



This first month as your commander has gone by quickly, but as I anticipated, I am already impressed with the quality of our troops and the dedication to our mission. My wife Leslie, my daughter Tracy, and I are very pleased to be a part of the Air Intelligence Agency team again and back in Texas. I look forward to visiting each AIA unit during my tenure,

but in the meantime, I am proudly aware of your many accomplishments and successes. Keep up the good work!

A few short weeks ago, I was the European Command Director of Intelligence, or EUCOM/J2. Bosnia, the Balkans, several non-combatant evacuations and humanitarian relief operations, a few crises, and a concerted effort to shape the environment to preclude future crises, ensured a high operations tempo for the EUCOM J2/J3/J5 team. The extremely busy activity in the operational environment was a daily reminder of a fact I first realized in Vietnam many years ago. The fact: the importance of intelligence and information operations with respect to every military operation and every commander in chief decision. I'm proud to say that I could see AIA fingerprints on many of the daily products and services. The bottomline is that you play a critical role in our nation's defense and power projection. You need to know, and be frequently reminded, that the work you do on a daily basis is important and required.

By now I'm sure all of you have heard or seen Secretary Widnall's and General Fogleman's words on the importance of Information Operations and Information Superiority. Those two phrases have been indelibly written into the Air Force lexicon, and we are pursuing improved IO capabilities with all due haste to ensure the United States retains the most formidable forces on the planet. Information Operations is the ability to gain, exploit, attack and defend the information domain; but, I want to make clear to you, there is a lot more to information superiority than defending computers against hacker attacks.

Our livelihood, now and in the future, is based on those same fundamental disciplines that were practiced in the '50s, '60s and '70s, such as human intelligence, imagery interpretation, foreign technology exploitation, technical intelligence, and signals collection and analysis. In an age of increasing importance and reliance on computers, I don't want us to lose sight of the fact that they're only as good as the information fed into them and the analysis drawn from them. We've been providing that input - and doing it exceedingly well - for several generations now, and there is no end in sight to that work. Our

analyses help our leaders make national-level decisions, our interpretations help put bombs on target, and our exploitation helps keep our technology several steps ahead of the bad guys'. We do vital work for the nation at light tables, in the lab and in the field. It is the bedrock, the foundation, the "gain and exploit" piece of Information Operations, and it is our springboard for the research and work we do to defend and attack the information domain.

Just look at a few recent examples of how much we're doing to enhance not only our mission, but the missions of countless others. At the 480th IG, the age-old intelligence production process was improved by using web technology to hyperlink disparate sources to a single site, saving the customer approximately 85 percent of the time to research the issue independently. At the 544th IG, personnel are embedding into 14 Air Force units, while at the same time educating AIA personnel on space-based resources and applications.

The National Air Intelligence Center at Wright-Patterson Air Force Base has produced modeling and simulation of foreign aviation threats that can be used to train pilots about an enemy's capabilities and tactics, before they get in the cockpit, hopefully saving lives in the process. The 488th Intelligence Squadron at Royal Air Force Mildenhall, England, just completed 1,000 missions on the Rivet Joint, supporting Operation Provide Promise, Operation Deny Flight, Operation Deliberate Force and Operation Joint Endeavor. On the other side of the planet, the 381st IS at Elmendorf Air Force Base, Alaska, is providing key translators for joint Russian/American exercises. All of these milestones and accomplishments have been written about in recent issues of the *Spokesman*. I mention this because I believe the *Spokesman* is an essential forum for our Agency, to let people know, who might not otherwise have the means, exactly how much we contribute to the mission, to each other, and to our communities.

My concern is that while we must focus and commit resources to rapidly advance our IO capabilities, we must also pay attention to the incredibly significant work we're doing right now, every day, in numerous vital career fields throughout the Agency. I want to make sure, whether you're flying on the Rivet Joint, making threat assessments, or doing imagery interpretation, you understand the importance of what you do and it's visibility - to me, to the rest of the Agency, to our national leaders, and most of all, to the people who depend on your work to fulfill their mission. You are important, what you do is important, and by teaming together we make a tremendous impact on the state of our nation's well-being. I look forward to working with you to meet the challenges of our information age.

James E. Mills

Information Operations Center

Taking AIA into the future



Photo by Boyd Belcher

Staff Sgt. Robert Kirkman briefs IOC visitors on the dais.

By Staff Sgt. Kimberley Young
HQ AIA/PA
Kelly Air Force Base, Texas

When Air Intelligence Agency leadership referred to the Information Operations Center here as the “hub” of information, it made for some big shoes to fill.

As the IOC became Detachment 1, Headquarters AIA/Intelligence Systems Group, in January, it got more than just a new name. The IOC took on a new role.

The IOC supports AIA’s mission of exploiting and defending the information domain by being the Air Force’s multi-dimensional, 24-hour operations center.

It focuses on integrating and conducting worldwide information operations with the primary functions of Information Warfare Indications and Warning (Cyberwatch), Situational Awareness and Operation Reachback .

Information operations not only encompasses traditional competencies in reconnaissance, surveillance and intelligence, but also defends and attacks information.

With new responsibilities, the IOC continues command post functions, however, it is no longer the primary focus. In a year’s time, the IOC implemented Cyberwatch, enhanced information operation capabilities and is defining the process and procedures for interfacing with IO detachments in the field.

“Our business is data. I like to think of us as ‘brokers of information.’ We don’t want to buy it or own it, we want to know what’s out there, acquire it and give it to the customer,” said Lt. Col. David Castillo, IOC commander.

“Our responsibility first and foremost is to AIA, to the operations that are here, to our units and our components, including our embedded presence in the Numbered Air Forces as we stand them up. Our second obligation is to the Air Force at large, and our third obligation is to the Department of Defense and other customers as a whole,” said Castillo.

"We are actively involved with several vendors here in San Antonio and the United States to look at some technologies the Internet may have to offer that will be applicable in our search to find information that is pertinent. The customer doesn't have time to find the data, analyze the data and make a decision," he said.

As a combined effort with the Defense Intelligence Agency, Cyberwatch has developed indicators to assess the abilities of foreign nations to conduct information attacks against the United States and its allies.

"I think it's an area that's important to the nation, not just for the Department of Defense, the Air Force or AIA," Castillo said.

The folks working Cyberwatch take operational data received from the Air Force Computer Emergency Response Team and merge it with intelligence and open source data. They piece this information together to develop a picture giving the customer advance warning of an attack based on demonstrated capabilities and stated intent.

"Customers are looking for one

thing - warning from a competent authority. Someone who's trained and experienced," said Castillo.

In addition to warning, Air Force operators need a vast amount of information to successfully conduct operations. Embedding in the numbered Air Forces is AIA's solution to that problem, said Castillo.

Embedded AIA people provide an information lifeline, ensuring that operational partners work under an umbrella of information superiority.

The embedded units will be AIA's forward presence. If the information operation detachments can't answer the question, they can reachback to the IOC for the required information.

"I'm impressed with the IOC. I will be reaching back and tapping into the resources AIA can provide," said Capt. Jim Klingmeyer, Det. 4, 67th Intelligence Group commander, Scott Air Force Base, Ill.

All things made possible in the IOC stem from the dais. The dais the raised platform positioned in the center of the room — the heart of the IOC. It lends itself out to nine different workstations and consists of four-

to eight-man flights, each flight pulling 12-hour shifts.

With a combination of seven to eight different Air Force Specialty codes, Castillo feels it is one of the IOC's strengths because there are subject matter experts in all aspects of Information Operations.

Operators on the dais have access to information from a variety of sources and classification levels. Using technology, the data is filtered and provided electronically to the appropriate position.

The Combat Intelligence System help desk is very popular. "We receive over 250 calls per week from customers asking questions," said Tech. Sgt. Ilda Zamora, chief of Information Management.

Also, the IOC has more than 6,000 visitors a year for a tour of the facility.

"Anytime something happens around the world, people call our office to find out what's going on. People consider the IOC as a one-stop shop for information," said Zamora.

"We are all part of a greater whole. All services utilize the IOC for information. We need to be great at finding information and getting it to the customer as soon as possible," said Capt. John Daberkow, chief of Flight Operations.

Continuing upgrades and improvements; the development of new concepts and capabilities; and incorporation of these evolving realities into the way we organize and plan to conduct effective Information Operations, will ensure the Air Force continues to provide theater commanders in chief and national decision makers Information Superiority — today and tomorrow.

It's a changing world and customer needs are changing.

The Information Operations Center was given the responsibility to provide information and they've proved they do it well. Thanks to technology, it will only get better. ■



Photo by Boyd Belcher

From left to right, Senior Airman Jeremy Knupp, 1st Lt. William Pruitt, and 1st Lt. Rodger Martin review a response to a customer.



1957...Imagery analysts conducted imagery analysis using photographic prints, glass measuring scale and mechanical calculator.



1997...Imagery analysis at an IDEX II softcopy work station. Enhancement, stereo viewing and mensuration at the analyst's fingertips.

Imagery Intelligence

NAIC's eyes on the world provide "big picture"

*by John Summerfield
NAIC/DXHF*

Wright-Patterson Air Force Base, Ohio

Necessity is the mother of all invention! This age-old adage describes perfectly the genesis of the National Air Intelligence Center's imagery intelligence capability.

During and after World War II, foreign materiel exploitation of captured German aircraft and weaponry was accomplished by NAIC's earliest forebearer, the T-2 intelligence section of the Air Materiel Command at Wright-Patterson Air Force Base, Ohio.

With the advent of the Cold War, assessment of Soviet aircraft through foreign materiel exploitation was all but denied.

Although hands-on access to new Soviet aircraft was virtually impossible, photographs were obtained from airshows and trade journals. As a result, other means of threat analysis were "invented."

In the early 1950's, Isadore Herman, director of Engineering Support at the Air Technical Intelligence Center, envisioned the analysis of photographs could provide accurate aircraft dimensions and airframe configurations.

This photogrammetric data could be used to contract engineering drawings which would be used to determine performance and capabilities of the weapon system through a reverse-engineering process. Thus was born the Imagery Exploitation Division of what is now NAIC. This IMINT capability has flourished and diversified over the last 45 years.

Through organizational name changes, NAIC's imagery analysts have established themselves and their products as unique and unsurpassed resources within the intelligence community.

The demand for scientific and technical IMINT expertise and the need for new intelligence products

burgeoned as weapons technology accelerated.

The development of foreign ballistic missiles, space satellites, early warning acquisition, guidance radars, along with the ever-increasing sophistication in aircraft technologies, places greater demands on national intelligence assessments.

The need for scientific and technical imagery intelligence increased proportionally, requiring NAIC imagery analysts to become experts in the analysis of all types of imagery, including satellite, hand-held, radar, infrared and video.

Detailed imagery analysis reports, engineering drawings and computer-aided design models became cornerstones for the integrated threat analysis studies produced by NAIC engineering and weapons systems analysts.

The collapse of the Soviet Union brought new challenges to NAIC's imagery analysts. With the prolifera-

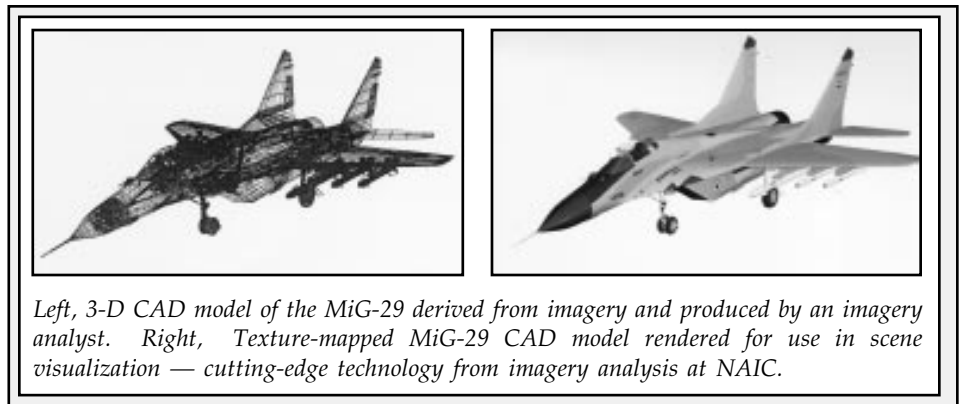
tion of weapons exports worldwide, the body of knowledge required for NAIC imagery analysts to maintain expertise increased dramatically.

The changing world situation, demonstrated in Desert Storm, brought rapid changes to NAIC's imagery exploitation operations. Direct support to warfighters became the number one priority and the electronic dissemination of IMINT to customers became the standard.

Today, INTELINK serves as an electronic pipeline providing NAIC's classified IMINT and products to all Department of Defense components. The dissemination of IMINT from all sources and events can now be quickly and efficiently accomplished.

The in-depth expertise by NAIC imagery analysts is unique. Specialized and tailored support is requested by non-typical customers such as the Aeronautical Systems Center's Armstrong Laboratories, Joint Task Force 6 and the Air Force Office of Special Investigation.

Cutting-edge technology utilizing IMINT products such as CAD models is now commonplace. Highly detailed 3-D models have been used to create radar cross section models using a stereolithography process where all model data are transmitted electronically to the SL laboratory. There, a polymer model is produced without



Left, 3-D CAD model of the MiG-29 derived from imagery and produced by an imagery analyst. Right, Texture-mapped MiG-29 CAD model rendered for use in scene visualization — cutting-edge technology from imagery analysis at NAIC.

mechanical intervention. CAD models of aircraft and air-launched weapons are also being used to build wind tunnel test models.

NAIC imagery analysts continue to embrace new technology, using CAD models to produce virtual reality scene visualizations from still imagery. Analysts attend national and international working groups and meetings to present and defend IMINT issues.

These experts also present IMINT briefings to Air Force leaders and to the Intelligence community upon request. Imagery analysis has been referred to as "an art and a science" — the imagery analysts at NAIC have set the standard for excellence in this profession.

Under the leadership of Lt. Col. Michael Ames, the Imagery Exploitation Division at NAIC stands ready to

respond to customers needing imagery intelligence to support their mission requirements.

The five imagery analysis production branches are:

- **Ballistic Missile System**
- **Bomber/Support Aircraft**
- **Electronics**
- **Fighter Aircraft**
- **Space Systems**

Supporting technical branches are:

- **Imagery Systems**
- **Imagery Operations**
- **Imagery Information**
- **Imagery Production**
- **Open Skies**

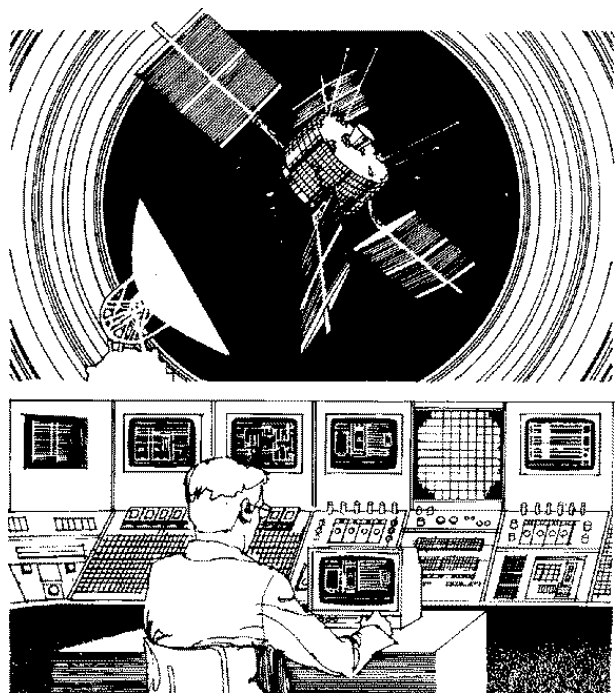
This 141-person-strong division represents a half-century legacy of imagery exploitation expertise and excellence, ready to support the technology and products of an unlimited future. ■



From ... 1967, imagery-derived hand-drawn engineering drawings on drafting tables.



To ... 1997, computer-aided design, 3-D models and 2-D engineering drawings on computer work stations..



Counting all factors of Information Operations

*by Maj. George Crawford
Commander, Det 1, 67th IG
Eglin Air Force Base, Fla.*

What types of information does a pilot, missileer, planner or information user need to perform his or her mission?

Operators want three things:

- To predict the enemy's future activity
- Inform them about their objective or target
- The background to understand their operational environment

Predictive Information

A user needs predictive information to stay safe while carrying out a mission. The information operations goal should be to understand the mission and provide courses of action that will minimize the threat's impact on that mission.

Courses of action can include attacking, exploiting and defending enemy information, thus reducing the enemy threat.

For example: Information on enemy air defense activities is important to a Viper F-16 driver who will drop 4,000 pounds of Pittsburgh steel and

Kentucky black powder or tritoniol on a chemical weapons plant. A combat controller might need to know the vertical obstructions within 200 yards of his drop zone.

Threat information helps the user think through possible courses of action and plan for mission success in spite of enemy activity.

Objective Information

A user needs to know what they're expected to do and why they're doing it.

Objective (target) information needs to answer:

- What is expected of the user?
- What is the significance of this mission relative to the overall allied effort?
- What will the result be on the enemy?
- What are the consequences if the mission doesn't succeed?

To accomplish the mission, the user needs to know everything relevant about that objective.

For example: A weaponeer may need to know the thickness of the walls in the communications room of a command post, as well as the walls of the civilian hospital next door. An airlift planner might want to know the condition of all runways over 3,000 feet within 25 miles of a planned non-combatant evacuation operation.

Again, this information must be tailored to the mission being performed. Information on the objective helps the user accomplish their assigned mission.

Perspective Intelligence

Perspective (background) intelligence information helps a user understand the overall environment in which they'll operate.

The information operations goal: educate the user about the mission environment. How will it affect the mission? Provide information on anything which could impact the mission.

For example: A soldier of the NATO Implementation Force will perform his mission better if he under-

stands why the Serbs, Bosnians and Croats are fighting.

The Joint Forces Air Component commander cares a great deal how many precision-guided weapons exist in-theater.

Perspective information helps the user adapt to this environment in order to function successfully.

These three categories are simply a frame of reference for looking at information needed to carry out a military activity.

How information is categorized isn't important. What is important is getting the information to the users in a useful format.

How? Empathy. It's that simple. Most users don't care where the information came from. Once disassociated from a collection system, 90 percent of the information received is releasable to anyone with a secret clearance.

Provide the user with everything possible so they can get in, get it done and get home safely. Have empathy with the user, whoever that user is.

Next time you're about to omit something from a briefing because of high-level classification, ask yourself "how can I share this information with the user without compromising the source?"

Before you get up to brief the next user, ask yourself these three simple questions.

- Is it necessary?
- What is my purpose?
- Who is my audience?

It may mean you'll have to do a bit more work, but the user is getting what he or she needs.

How do you know if you've succeeded?

You may never know, but one day you may run into a user who says, "You know that information you gave me was just what I needed." ■

AIA visibility gained in exercises

by Airman 1st Class Jennifer Gregoire
HQ AIA/PA
Kelly Air Force Base, Texas

Within the past two years, the Readiness and Exercise Branch of the Directorate of Operations has grown to meet the needs of its customers and major commands and increased the Air Intelligence Agency's involvement in exercises.

By participation in planning conferences and exercises, AIA awareness is now Department of Defense wide.

"We provide intelligence products to military operations, inserting information operations capabilities, giving the warfighter a valuable force enhancement tool to ensure mission success," said Maj. Gregory Tindall, chief of command exercises.

"In addition, through exercises, we optimize our training opportunities for AIA information operators," said Tindall.

"People need to think of AIA

as a force multiplier and co-warfighter, not just support," said Lt. Col. Bernard Barris, chief, readiness and exercises branch. "We need to gain visibility by including information operations in every exercise to stay current with AIA's vision," said Barris.

Exercises like Blue Flag, Green Flag and Ulchi Focus Lens are excellent examples of where AIA has done just that.

"You cannot perform a military operation without information operations. Without accurate weather, for instance, you cannot plan. And without knowing an adversary's capabilities, you can't bring the right forces to the fight," said Capt. Shane DuGuay, officer in charge of command exercises.

"AIA needs to be in the initial planning process for an exercise. We need to know what the sponsor wants to accomplish, their training objec-

tives and their emphasis on the use of information operations," said DuGuay.

"In the initial planning conference, the customer may not always be keen on AIA's capabilities, but because it is the initial conference, there is still time to plan AIA resources in the exercises."

AIA's goal is to exercise information operations to enhance combat forces' warfighting mission. This can be done by teaming with the air component or Numbered Air Force and understanding their objectives, conducting information operations which contribute to exercise success, refining the information operations detachment embedding concept, executing reachback and identifying training opportunities for the agency. In short: demonstrating the AIA team capability. ■

315th improves force protection

by Capt. M. L. Yesville
315th IS
Yokota Air Base, Japan

Hacking attempts on Air Force Assets are detected daily and hacking is just one example of the damage that can be caused to command and control systems.

The 315th Intelligence Squadron, Yokota Air Base, Japan, developed a plan for command and control protection to demonstrate information operations application in force protection to protect against attacks.

The C2 Protect Project was proposed by Capt. Anthony Packard, former squadron director of operations, in 1996.

The 374th Airlift Wing utilized this C2-protect cycle. Many organizations provided information that was fused into a Yokota-specific threat analysis. Sixteen operational squadrons throughout Yokota Air Base compiled vulnerability information including communication links, methods and procedures.

The six steps:

Identify Critical Information

Critical information is a subset of essential elements of friendly information that should be concealed from adversaries.

Critical information is unclassified, but when pieced together, can give valuable clues to friendly plans and operations.

Identify Indicators

Events that precede critical activities can be indicators of pending operations.

Special or unusual support arrangements made prior to operations can give indications; non-secured paper trails can spell out details of a plan.

Analyze the Threat

The threat depends on the adversary, the types of collection systems and methods the adversary processes and the capabilities of his systems.

Analyze Friendly Vulnerabilities

Friendly vulnerabilities result from communications procedures, information flow and open or non-secure conversations about work conducted in a manner exploitable by an adversary.

The greatest vulnerability to security of any discipline is probably a lack of awareness about adversary intelligence collection capabilities, inherit vulnerabilities of friendly information systems and the usefulness of unclassified details to hostile intelligence analysts.

Assess the Risk of Loss versus the Cost of Protection

Since risk management was the goal, it was necessary to evaluate the loss versus cost. The risks and potential benefits associated with using vulnerable communications and processes compared to the benefits and costs of implementing stricter security.

Apply New C2 Protect Measures

The last step of the process involves putting the new plan into action, re-assessing it while keeping in mind that vulnerabilities still exist and remembering those vulnerabilities.

The 315th IS tailored the C2 protect report to focus on the highest priority threat nations in the Pacific region and threats indigenous to Japan.

The report identified threats and vulnerabilities with recommendations to reduce, eliminate or exploit them, given factors such as cost, impact on mission effectiveness and the probability of exploitation by adversaries.

The report also included a 374th AW-specific threat matrix, a frequency usage table and an information flow chart identifying exploitable communication links.

The threat matrix reflects the analysis of the vulnerabilities of friendly functions versus adversary capabilities to exploit them. The data for compiling the matrix was contained within the report and summarizes multiple pages into one quick-reference page.

The frequency usage table is a consolidated list used as a reference tool for assessing the vulnerabilities of 374th radio transmissions. The readily available listing of frequencies and users makes it easy for the commander to visualize the vulnerabilities his radio communications present to operations security.

A graphic displaying the information flow sequence for contingency tasking was also included to depict the flow of tasking information from the point of origin, the paths from organization to organization and the modes of communications used for each transmission.

Vulnerabilities associated with each mode of transmission were identified and applied to the threat matrix to determine the likelihood of intercept and exploitation.

Months of work on this six-step cycle resulted in better force protection in addition to command and control protection. ■