that test Air Force systems for known computer security vulnerabilities, measure system administrator detection and reporting capabilities and exercise protection capability.

② AUTOMATED SECURITY INCIDENT MEASUREMENT

Automated Security Incident Measurement is a computer program that supports Air Force computer security incidents detection, provides early warning of attack, quantifies unauthorized network activity and exercises detection capability.

③ INCIDENT RESPONSE

Incident Response is the process the AFCERT uses to address or handle unauthorized activities on Air Force Networks. IR can be broken down into six steps: detection, notification, verification, isolation and containment, criminal investigation and recovery.

1) Detection:

Incidents are detected either through ASIM or through Air Force personnel detecting possible intrusions on their own.

2) Notification:

The AFCERT is notified of a possible incident either through the ASIM or through Air Force personnel contacting the AFCERT.

3) Verification:

The AFCERT contacts the affected base's Computer Systems Security Officer (CSSO) and requests that he or she verify whether the activity was authorized.

4) Isolation and Containment:

The compromised system is moved into an environment that allows investigators to observe an unauthorized intruder but limits his or her actions.

5) Criminal Investigation:

The Air Force Office of Special Investigations is responsible for investigating all verified computer security incidents. The AFCERT will assist them in their evidence collection, but the AFCERT'S role is resource protection, not law enforcement.

6) Recovery:

The commander of the compromised system determines when the system is recovered based on his mission needs. The system administrator is responsible for the recovery, but the AFCERT will assist him, or her, if requested.