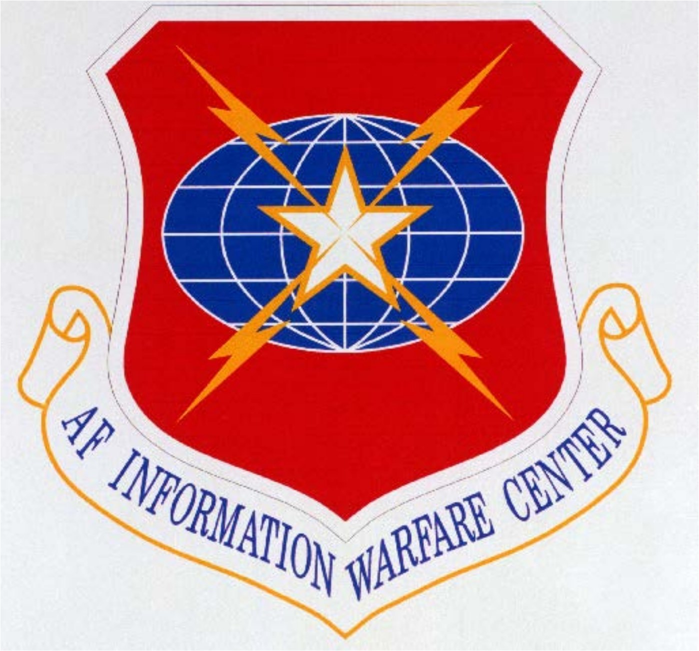
AIR FORCE INFORMATION WARFARE CENTER



LINEAGE

STATIONS
Kelly AFB, TX

ASSIGNMENTS

COMMANDERS

HONORS
Service Streamers

Campaign Streamers

Armed Forces Expeditionary Streamers

Decorations

EMBLEM

EMBLEM SIGNIFICANCE

MOTTO

NICKNAME

OPERATIONS

The Air Force Information Warfare Center, collocated with the Air Intelligence Agency, was created to he an information superiority center of excellence, dedicated to offensive and defensive counter information and information operations AFIWC was originally activated as We 6901st Special Communication Center in Jul 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 team of UDC 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.

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 1W 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 1W capabilities; organize, train, and equip Air Force IW forces; and influence development of I V11 doctrine and tactics, Advanced Programs foster the development and employment of advanced RV 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.

he Air Force Computer Emergency Response Team is the Air Force's global command center for handling worldwide networked computer system security issues The FLIRT is the single point in the Air Force for reporting networked computer intrusions and problems AKA1(1 responded to 47 computer security incidents in 19% and expanded its internal security database 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 M counter current, future and reactive threats.

Operations Support trains, equips and deploys personnel to provide 1W and intelligence to the warfighter during contingencies, special operations and exercises. Deployable information in warfare support teams provide planning support for operations security, military deception, command and other operations to Air Operations Centers and Mint 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.

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 per- cannel 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 For computer systems through its On-Line Survey program. Through the OLS, the ACCEPT 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-21 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 during 1996 The investigations identified 10 suspects, including three foreign individuals. Five cases were considered serious enough to pursue prosecuttim 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 (or 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 AFCFRT continues to educate the world on Air Force computer security opera lions, techniques, tools and procedures.

The AFCERT plans to grow from an S-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. I his required new billets, personnel and the training program to ready them for duty.

The AFC.FIRT also provides computer security education and awareness through AFCFRT 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 provide information on known vulnerabilities and recommended preventive Measures.

The AFCERT's home page iris 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 IF 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 Department 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 ITC 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 CHIVE 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 going through leadership and support

The AFCERT plans to improve Air Force computer security operations by expanding the 121PC concept of moving more responsibilities and capabilities to the major command and hose 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 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 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 the impact of various C2W actions that must 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 for 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 LADS processes such as detection, tracking, communication, decision making and engagement. An understanding of the enemy's TADS can be achieved by examining the processes in detail and how they function Et-ignition The CATT model has a control screen and at least one LADS command screen. The control screen shows the ground truth for the LADS scenario with the flight paths overlaid. The LADS command screens depict what a red (hostile) operator would see in the LADS structure.

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

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 AFIWCs 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:
Assist in linking the technology requirements of the various directorates to potential solutions

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 inhumation 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 through out the year The OT staff also integrated the joint service Miniature Data Acquisition system into the ARMY architecture.

This prototype Mini-DAS system, along with the TETON system, placed a significant role in this years 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 Learn. This data was they processed by the Mini-DAS.

This program pulls shared resource from throughout AIA, as well as the AFTWC, 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 tears and conflicts. The bipolar threat environment has essentially disappeared and a multi-regional threat environment has emerged.

The current and future battles will necessarily be fought physically, but may occur electronically or through information systems. Intelligence support to the warfighters will he 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 fool 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 fire 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 servos as a foundation and starting point for planners to use in understanding all 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 We 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.

The need to establish the AIA stemmed from Air Force Chief of Staff General Merrill A. McPeak's decision to implement an objective Air Force and a one base, one boss concept. His concept led to a restructuring of Air Force intelligence by redesignating the AFIC as the AIA on 1 October 1993. Commanded by Maj Gen Kenneth A. Minihan, the new organization reported directly to the USAF Assistant Chief of Staff for Intelligence. This move signaled increased support to the warfighter. The change began with the 10 September 1993 establishment of the Air Force Information Warfare Center (AFIWC) at Kelly AFB. That action combined the AFEWC with the security functions from the Air Force Cryptologic Support Center. The AFIWC received a primary mission to channel all electronic battle field information toward the objective of gaining information dominance over any adversary. Thus, AFIWC became a significant player in AIA activities.

In 1967, USAFSS assigned its new electronic warfare evaluation mission to AFSCC (later AFIWC) at Kelly AFB, Tex. USAFSS assigned the mission to AFSCC because the center had a cadre of experienced analysts. In addition, the phase out of the center's analytic task made the necessary office space available. This new electronic mission was the first major change in the command's responsibilities in many years. The command disseminated its initial evaluations electronically in Comfy Coat reports. Later, the command expanded the effort to cover the evaluation of Navy and ground electronic warfare, and Army, Navy, and Marine personnel who were assigned to AFSCC.

On 10 September, the HQ Air Force Electronic Warfare Center was redesignated HQ Air Force Information Warfare Center (AFIWC). 1993

On 13 August Col James C. Massaro assumed command of the 67 IW. He previously commanded the AFIWC.1999

On 1 October, the Air Force redesignated the Air Force Information Warfare Center as the Air Force Information Operations Center (AFIOC). 2006

The change began with the 10 September 1993 establishment of the Air Force Information Warfare Center (AFIWC) at Kelly AFB. That action combined the AFEWC with the security functions from the Air Force Cryptologic Support Center. The AFIWC received a primary mission to channel all electronic battle field information toward the objective of gaining information dominance over any adversary. Thus, AFIWC became a significant player in AIA activities.

AFIWC

The Air Intelligence Agency created the Air Force Information Warfare Center to be an information superiority center of excellence—dedicated to offensive and defensive counter information and information operations. Colocated with AIA Headquarters on Security Hill, the AFIWC replaced the Air Force Electronic Warfare Center on 10 September 1993.

The AFIWC mission was to "explore, apply and migrate offensive and defensive information warfare (IW) capabilities for operations, acquisition and testing, and provide advanced IW training for the Air Force."283 On 20 December 1993, the AFIWC opened Operations Support Central—the agency's round-the-clock single point of contact for information and assistance to forces deployed around the globe.

AFCERT

In 1993, the AFIWC created the Air Force Computer Emergency Response Team to address known vulnerabilities inherent in computer networks. The AFCERT had grown to 60 professionals by 1997—computer scientists, computer analysts, engineers, programmers, intelligence operators, database experts, displays experts and a representative from the Air Force Office of Special Investigations. Operating out of the AFIWC, the response team constitutes the single point of contact in the Air Force for the reporting and handling of all computer security incidents and vulnerabilities.

Air Force Information Warfare Center

The Air Force Information Warfare Center, collocated with 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 the 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.

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, data-base 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, train, and equip Air Force IW forces; and influence development of IW doc-trine 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 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 aware-ness 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.

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, auto-mated intrusion detection and security incident response.

The AFCERT's accomplishments in 1996 include:

improved worldwide Air Force automated intrusion detection cover-age 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 soft-ware 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 com-puter 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 at-tempts 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 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 be-ginning 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 any-time 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 Department 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.

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 over-laid. 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 War-fare 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 war-fare 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 sup-ports 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 in-formation superiority.

Air Force Information Warfare Center

The Air Force Information Warfare Center at Kelly Air Force Base, Texas, is engaged in a myriad of activities supporting its role as the Air Force information warfare executive agent. Its mission is to develop, maintain and deploy information warfare/ command and control warfare capabilities in support of operations, campaign planning, acquisition and testing. The center acts as the time sensitive, single focal point for intelligence data and C2W services. It provides technical expertise for computer and communications security and is the Air Force's focal point for tactical deception and operations security training. The AFIWC was activated Sept. 10, 1993, by combining the Air Force Electronic Warfare Center, and elements of the Air Force Cryptologic Support Center's securities directorate. The AFEWC provided electronic combat and technical expertise for Desert Storm C2W successes. Coupled with AFCSC's technical skills in command, control, communications and computer systems security, the merger of the two organizations provided a solid baseline for the new IW mission.

Air Force Order of Battle
Created: 19 Sep 2010
Updated:

Sources
AFHRA