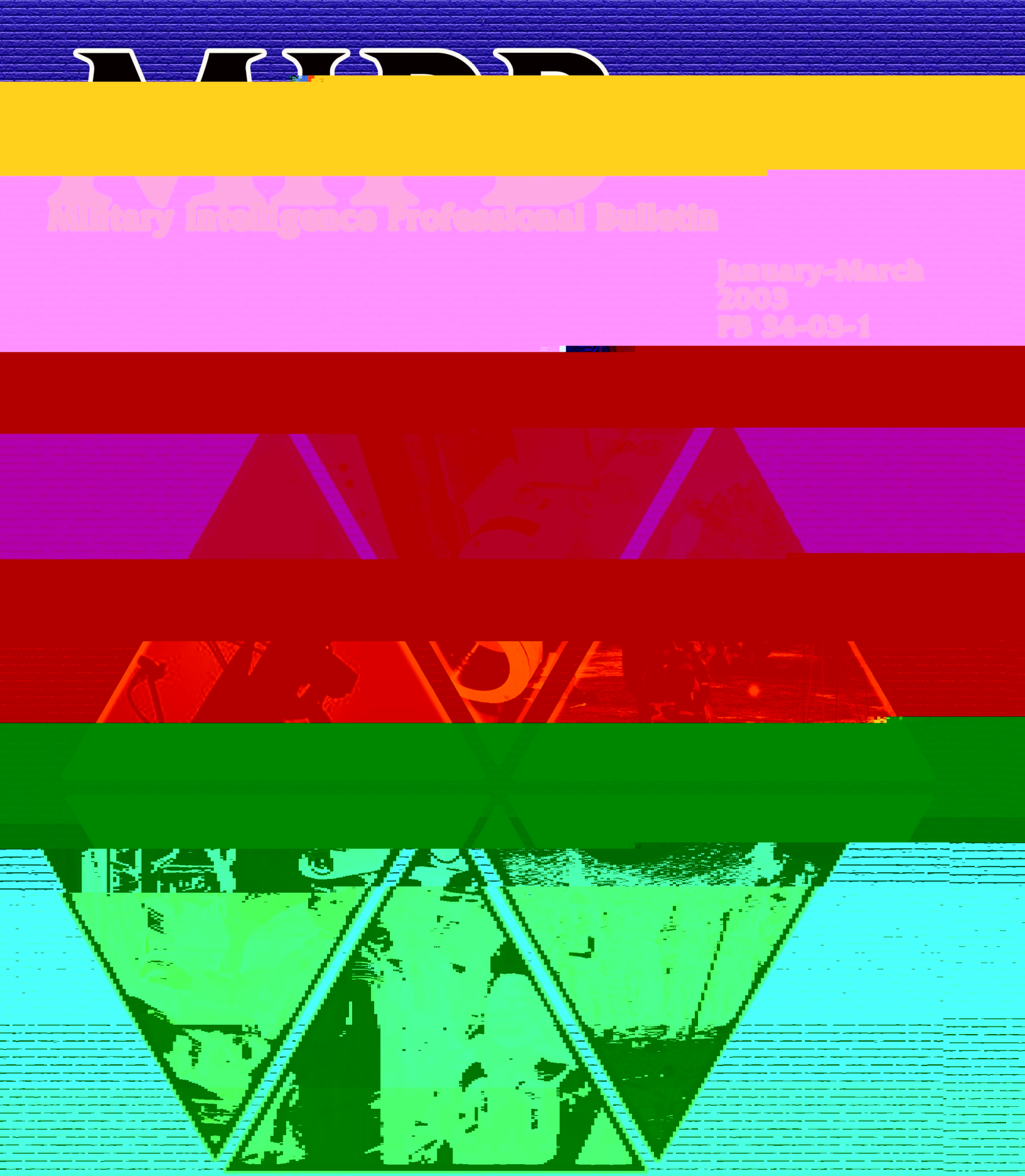
MIPB

Military Intelligence Professional Bulletin

January-March
2003
PB 34-03-1



Fundamentals of Intelligence

From the Editor

The initial theme of this issue of ***MIPB*** addressed a single aspect of the U.S. Army's ongoing Transformation, "Intelligence Synchronization." However, in light of the number and diversity of changes affecting the Military Intelligence community, it was determined that we needed to broaden the issue's scope. The change to "The Fundamentals of Intelligence" was designed to review the unchanging foundation of what we do in light of the ongoing Transformation.

These unchanging foundations can be distilled to three basic functions: collection, analysis, and production. While these functions capture the foundation of Army MI support to operations, we must expand upon their most basic form in order to reflect the greater specialization to support the full spectrum of Army operations from the six Intelligence tasks. These intelligence tasks reflect the unchanging foundations of what we do as MI professionals. However, they were neither codified nor aligned with the Intelligence Battlefield Operating System (BOS) tasks presented in the Army Universal Task List (AUTL).

The MI Doctrine Division seized upon the opportunity to not only ensure the Intelligence BOS AUTL tasks were synonymous with the Intelligence Tasks, but also to update the Intelligence Tasks to reflect their support to the force, and MI's role in supporting the Army Transformation. As you will see, the Intelligence Tasks are now subsumed under the four new Intelligence Tasks–which are also the Intelligence BOS tasks listed in the AUTL (FM 7-15).

The Army's Transformation process has addressed every BOS and every branch which will lead many revisions to our doctrine. FM 2-0, Intelligence (Draft), will serve as the Military Intelligence Corps' Tier 1 (Keystone) field manual. This field manual identifies the fundamental Intelligence tasks:

- Support to Situational Understanding
  - Perform Intelligence Preparation of the Battlefield (IPB)
  - Perform Situational Development
  - Support to Force Protection
- Support to Strategic Responsiveness
  - Perform Indications and Warnings (I&W)
  - Intelligence Readiness
- Intelligence, Surveillance, and Reconnaissance (ISR)
  - Perform Intelligence Synchronization
  - Perform ISR Integration
  - Conduct Reconnaissance
  - Conduct Surveillance
- Support to Effects
  - Support to Targeting
  - Support to Information Operations
  - Perform Battle Damage Assessment

This issue of ***MIPB*** provides many articles addressing one or more aspects of the fundamentals of intelligence. We cannot, however, point to these fundamentals alone as the reasons behind our success. We must not forget the most important element, the soldiers and civilians who execute the Intelligence mission day in and day out. The fundamentals offer a road map on what they are to accomplish and how they will accomplish it. It is for the MI soldiers and civilians, however, to achieve success through their training, innovation, adaptive thinking, and increasingly capable enabling tools. This issue of ***MIPB*** provides many insights on how that may be accomplished.

Michael P. Ley

Michael P. Ley

MILITARY INTELLIGENCE
Professional Bulletin

ALWAYS OUT FRONT

PB 34-03-1
Volume 29 Number 1
January-March 2003

FEATURES

DEPARTMENTS

By order of the Secretary of the Army:
Official:

JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army
0233801

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Always Out Front

by Brigadier General John M. Custer
Commander, U.S. Army Intelligence Center and Fort Huachuca

Much has been written recently about the Transformation of our Army. We are on a path from an "Iron Army" (whose strength has been based on layers of rolled homogeneous steel) to an "Information Army" (whose power revolves around the commander's situational understanding). This transformation portends great changes within Military Intelligence…our Branch. We should, however, understand up front that although the "how" of our business may drastically change, the "what" will remain constant throughout the Army's transformation. The "what" are the Military Intelligence core competencies that will provide the critical path in gaining greater importance and value as our Army transforms to a more flexible, more deployable, more lethal force.

The basic framework of the future force "See First, Understand First, Act First, and Finish Decisively" is firmly rooted in our core competencies. The systems we develop and the soldiers we train will prove to be both the enabling and the deciding factors in the Objective Force's ultimate success. The five Military Intelligence core competencies comprise the fundamental processes that make our branch so important to the Army today and so critical to the force we hope to build in the future. I use the acronym "ICAP2" to quickly enumerate our Military Intelligence core competencies. These equate to—

- **I**SR Synchronization.
- **C**ollection.
- **A**nalysis.
- **P**resentation.
- **P**rotection.

ISR Synchronization: The Objective Force's Future Combat System (FCS) will depend on the systems and sensor integration performed by intelligence soldiers, noncommissioned officers, and officers throughout the Unit of Action (UA) and Unit of Employment (UE). With thousands of sensors sending millions of reports, it quickly becomes clear that the synchronization and fusion of such vast amounts of information will be the critical path in the "See First" paradigm. Synchronization of sensors and systems from "mud to space" has long been viewed as a primary mission of Military Intelligence.

Collection: The unique collection capabilities of our branch will continue to be a vital resource for the Objective Force, and no other branch will contribute as much to the commander's situational awareness. The information provided by Aerial Common Sensor (ACS), Prophet, and the fleet of unmanned aerial vehicles (UAVs) will be crucial to the "Understand First" construct. Our human intelligence and counterintelligence professionals provide another facet to the unique collection equation, and automation or any other capability simply cannot replicate their contributions.

Analysis: Even as we build the future Army the need for human analysis at every echelon remains constant, as the "soldier in the loop" can never be replaced by computers. The Distributed Common Ground System-Army (DCGS-A) architecture will provide new analytical tools and the dissemination path for vast amounts of required information. Target recognition technologies hold great promise, but targeting success will require a human brain to decide whether a truck moving through enemy territory is in fact carrying artillery shells or school children. The advent of network-centric collaborative tools, flattened information environments, and reach to the joint level to facilitate targeting capabilities will prove the continuing requirement for human analysis at every echelon.

Presentation: The method a commander's staff uses to process data into information and ultimately knowledge

(Continued on page 4)

CSM Forum

by Command Sergeant Major Lawrence J. Haubrich
U.S. Army Military Intelligence Corps

In my last article I outlined in great detail the Quality Assurance Operating System (QAOS) and the Leader's Survey Program. The bottom line up front is: The surveys provide our Military Intelligence Corps the means to ensure that we train our soldiers to meet the needs in your formations and that Military Intelligence (MI) soldiers are trained to standard. I want to thank you, the MI leadership, for taking this Green Tab issue and making our MI Corps stronger and preparing our MI Warriors for success in the Objective Force.

Again, I ask our great MI leadership for assistance in building a stronger MI Corps in the Objective Force. Another Green Tab issue is that we need the leadership to look into the "STAR MOSs" in our great Corps. In the past, I have sent out several emails concerning MI STAR MOSs to the Command Sergeants Major and Sergeants Major in the MI Corps asking them to board our soldiers for promotion to Sergeant and Staff Sergeant. My comments regarding MI STAR MOSs are direct and to the point; we are not taking care of soldiers. We need to work on our STAR MOSs and leadership development for our Noncommissioned Officer (NCO) Corps to be successful in the Army and the Objective Force. I ask each of you to coach, teach, develop, and mentor our MI soldiers to be your NCO replacement. This process starts as soon as the soldier signs into your formation from initial entry training (IET). Promote those great MI warriors when they enter the zone and deserve to be recommended for the next grade. We are responsible for growing our NCO Corps.

I ask you, the MI leadership, to look in the mirror. Remember the NCO or Officer who took you under his or her wing, took a chance on you, and recommended that you go before the promotion board. Remember too that after you went to the promotion board, this process of coaching, teaching, developing, and mentoring continued. **Someone took a chance on Specialist 5 Lawrence J. Haubrich. Someone coached, taught, developed, and mentored him! That someone, who took a chance on Specialist 5 Haubrich, mentored him to become your MI Corps CSM.** I ask you, the MI leadership, to take that same chance. Groom those great MI warriors to become that NCO—the NCO that will take a chance on the future soldiers of the MI Corps.

During the last six months I was very fortunate to visit the 5th of the 104th Reserve MI Total Army School System (TASS) Battalion from Fort Huachuca, AZ, at Camp Parks Reserve Training area, Dublin, CA. There I observed our MI soldiers conducting a mobile training team (MTT) and training to standard those reclassified soldiers in MOSs 97B and 97E. While at Camp Parks I also visited the Western Army Reserve Intelligence Support Center (WARISC), the 250th MI BN (TE), located in San Rafael, CA, and the 223d MI BN (Linguist) located in San Francisco, CA. I want to thank their leaders for showing me around their units, briefing me on their mission and upcoming deployments, and, most importantly, for providing me with the opportunity to talk with those great MI warriors assigned to their units. I also attended the XIV Annual Army Technical Control and Analysis Element (ATCAE) Conference 2002 at the National Security Agency (NSA). There I had the opportunity to talk with soldiers assigned to the ATCAE and meet with several soldiers assigned to the 704th MI Brigade who work in various sections in NSA. NSA provides yet another example of our MI soldiers doing great things in the joint environment, "Worldwide Support to the Warfighter."

Thank you all for what you do for our MI Corps and our Army. As always, let us take care of each other and our families. You train hard, you die hard; you train easy, you die easy. Peace needs protection!

ALWAYS OUT FRONT!

(Continued from page 2)

makes the presentation of information another critical factor for a force that will perform battle command on the move. How the S2, or "Knowledge Officer," of the future packages and presents information will directly influence the commander's decision. This concept of "presentation" will emerge as an even more significant consideration for intelligence training as our automated processes constantly increase both reporting speed and the amount of information available to commanders. The S2, or "Knowledge Officer," will have to be confident and expert in selecting the crucial "nuggets" of information the commander requires. There simply will not be time for the commander to analyze everything, and any attempt will quickly debilitate unit operations.

The Military Intelligence core competencies will continue to provide the foundation for our Army's success in the Objective Force. Beginning long before deployment, these core competencies will continue to shape the battlefield and provide the cornerstone for victory. The allure of technology is narcotic but we must constantly remind ourselves that both today's Army and the Army of tomorrow need trained intelligence professionals who understand how to support tactical commanders by manipulating emerging technologies. These professionals will continue to be the centerpiece of our Branch and the Army.

Protection: Force Protection will continue to be of great importance to commanders, a requirement that must continue to be answered by Military Intelligence units and soldiers deployed across the battlefield. Every soldier bears a responsibility to protect the force but few have the total battlefield perspective of our branch. As we report enemy locations, activities, and intentions, Military Intelligence personnel are specifically contributing to the overall force protection effort.

Synchronized Chaos:
Visualization, Integration, and Dynamic Thinking

by LTC Stephen K. Iwicki

"See First, Understand First, Act First, Finish Decisively"

—Objective Force Concept

Across the spectrum of operations, intelligence is a dynamic and exciting endeavor. It involves interactions with many different organizations, systems, data networks, and most importantly people. The intriguing dynamic nature of the profession feeds life to the intelligence process and its people. As we enter transformation with a heavier reliance on automated systems, we must concentrate on developing free-thinking analysts rather than machine operators. We must recognize that it is the interaction of the human brain with the many different automated tools as well as with other analysts that allows us to make accurate assessments that support the decision-makers.

Our Army, our military, and our nation are undergoing a massive operational transformation as a result of significant international and domestic events over the last five years. The developments associated with our military's transformation efforts are forcing us to make major cultural changes in the way we perform intelligence operations. These factors challenge us to change the ways we visualize and present information, synchronize operations, and train the people who perform these critical missions.

Objective Force mission accomplishment and survivability depend heavily on accurate intelligence and reliable communications networks to enable rapid standoff engagements to destroy the enemy. Our Objective Force goals of near-perfect intelligence, high situation understanding, and timely, accurate targeting are critical if we are going to minimize the number of force-on-force fights. We must enable our units to maneuver out of contact while maintaining their situational understanding. It will be the Unit of Action (UA) (brigade of today) Commander's responsibility to synchronize all of these moving pieces, including information management, on a scale we have never seen before.

Our intelligence mission will be driven by the need for accurate databases. Graphics and text are the outputs of our analysis, but databases represent a large portion of the path to those products and as a result drive all of our visualization systems. Databases are essential to in-depth analysis, predictive assessments, time-sensitive targeting, and situational development for 0-96 hours. As intelligence professionals, our mission is to go beyond "CNN-type situation reporting" and identify trends and predict future enemy operations. While this type of product is often presented graphically, its analysis is based on historical tracking and link and nodal analysis, as well as the fusion and retention power of our individual analysts. If a unit does not take the time to build data libraries, there will be no historical research capability, and this will lead to flawed analysis.

The Army is making great strides as we transform to the Objective Force. More and more of our systems are continuing to achieve better connectivity towards creating the Common Operational Picture (COP). As a result, we are collecting more pieces of information that come to us over a growing variety of automated systems, communications networks, and data formats. If left unmanaged, we surrender increased situation awareness capabilities to chaos. The key to our current and future success is to synchronize the flow of intelligence to keep it alive, channeled to the right places, and constantly adjusting focus to meet the changing needs of our commanders. There are three steps necessary to achieve this basic goal: visualization, integration, and dynamic thinking.

Visualization: Developing and Monitoring with Interpretive Tools

Visualization is a term we loosely throw around in casual conversation without much thought. Most people equate visualization with sitting in front of a bank of monitors watching several visual feeds. Visualization is far more complex and begins with defining the scope of the problem and the commander's intent. This is our starting point for developing a common understanding of the situation and the direction we want to proceed.

We fuse our intelligence preparation of the battlefield (IPB) factors (enemy, friendly, and environment) to form the basis of the COP. Next we add our operational plan to broadly define the future situation and identify what we must accomplish to meet our objectives. Finally, we must communicate and display this "picture" so that the staff and subordinate commanders understand a shared vision. This is the critical starting point for all visualization efforts. It is difficult to achieve when the commander and staff are collocated. We are about to further complicate this endeavor by adding the new dimension of networked collaborative analysis ventures under the Objective Force operating concepts.

Now that we have started the process by creating in effect a static COP, we must move forward and put our visualization process in motion. We must collect the information

available to us and determine which data sources we can have pushed to us, which we must pull, and which ones we may only be capable of observing. The dimensions of *"Push, Pull, Observe"* will change dramatically as we move from the Legacy Force to the Interim Force and finally reach the Objective Force.

Push

Today, we need to have record message traffic pushed to us to populate database systems. We also need to push non-record message traffic products, such as briefings and assessments, via email from the relevant commands with whom we participate. As we reach Objective Force capabilities, data will be pushed across distributed networks to automatically populate common databases accessable to the entire force. Smart filters and defined user profiles will help ensure that users get what they want without having to specifically ask for it.

Pull

We need to be able to pull products that organizations post to their secure home pages. This is important because usually the higher organizations never receive the complete distribution list for record message traffic. Often times, it is quicker for a tactical end-user to pull the message or product from a secure home page instead of waiting hours for the record message traffic to hopefully arrive over a small communications pipe. Additionally, over the last few years, a new problem has arisen where several other service organizations only post their reports and no longer bother to send out record message traffic. That means find it, pull it, or never see it. As we reach the Objective Force, the pull function will merge with our virtual collaboration efforts with lower, lateral, and higher headquarters via the Global Information Grid (GiG).

Observe

This aspect is something we do all the time but do not always incorporate it into the formal doctrinal process. There are many aspects of intelligence that come to our attention via near- real time (NRT) displays. These include unmanned aerial vehicles (UAVs), air defense artillery (ADA), counterfire data, some theater imagery intelligence (IMINT), and real-time human intelligence (HUMINT) reporting via radio, to name a few. Most of these are critical pieces of our decision cycle that must make it into a database because they are mentally integrated into our analysis process. As this currently occurs, by the time an analyst takes the time (if they do it at all) to generate a record message traffic report to send to and correlate into all-source analysis system (ASAS) or the COP, the value of the information has likely expired. We will leverage advances in metadata tagging technology and automatic target recognition (ATR) to solve this problem. The benefits of technical meta data use include source system identification, data quality measurement, and improved database administration. ATR will eliminate the current gap of information collected but never entered in the database. Databasing information from visual products will remain a significant challenge until this technology matures.

***Doctrinal Note**: ATR is also listed as target recognition aides.*

Combining *"Push, Pull, Observe"* is the most difficult visualization challenge that we face. We must figure out a way to bring all three of these information dimensions together in an integrated, time sensitive, ergonomically smart automation environment that updates the COP and our common databases in NRT. Some of these feeds do not belong to the Intelligence Battlefield Operating System (BOS), but are critical for our success. We must also ensure we have a common understanding of both visualization systems and visualization needs across the command.

This entire system has come a long way since the days of Desert Storm when we had paper maps, no web pages, no email, and a lot of courier missions. We have a long way to go if we are going to make the next technological leap forward (not a small percentage improvement) that is required for the "near perfect intel" expected with the Objective Force. What it really means are better trained, proactive collection managers and analysts that understand dissemination is a two-way street and are prepared to lead data-mining efforts to monitor our situation development and targeting; locate the answers in a timely manner; and present that intelligence in a manner consistent with our commander's visualization needs.

Integration: Information Channeling and Management

While visualization helps show us what we know, the integration process is how we maintain the COP, enable situational understanding and, more importantly, define our information gaps. I recently had the chance to hear four senior intelligence officials from the Department of Defense (DOD), Congress, and the National Intelligence Community speak in separate forums about what they felt were the major changes needed in the U.S. Intelligence Community. They all had several common themes that point to integration. First, all were in agreement that people are our most valuable asset and we need to better train and manage them. Second, they all mentioned that decision-makers generally follow three rules when receiving information: Tell me what you know; Tell me what you DON'T know, and Tell me what it means. Most of these individuals ranked telling what we don't know as the most important of the three factors since it represented the area

of greatest risk when making a decision.

Integration is the means by which we manage the complex process of simultaneous intelligence operations. It is simultaneous because we are performing many different analytical functions at the same time. We are working the current fight, shaping the decisive fight, and sustaining intelligence operations while simultaneously contributing to the future fight and working toward the desired endstate conditions. We have to manage multiple information cycles and integrate a wide variety of data formats to make this process work.

Data integration technology is changing rapidly. We are shifting to a knowledge-based force. The Army is trading off 50 tons of rolled steel protection (tanks) for the ability to rapidly deploy, see first, understand first, act first, and finish decisively. That means our Army is more dependent on accurate intelligence than ever before. A conservative estimate is that the UA will receive over 17,000 reports per hour from organic sensors alone. Some of these inputs will be fully automated, some will require human cognitive interaction, and some will be automation-assisted actions. The UA will have a varying requirement for outside intelligence support as it moves across the spectrum of operations. The UA will be heavily dependent on outside sources during deployment and entry operations (much like we are dependent on higher and national today). It will be heavily dependent on organic intelligence, surveillance, and reconnaissance (ISR) during decisive operations (similar to today, but with much greater organic capabilities). The challenge is making it all come together faster and with a smaller forward footprint.

Automated sensor exploitation and sensor correlation provides a degree of data and information fusion, but only a human can generate knowledge. Knowledge-centric warfare means that precise, detailed, timely, and relevant knowledge is required to enable full spectrum operations. Knowledge enables the commander's understanding and guides his decisions on where to fight, when to fight, and how to fight. Senior Army leaders have seriously asked if the UA S2 needs to be a lieutenant colonel (LTC). That is not as far-fetched as some may think. The job probably will be as hard or harder than the job of a Division G2 today.

We all have to remember that information fusion and analysis are processes that require a combination of smart automated processing systems and interaction with the human brain. Any automation system is simply a tool we use in our trade. If we are good at it, we can exploit it to answer our commander's needs. These systems come in many forms that allow us to access raw and finished products, view live imagery, maintain situational awareness, and engage the enemy through the targeting process. Our systems and people reach up, down, and laterally to push, pull, and observe information. In order for us to be effective, we must bring all of these factors together to understand and communicate what it means. The technology revolution has transformed our primary method of disseminating information to classified web posting, electronic sharing of files over networks, and email. During Operation ALLIED FORCE in 1999, we could rapidly pull imagery and reports from a secure homepage within several hours, while the record message report distribution usually did not arrive until several days later. That is a major difference in the timeliness of reporting. As a result, a critical issue for Army Intelligence is that the Intelligence Community is evolving beyond our dependence on stovepiped record message traffic. We must now address all the planning factors and data formats shown in Figure 1.

This change is due to increasing demands for quicker, NRT reporting and fusion that our current dissemi-

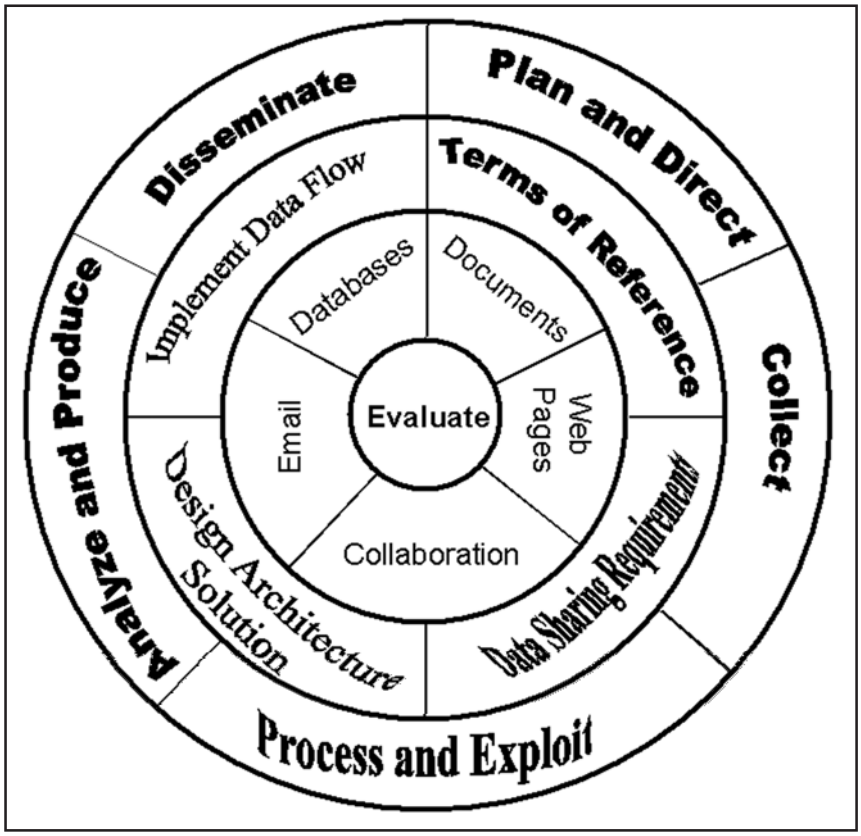


Figure 1. Planning factors and data formats.

nation channels simply cannot process quickly enough. *Commanders now demand intelligence reporting in minutes and hours, vice hours and days.* We now use voice reporting, classified E-mail, and web postings to share information with consumers quickly. Despite U.S. Message Text Format (USMTF) requirements, in reality, formats are no longer standardized and vary with each unit, command, and operation. No current system is capable of taking these various inputs and correlating them into a common database without significant human effort.

The Intelligence Community has significantly evolved since the birth of our first flagship system, the All-Source Analysis System (ASAS). We have added significant real-time and NRT intelligence collection systems that provide a variety of visual product formats. As a result, the MI Branch capabilities have evolved and the timeliness of our information has dramatically improved.

Our current challenge is to process properly the increasing quantities of information that come in many different formats and fuse it into usable intelligence support to our commanders. ASAS is the fusion system that will take us from the Legacy to Objective Force. In the Objective Force, the new Distributed Common Ground System-Army (DCGS-A) will be the key ISR processor at all echelons, receiving and managing data from national and Joint ISR sensors, aerial common sensor, tactical UAVs, Prophet, and all the way down to UA organic sensors.

Despite all of these challenges, the major drawback with visualization and integration is that it tends to ignore our information gaps. This is where dynamic thinking comes into play. We must remember that machines are only tools of our trade and we cannot rely on them to hand us the correct answers.

Dynamic Thinking: The Necessary Synthesis Skills

It is our job to understand the decision-maker's intelligence requirements and manage our efforts to meet those needs. Synchronizing the chaotic information sphere is critical to our success. Are we thinking multidiscipline? Are we cross-cueing assets based on single-source tip-offs? Are we monitoring all available NRT collection systems and correlating what we see against both an all-source database and the COP? When leaders ensure these types of things are happening, the people in our organizations will virtually guide themselves to answering the commander's needs. It is not magic, it takes trained people who know their assigned systems, know where to look for the necessary inputs, and, most importantly, constantly communicate with each other. The danger is that we become "COP-centric" in our focus and fail to be predictive in our assessments and mission planning.

As I stated earlier, it is at this stage that we must synchronize the flow of information, to keep it alive, channeled to the right places, and constantly adjusting focus to meet the changing needs of our commanders. I strongly believe technology is the number one enabler for our MI soldiers. Technology will never replace the analytical power of the human brain but, in the hands of a good analyst, it is a major combat multiplier. We should embrace technology and experimentation at every opportunity. This is not always a conventional approach, but it has always been a learning experience for our soldiers and an improvement to the way we produce intelligence. No task is impossible. We just lack the imagination to see the solution.

While MI is clearly a system of systems, many of us fail to recognize that computers and other technologies are the weapons system for MI. Leaders and analysts use them across all three networks (Unclassified, Collateral, SCI) to conduct a variety of intelligence functions. We will increase our reliance on these systems as we move towards multi-level security networks and virtual intelligence centers that tie together subject matter experts working in collaborative environments.

We need to develop our analysts and leaders better so that they are capable of dealing with the dynamic nature of our business. Our leaders must understand how to set the analytical focus of our intelligence organizations and they must clearly understand the commander's requirements, his language terms, and recognize where trade-offs may have to occur to reach those objectives. Our leaders must recognize the impacts that the fluid nature of battle has on their intelligence operations. We must be dynamic in our thinking and our actions. We must synchronize intelligence support to multiple full-spectrum fights while constantly performing a mental ISR wargame of possible branches and sequels to the current analytical effort.

Developing intelligence soldiers of all ranks is crucial. We may need to reverse current trends and start junior soldiers and officers working at the higher echelons of the Intelligence Community to learn both the analytical process and the resources of the information environment. We will need our best and most experienced MI soldiers serving on the front lines in the UA.

The Future

As we continue with transformation, we need people who are "master" intelligence analysts, understand the language and meaning of tactical operations, are automation system smart, and know our U.S. and coalition information sphere well enough to know where to look for the answers we need. You do not learn this

(Continued on page 14)

BENCHMARK FOR INTELLIGENCE TRANSFORMATION

by Michael C. Taylor

The views expressed in this article are those of the author and do not supersede approved Army intelligence doctrinal litearture. Details of emerging doctrine as reflected in FM 2.0, Intelligence, can be found in this issue in Mr. Chet Brown's article in the Doctrine Corner.

The Army is entering a period of intense self-examination and change that will alter our current understanding and expectations of the Intelligence Battlefield Operating System (BOS). Specifically, the "what" and "how" of intelligence, surveillance, and reconnaissance (ISR) will change over the next few years as new concepts, doctrine, and materiel transform the Army into the Objective Force (OF). The success of the transformation of intelligence hinges in part on building a common understanding of the fundamental features of the Intelligence BOS. This article attempts to facilitate that understanding and provide a benchmark for analysis by sharing some insights on current intelligence operations developed since the publication of FM 34-1, *Intelligence and Electronic Warfare Operations*, in 1994.

INTELLIGENCE BATTLEFIELD OPERATING SYSTEM

What is the Intelligence BOS? The Intelligence BOS is one of the Army's seven BOSs. Based on the definition of BOS in FM 3-0, *Operations*, the Intelligence BOS is a flexible force of personnel, organizations, equipment, tactics, techniques, and procedures that, individually and collectively, provide commanders with the relevant information and intelligence they need to visualize the battlefield, understand the situation, and direct military actions. Inherent within the Intelligence BOS is the capability to plan and direct intelligence operations; collect and process data into information; produce intelligence; and disseminate the intelligence and other critical information in an understandable form to those who need it, when they need it. Additionally, electronic warfare and counterintelligence capabilities within the Intelligence BOS support the commander in achieving information superiority on the battlefield.

Essential Terminology

What are the essential definitions used within the Intelligence BOS? There are several, but in recent years the use of three words has brought both confusion and clarity to Army concepts, doctrine, and training. The terms are *intelligence*, *surveillance*, and *reconnaissance*. The confusion stems in part from the challenges inherent within the spiral development of concepts, doctrine, training, force structure, and materiel. The spiral creates a swirling mixture of new, misused, and obsolete terminology that often undermines our ability to understand emerging concepts and doctrine. Common understanding of the meaning and usage of ISR is essential to an objective assessment of how to improve the Army's ability to "See First" and "Understand First."

The May 2002 draft of FM 6-0, *Command and Control*, clarified the collective use of ISR as *"an enabling operation that integrates and synchronizes all battlefield operating systems to collect and produce relevant information about the enemy and environment to facilitate the commander's decision-making."* This statement establishes the symbiotic relationship between collection (surveillance and reconnaissance) missions and intelligence production. Simply put, surveillance and reconnaissance are "how" the Army collects information while intelligence is "what" results from the analysis of that information.

With the relationship established, the next hurdle is to define each term. The following proposed definitions attempt to clarify each word by refining, updating, or expanding the definitions found in current Army and Joint doctrine.

- **Intelligence.** Facts and estimates derived from the evaluation, analysis, and interpretation of information about enemy and other features of the operational environment. The purpose of intelligence is to provide knowledge of the enemy and environment that supports situational understanding and decisive action.
- **Reconnaissance.** Transitory observation of an enemy and other features of the operational environment within which friendly

ARMY BATTLEFIELD OPERATING SYSTEMS

Intelligence
Maneuver
Fire Support
Air Defense
Mobility, Countermobility, and Survivability
Combat Service Support
Command and Control

and enemy forces may operate. The purpose of reconnaissance is to collect information that establishes the current disposition, activity, and capability of an enemy or the current condition of environmental and geographical characteristics of an area.

- **Surveillance.** Sustained observation of an enemy and other features of the operational environment within which friendly and enemy forces may operate. The purpose of surveillance is to collect information that establishes norms and detects change in enemy, environmental, and geographical characteristics.

It is important to note that intelligence does not equate exclusively to the U.S. Army's Military Intelligence (MI) Branch. Intelligence operations are the missions and actions taken to collect information and produce intelligence on the enemy and operational environment. For the most part, intelligence products do result from the application of specialized skills of MI personnel. The process, however, relies upon MI and non-MI personnel of all military services as well as other federal organizations.

It is also important to understand that surveillance and reconnaissance are not limited to missions undertaken by infantry and cavalry scouts, special operations personnel, and MI units. In reality, each soldier and all types of units are potential reconnaissance and surveillance (R&S) resources. Whether directed in orders or in accordance with standing operating procedures, these resources collect and report information on the enemy and other features of the operational environment. When coordinated, these resources coupled with units trained and equipped specifically for R&S provide the situational awareness that contributes to situational understanding and decisive action.

FUNDAMENTAL PRINCIPLES

What are the principles that guide the Intelligence BOS through the spectrum of military operations? The 1994 edition of FM 34-1 lists five principles for "Force Projection Intelligence and Electronic Warfare" operations. Since then, however, these principles have been looked upon as one principle and four techniques. The "Primary Features of the Intelligence BOS" in the same manual are probably a better representation of the fundamental principles of the Intelligence BOS. Based on these features and emerging OF concepts, there are at least four emerging principles that could guide the Intelligence BOS:

- **Engaged.** The Intelligence BOS is always engaged. Sustained, real-world intelligence operations are critical to the strategic responsiveness of the Army and the success of intelligence operations. Through continuous peacetime intelligence operations, commanders ensure collection, processing, production, and dissemination infrastructure is in place and prepared to provide ISR support throughout the range of military operations. The commander and intelligence staff must assess each contingency to determine information requirements and develop a plan for filling information voids. This principle is tempered by the imperative to prioritize efforts and prepare thoroughly for most likely contingency missions. During execution, the personnel of the Intelligence BOS ensure commanders, their staffs, and their subordinates have the intelligence they need to understand the operational environment, act decisively, and protect the force from deployment through redeployment.
- **Focused.** The Intelligence BOS must focus on the missions, requirements, and battlespace of the operational, and tactical forces. Intelligence BOS personnel must have the situational awareness and initiative to anticipate and satisfy the information requirements of these forces. ISR organizations at each echelon must collect information and produce intelligence tailored to the needs and capabilities of these forces. Personnel of the Intelligence BOS must ensure critical information reaches decision-makers in time to influence planning, preparation, and execution of their operations.
- **Networked.** The Intelligence BOS is a part of a seamless information environment in which networked organizations share information to enhance the awareness and effectiveness of all users. The Intelligence BOS relies upon trained personnel and technology to continuously improve its ability to process data, share information, and disseminate intelligence. Its networked operations provide access to data, information, and intelligence within a secure communications and processing architecture. The Intelligence BOS maintains an architecture that ensures the "push" of critical information from National, Joint, and theater organizations to the lowest tactical unit. At the same time, the BOS ensures the operational and tactical force have the ability to access relevant information and expertise resident in supporting intelligence organizations. Each organization or node within the Intelligence BOS architecture facilitates the accessibility and exchange of data, information, and intelligence.
- **Disciplined.** The Intelligence BOS is a disciplined force that ensures its operations comply with the letter and intent of the laws and regulations of the United

States, specifically those governing the rights of U.S. persons and the protection of classified information, sources, and methods.

PRIMARY MISSIONS

What are the missions of the Intelligence BOS? As shown in the Figure 1, the military, civilian, and contractor personnel within the Intelligence BOS conduct five primary missions that incorporate and provide context to the primary intelligence tasks found in FM 34-1.

Support Readiness and Planning

The Intelligence BOS supports unit readiness and planning by knowing how the enemy organizes, equips, trains, fights, and controls its forces within diverse operational environments. Intelligence staff must provide the knowledge of the enemy that the commander needs to efectively plan and prepare the unit for military operations. The commander looks to the intelligence staff for mission-oriented intelligence and intelligence training on potential enemy forces and operational environments. The intelligence staff depends upon ISR personnel within the command and supporting organizations to be sources of information and knowledge on the enemy and environment. Using these sources, the intelligence staff develops general military intelligence (GMI) and intelligence preparation of the battlefield (IPB) products that enable understanding of the enemy and the military aspects of terrain, weather, and civilian population.

The accuracy and detail of the GMI products have a direct impact on how well units plan and prepare for operations. The intelligence staff creates and refines GMI by gathering open-source information, requesting intelligence products from higher echelon intelligence organizations, and using information from supporting intelligence production elements. A comprehensive intelligence database derived from open-source and GMI products results in the intelligence staff's developing an objective assessment of the enemy that commanders can use to—

- ❑ Conduct realistic training.
- ❑ Recognize potential enemy intentions, objectives, capabilities, and courses of action (COAs).
- ❑ Focus the ISR effort.
- ❑ Employ effective tactics and techniques.
- ❑ Take appropriate security measures.

IPB begins with the GMI products and products accompanying operations orders. IPB is an analytic procedure that helps commanders develop a clear understanding of the current state, envision a desired end state, and then visualize the sequence of activity that will move forces from their current state to the end state. The staff's integration and presentation of IPB products during planning ensures commanders can visualize the battlefield, a key aspect of battle command. IPB products developed during mission analysis and refined during wargaming provide the analytical foundation needed to plan operations and apply combat power or effects at the critical points on the battlefield, both in time and space. Successful situation development, support to targeting, support to force protection, and requirements management (RM) all hinge upon the understanding of the enemy, terrain, weather, and civilian considerations developed through the IPB process.

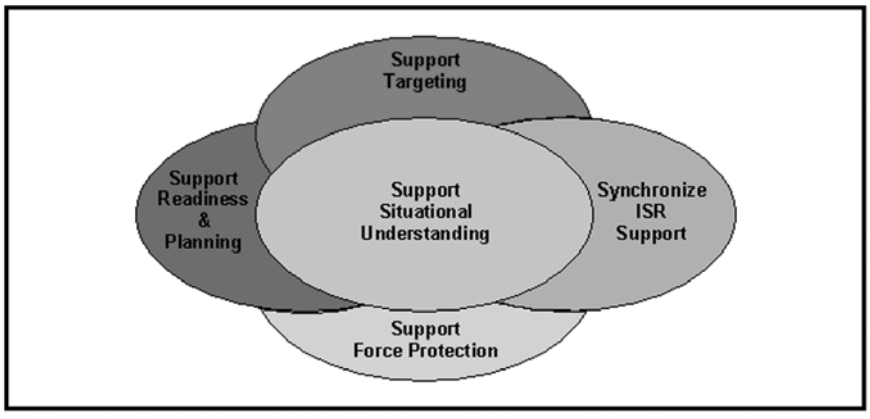


Figure 1. Primary Intelligence BOS Missions.

Support Situational Understanding

The Intelligence BOS supports situational understanding by analyzing and interpreting information on the disposition, activity, and capabilities of the enemy. To begin analyzing the enemy situation, the intelligence and operations staffs must first develop and manage a flexible ISR plan that describes how the Intelligence BOS will answer the commander's priority intelligence requirements (PIRs). The plan identifies the information requirements (IRs) that provide the focus for ISR efforts against the enemy and environment within the command's area of operation (AO), area of interest (AOI), and area of intelligence responsibility (AOIR). The plan is an integrated staff effort that ensures the Intelligence BOS supports the preparation for and execution of the unit's maneuver, fire support, logistics, and security operations. Through the plan, the staff can monitor and assess the information and intelligence that form the basis of situation development.

Situation development is an analytic procedure for producing current intelligence about the enemy and environment during operations. The procedure helps the intelligence staff recognize and interpret the indicators of enemy intentions, objectives, combat effectiveness, and potential COAs. Through situation development, the intelligence staff is able to monitor enemy activity, identify in-

formation gaps, make recommendations, explain enemy activities in relation to the command's current and future operations, and assist the commander in gaining situational understanding. The intelligence staff maintains, presents, and disseminates the results of situation development through personal interaction with the commander and staff as well as in the command's common operational picture (COP) and tailored intelligence products.

Support Targeting

The Intelligence BOS supports the targeting process through target development, target acquisition, electronic attack (EA), and battle damage assessment (BDA). During the DECIDE phase of targeting, the intelligence staff in conjunction with the operations staff uses target development techniques to systematically analyze enemy forces and operations to determine high-value targets (HVTs), target systems, and system components for potential attack through maneuver, fires, or information. In the DETECT phase, target acquisition requires surveillance and reconnaissance resources to detect, identify, locate, and track high-payoff targets (HPTs) for delivery of lethal or nonlethal effects. During the DELIVER phase, these effects may include the use of EA against enemy command and control systems as part of the command's fire support plan and information operations (IO) objectives. For selected HPTs, ISR resources collect information and produce BDAs on the effects of the targeting effort. This role in the ASSESS phase of the targeting process supports the staff in developing combat assessments and reattack recommendations for the commander.

Support Force Protection

The Intelligence BOS supports force protection through sustained intelligence and CI operations. These operations provide indications and warning (I&W) of enemy intentions and unanticipated actions that threaten the unit's preparation for and execution of its operations. They assist the commander in identifying and protecting friendly forces as well as essential elements of friendly information (EEFI) from enemy intelligence assets, terrorism, subversion, and espionage. Specifically, CI resources identify and evaluate enemy ISR capabilities as they affect the command's security and deception operations. The assessment supports the commander and staff in developing the command's security program, conducting counterreconnaissance and rear area security operations.

Synchronize ISR Support

The Intelligence BOS synchronizes the collection, processing, and production functions of the intelligence process into a unified, multi-source, and multi-echelon effort that answers the commander's PIRs. Synchronization, in conjunction with the integration of ISR missions within the unit's operation, is a fundamental aspect of achieving an accurate and comprehensive understanding of the enemy and environment. In its simplest form, intelligence synchronization recognizes the potential of each soldier and unit, when properly coordinated and directed, to be a collection asset capable of gathering information that the commander and staff can use to understand the situation, plan operations, target the enemy, and protect the force.

The intelligence staff uses RM techniques and procedures to synchronize intelligence operations into the commander's planning, preparation, execution, and assessment of operations. The operations staff uses the Military Decision-Making Process (MDMP) to integrate ISR tasks and resources into the task organization and missions of subordinate units. Analysis and control mechanisms within the Intelligence BOS help the staff to identify information shortfalls and to rapidly redirect resources to new collection and production priorities. Where the commander needs to "see" beyond the capabilities of organic assets, the intelligence staff uses RM procedures to leverage higher echelon ISR resources to collect information and produce intelligence that answer the commander's PIRs.

INTELLIGENCE PROCESS

How does the Intelligence BOS accomplish its primary missions? Successful commanders ensure the synchronization and integration of ISR activities into the planning, preparation, execution, and assessment of their operations. The Intelligence BOS uses the intelligence process, focused through RM, to synchronize ISR support and accomplish the primary missions described earlier. The intelligence process is based on a cyclical model that depicts how the Intelligence BOS uses information management to collect information and produce intelligence that answers the commander's IRs. Each function in the intelligence process is designed to deliver relevant information and produce knowledge (intelligence) that supports the commander's mission and concept of operation. The Figure 2 illustrates how the intelligence process, coupled with ISR management, answers the commander's information requirements (objectives).

Plan and Direct

The planning and directing function of the intelligence process begins with the commander's initial assessment and guidance to the staff following receipt of mission from higher headquarters. In his guidance, the commander states his initial information needs regarding the friendly forces, the enemy, and the environment. Refined and prioritized in later steps of the MDMP, the commander's critical information requirements (CCIR) identify the information the commander must know about the enemy and the environment by a particular time or event to successfully plan, prepare, execute, and assess operations. Concurrent with

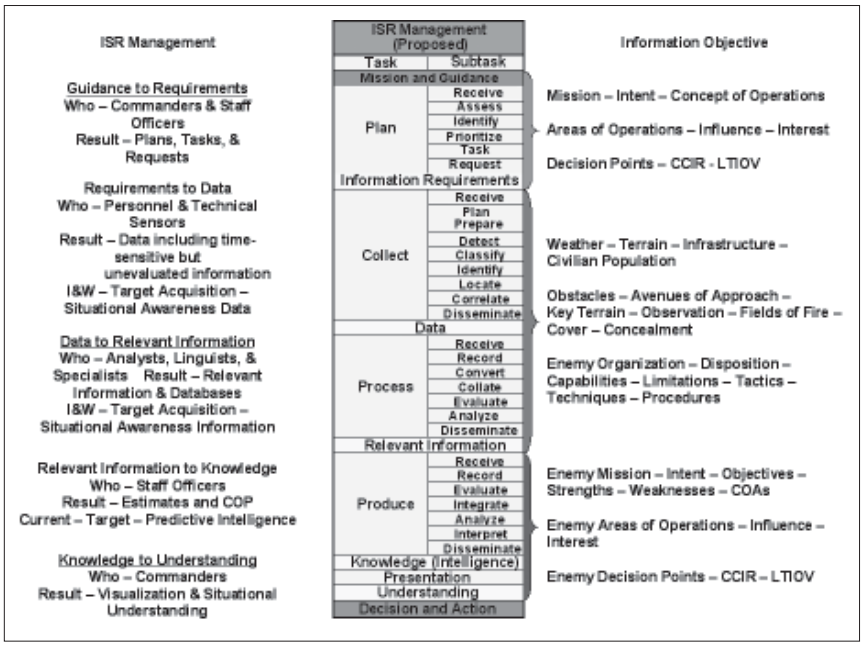


Figure 2. Army Intelligence Process.

the development and approval of the PIRs, the intelligence staff produces its staff estimate and an ISR plan that considers all available ISR resources. The intelligence staff expresses the requirements as either production or collection requirements and requirements that cannot be satisfied by organic or attached ISR assets are forwarded to the supporting intelligence organizations for validation and inclusion in their ISR efforts.

Collect and Process

Collecting and processing functions begin with the receipt of a task or order and end with the reporting of processed data as relevant information to the commander, staff, and other appropriate users in a form suitable for action or production of intelligence. The collection function includes the command, control, organization, and maneuver of organic or supporting R&S assets into positions where they can satisfy collection objectives and report the information. The intelligence staff works with the unit's operations staff to develop orders and requests that direct the execution of the ISR plan. The processing function entails the conversion of raw data into information that the intelligence analysts can use to produce intelligence or, when of critical or exceptional nature, the commander and staff can readily act upon. Normally, the collecting unit also controls the processing personnel and sensor-unique processing equipment thereby allowing the unit to evaluate the relevance of the information before reporting it. Once data is collected and processed (if necessary), the R&S resource reports the relevant information in accordance with the collection objective and reporting instructions. This relevant information, while potentially actionable, remains distinct from the intelligence because the information has not undergone the scrutiny of analysis within the intelligence staff or supporting intelligence production organization.

Produce

Intelligence analysts evaluate, analyze, and interpret information from single or multiple sources to produce intelligence. Analysis adds value to information by determining the accuracy and validity of combat information and single discipline intelligence reports, thus reducing the potential for deception or erroneous information reaching decision makers and entering into intelligence databases. Analysis and production are driven by expressed and anticipated information requirements on an AO, AOI, and AOIR. The intelligence staff coordinates and directs intelligence production to provide tailored intelligence products to the unit commander, staff, and subordinate forces. Analysis and production occur in the intelligence staff and separate production elements at each echelon from battalion to national level agencies. Effective production management ensures that the unit receives the intelligence products and services required to accomplish the assigned mission.

Disseminate

The intelligence staff disseminates intelligence within the staff and to headquarters of higher, adjacent, and subordinate commands. The intelligence staff also ensures the timely delivery, integration, and presentation of relevant information and intelligence in a tailored form that is readily understood and directly usable by the unit commander, staff, and subordinates. These products should not overload the commander, staff, or the unit's information system capabilities. During multinational operations, the intelligence staff must work with a number of intelligence organizations to ensure that classification and releasability instructions support the timely dissemination of intelligence and CI products to multinational forces.

Dissemination consists of both "push" and "pull" techniques. The information push technique ensures subordinate, higher, and adjacent units receive time-sensitive and critical I&W, targeting, and situational awareness information. The information pull technique allows units to retrieve products considered relevant to their operations. The pull technique requires the unit to have direct electronic access to databases, intelligence files, web-based homepages, or other repositories of higher and lower echelon intelligence organizations.

Assess

While not a distinct function in traditional intelligence cycles, assessment occurs during each function of the intelligence process. The assessment begins when the commander and staff receive the mission and determine information requirements. Prioritized into CCIR, these requirements drive information collection and intelligence production efforts. The commander and staff measure the effectiveness of the ISR effort against the following standards:

- **Timely.** Relevant information and intelligence must reach the commander with sufficient time remaining to influence decisions, prevent surprise, and support planning. Timely reporting, analysis, and presentation of critical information enables the commander to understand first, act first, and finish decisively.
- **Relevant.** Intelligence must answer the commander's IRs about the operational environment within his AO and AOI. ISR resources must collect, process, produce, and disseminate information that helps the commander to visualize and understand his battlespace.
- **Accurate.** Intelligence must provide a balanced, complete, and objective picture of the operational environment. When doubt exists, the intelligence staff must capture and present that uncertainty in measurable terms to the commander. The commander then makes the decision as to whether the risk fostered by uncertainty of the enemy situation is acceptable or unacceptable to the mission.
- **Predictive.** Intelligence must provide the commander with the facts and estimates needed to anticipate enemy intentions, objectives, capabilities, and COAs as well as other factors of the operational environment. Predictive intelligence, coupled with an uninterrupted flow of current relevant information, provides the operational advantage the commander needs to achieve information superiority and act decisively.

Conclusion

The Army will transform into the Objective Force. The success of the Intelligence BOS's transformation will hinge on developing a common understanding of how the Army operates and what needs to change. Hopefully, this article in some measure facilitates that understanding and provides a benchmark from which to shape the future of Army Intelligence.

*Mr. Taylor was the primary writer for the 1994 edition of **FM 34-1, Intelligence and Electronic Warfare Operations**. Since his retirement in 1999, he has worked as a contractor leading the U.S. Army Intelligence Center's doctrine development effort for the Force XXI and the Objective Force. His other published works include FMs on the All-Source Analysis System, digital division and brigade intelligence operations, and the Initial Brigade Combat Team as well as several articles in MIPB. His military service included assignments as a signals intelligence analyst at tactical, operational, and strategic intelligence organizations supporting U.S. operations in Europe, Southwest Asia, and Korea. He holds a Bachelor of Arts in Russian Studies from the University of Maryland. He is a certified National Security Agency Traffic Analyst and a graduate of the Senior Enlisted Cryptologic Supervisor Course. Readers can reach Mr. Taylor through the Chief of Doctrine Division at comm. (520) 538-1749 or taylor1m@fhu.disa.mil.*

Synchronized Chaos:

(Continued from page 8)

in a schoolhouse environment, but through experience on the job and old-fashioned mentoring. Mentoring is something that we do very poorly these days, but it is also the key element in growing the soldiers required across our rank structure.

Our leaders must also have ergonomically designed display systems that let them toggle back and forth between relative sources of live information and assessed intelligence feeds from a relatively small "battle bridge." DCGS-A is one tool to meet this requirement. DGCS-A will have a variety of configurations that range from software applications within the Future Combat System (FCS) vehicles, to workstations in the UA, to serving as the "mainframe" conduit at Home Station Operations Centers (HSOCs), regional Information Dominance Centers (IDCs), and Knowledge Centers at the theater, joint, and national levels.

The shape of our intelligence organizations is also likely to change dramatically. Many of the functions traditionally done in the analysis and controls element (ACE) may be performed with the majority of our analysts operating from HSOC with a smaller number of personnel and equipment deployed forward in the area of operation. I believe the NRT aspect of the ACE will no longer function from a centralized location, and the ACE will become more of a virtual organization.

Exciting times are ahead for the Army Intelligence Community. We need to work closely with the Objective Force equipment designers to ensure they understand our requirements and deliver the equipment, organizations, and battle command systems we need to provide the near-perfect intelligence picture of the Objective Force. The soldiers fighting on the battlefield are depending on ISR to make up for the trade-off of 50 tons of steel protection. We cannot afford to let even one of them down.

Supporting Close Combat:
Intelligence Synchronization

by Dennis Lewis

ISR operations allow units to produce intelligence…necessary to make decisions.

—FM 3-0, Operations

Attaining Intelligence Synchronization

"Fight the enemy, not the plan."

So many commanders, instructors, and operations officers have repeated that line that it is now cliché. Since we all recognize the need, why do we keep repeating the line? While probably there are many reasons, our inability to maintain situational awareness and situational understanding is a major contributing factor. Situational awareness and situational understanding each have many facets; but from an intelligence standpoint, we often have difficulty in seeing the activities that reveal enemy intentions *in time for someone to do something about it.* In short, our intelligence, surveillance, and reconnaissance (ISR) effort is not synchronized with the remainder of the maneuver plan. Continuing advances in technology will provide the future Objective Force with great potential for increased ISR capabilities and effects, but we will not realize the full potential of these advances until we resolve our basic synchronization issues.

Units do not achieve intelligence synchronization because they divorce ISR planning from the decision-making process, viewing it as distinct from the remainder of the military decision-making process (MDMP). This results in ISR planning occurring late in the decision-making process. Worse, it is often developed solely by the S2 (or the assistant S2), resulting in an ISR plan that cannot support the scheme of maneuver. The plan is not designed to tell the commander what he needs to know in time for him to make a planned decision or trigger an enemy-related event.

The purpose of this article is to explore intelligence synchronization in relation to our decision-making process. We'll approach the subject from the standpoint of synchronization between ISR and the remainder of the maneuver plan; while I believe the synchronization issues explored here are valid regardless of the echelon in question or the technology in use, the focus in this article is on ISR at the maneuver battalion, task force, and squadron level, with their organic and routinely attached assets.

Why is ISR synchronization so important? What exactly is ISR anyway? To answer the first question, synchronization is the method for "achieving mass"—a principle of war, and the only characteristic that both offensive and defensive operations have in common.[1] Officially, FM 3-0, *Operations*, states that synchronization is "arranging activities in time, space, and purpose to mass maximum combat power at the decisive place and time." ISR is one of those "activities" alluded to above. ISR synchronization, then, is the consolidation correlation of the timing, disposition, and purpose of our ISR effort with the close combat aspects of our plan.

Because ISR is the underpinning of successful maneuver, it serves as the basis for answering priority intelligence requirements (PIRs), thereby supporting decisions and triggering friendly actions. The goal of ISR synchronization is putting the right observer in the right place and looking at the right named area of interest (NAI) at the right time. The purpose of ISR synchronization is to identify the enemy's adopted course of action (COA) early enough for the friendly commander to make some decision (such as adjusting the base plan or executing a branch plan) or to trigger some friendly action (like beginning preparatory fires or executing a counterattack option).

Our doctrine is not directive in how a staff should plan ISR operations. However, it does imply an overall framework for accomplishing the task, and places explicit responsibility for ISR planning on the S3.[2] The S2 initiates the process and is a primary contributor to the effort, and every staff member has a role; but the S3, as the echelon operations officer, is the right person to ensure integration. It should be fundamental to his plan.

ISR planning is embedded both in the intelligence preparation of the battlefield (IPB) process and in the MDMP, although it is often overlooked. While synchronization is a continuous process, there are at least four times during the planning process when the S2 and S3 should specifically consider aspects of ISR synchronization. Attaining ISR synchronization starts during mission analysis. Step nine of mission analysis, "development of the initial reconnaissance annex," corresponds with the fourth step in the IPB process, "determine threat COAs." Determining threat COAs has an often-overlooked sub-step of "identify initial collection requirements." Our doctrine writers are telling us something here. One of the final steps of mission analysis corresponds with the final task in IPB. By the time initial mission analysis and initial IPB are complete, someone on the staff should have a good idea of our initial collection requirements. That someone should be the S2; he has completed three steps of IPB, and has

nearly completed the fourth. He should know his intelligence gaps, and should have an idea of what activities and areas will fill those gaps. Staff integration is important here; by now, the S3 has a thorough understanding of his mission, tasks, and purposes. If he is close to the commander, he should have some idea of how the unit will fight—a draft scheme of maneuver, even if it's just in his head. These factors are important. The closer the S2 and S3 are to a common vision of the friendly operation, the better they can focus the initial effort. For example, will the concept of the operation require reconnaissance-push or reconnaissance-pull?

After talking with the S3 and considering the pertinent information, the S2 should propose an initial ISR COA from which the S3 can develop the initial ISR annex.[3] The purpose of the initial ISR annex is to allow our reconnaissance, surveillance, and target acquisition assets to begin troop-leading procedures so that they start infiltration quickly. This not only supports the fundamental of continuous reconnaissance but also gives leaders options for more deliberate infiltration techniques—dismounted, for example. It is important to note that the initial annex must contain all the information required for ISR assets to begin infiltration. FM 101-5 states that this includes—

- ❑ The reconnaissance area of operations.
- ❑ Mission statement.
- ❑ Task organization.
- ❑ PIRs and information requirements (IRs). (At this point, we should have IR only; it is unlikely the commander will have designated PIRs this early in the process.)
- ❑ Line of departure times.
- ❑ Initial NAIs.
- ❑ Routes and passage of lines instructions.
- ❑ Communication and logistic support measures.
- ❑ Fire support measures.
- ❑ Casualty evacuation information.

To the above, I would add any information, known or templated, on the enemy's counterreconnaissance effort, including known enemy and friendly obstacles.

Note the wide variety of information needed. This requires close coordination between the S2, S3, and many other members of the staff. This is a substantial effort, but worth the cost in time. Once ISR assets have started infiltration, they will begin to fill in intelligence gaps, and can provide information that will support the rest of the planning process.

The second time when the staff must consider aspects of ISR is during step four of COA development, "develop the scheme of maneuver." Here, among many other things, the staff works to integrate its available resources into an effective force arrayal. For ISR, the focus is on the relationship of ISR assets to other friendly forces, the terrain, and the enemy. We must have a clear understanding of the purpose of each asset (calling for fires or providing obstacle intelligence are two examples), and we must plan to position the assets on the terrain that allows them to fulfill their purpose.

Normally, suspected enemy locations or activities will drive our terrain considerations, which the S2 and S3 should designate as NAIs or target areas of interest (TAIs). TERRABASE, or some other automated terrain tool, can help here; an effective technique is to plot a 360° line-of-sight fan from the NAI. This allows for rapid identification of all potential observation post (OP) locations. Based on the potential OPs and desired effect in the area of interest (AOI), the S2 must then consider the survivability, mobility, communication, and limited visibility capability of all available assets. He can then recommend which asset is best suited to support the NAI—engineers, fire support team (FIST), scouts, air defense teams, maneuver elements, and ground surveillance radar all have different strengths and weaknesses that the staff should examine in order to achieve full effectiveness.

The staff must also consider how mixing, redundancy, and cueing should be used to offset shortcomings in different collection systems.[4]

- ❑ *Mixing* is using two or more different systems to collect on the same intelligence requirement. At the task force level, this could mean using both a scout and a FIST to observe linked NAIs and TAIs to meet the technical and tactical triggers for planned indirect fires.
- ❑ *Redundancy* is using two or more like assets to collect on the same intelligence requirement. A simple example here is the use of primary and alternate scout OPs to observe the same NAI.
- ❑ *Cueing* is using one or more intelligence types or systems to direct follow-on collection by other assets. At the squadron level, this could be an OH-58D conducting "target handoff" with a ground cavalry troop; at the task force level, a ground surveillance radar (GSR) alerting a scout to the presence of moving target indicators entering an NAI. Regardless of the specific assets available, the staff must consider how these systems complement each other and how they should be used to increase situational awareness.

The third point in the MDMP when staffs have an opportunity to incorporate ISR planning is step eight of COA analysis, "wargame the battle and assess the results." Because COA analysis is iterative, using the action-reaction-counteraction process, it is the logical point to consider the timing of our ISR activities. There are two important aspects of timing:

- ❑ First, there is the maneuver of our assets throughout the battlefield; the time required to move

and achieve positioning that allows surveillance or reconnaissance. As mentioned before, earlier is almost always better in that it gives subordinate leaders more time to maneuver their assets and take advantage of the synergistic effects of mixing, redundancy, and cueing—all of which can increase the chances of a successful infiltration of an enemy's defensive area.

- Second, the staff should consider its relationship to anticipated decisions. The S2's event template is important here, and it is an integral product for COA analysis.[5] We all understand that ISR assets must be positioned to observe NAIs; what we sometimes fail to consider is the importance of proper NAI placement in relation to time.

To support a complex maneuver associated with a PIR and decision point (DP) (such as the execution of a branch plan), the NAI will have to be placed far enough "forward" to allow identification of the indicator, transmission time and processing by the commander and staff (including the recognition that a decision needs to be made), transmission of the order to affected elements, and then maneuver of those elements. In other words, the NAI will probably need to be "before" the DP. NAI placement is just as important in planning triggers. For example, indirect fire planning might call for two AOIs: an NAI as a tactical trigger and a TAI that by definition should cover both the technical trigger and the engagement area.[6]

Wargaming is also the point were the S2 should identify and record latest time information is of value (LTIOVs). LTIOVs probably should not be a set hour but rather should be tied to a maneuver event on the ground; for example, "before Alpha Company crosses Phase Line Earl." LTIOVs will help you later with managing the whole ISR process. The implication of these timing requirements is that you cannot solidify your ISR plan until wargaming is complete. Only then will you have an understanding of the friendly planned decisions, with their associated PIRs, NAIs, and indicators.

Finally, the S2 must develop the indicators, IRs, and specific instructions to support analysis and help focus what is often a limited number of ISR assets. An effective technique is to consider indicators and specific information requirements (SIRs) as analytical tools, while specific orders or requests (SORs) and a consolidated ISR overlay are execution tools. Your ISR assets are unlikely to have the time to correlate each observation against lists of indicators and SIRs. Even if they were to have the time, it is unlikely you would want them to—they see a relatively small portion of the battlefield (although with great clarity), while the staff at the tactical operations center (TOC) has awareness of the larger battlespace. ISR assets at the task force and squadron level need good execution tools, with good SORs above any other staff product. A consolidated ISR overlay, situation templates depicting enemy security operations, and PIRs are next in order of importance. The staff, clearly in the best position to attain overall situational understanding, need analytical products–PIRs, indicators, SIRs, the event template, and event matrix.

Maintaining Intelligence Synchronization

Early planning, combined with event templating and wargaming, allows units to attain intelligence synchronization. Maintaining synchronization can only occur through active management of the effort. The staff (primarily the S2, S3, and executive officer) must constantly evaluate reporting to determine how well the system is satisfying intelligence requirements, and then adjust the ISR plan to optimize the collection effort as the friendly and enemy situation changes.[7] These changes in the situation can require changes to the ISR plan. Not every asset will have a successful infiltration. While most S2s track asset locations carefully, few actively manage the process; for example, directing that an asset reposition to cover an NAI for which the original observer has been destroyed. (This requires clear understanding throughout the unit on who has the authority to direct movement of ISR assets.) Answering a PIR or IR may also drive changes to the ISR plan. Likewise, changes in the enemy situation or unanticipated enemy actions may demand adjustments to the ISR plan. For example, a friendly higher echelon may have interdicted the enemy formation we expected to see.

Whatever the case, someone in the command post (CP) must manage the process. An effective technique is to think of NAIs as "active" or "inactive." An active NAI is one that has an observer in place and in communication with the CP, with a no-fire area around the observer. If the NAI supports a DP, it should not be considered fully active until an alternate observer is also in place and communicating. (Understand that this is just a technique, not doctrine.) The fact that a decision-linked NAI is active may need to be designated as a friendly force information requirement by the commander. Well-defined priority NAIs by phase will help in the overall management effort.

ISR—The Keys

This article has explored intelligence synchronization in relation to the MDMP. I have tried to show that units have difficulty achieving intelligence synchronization due to the separation of ISR planning from the remainder of the maneuver plan, and that staffs can overcome this shortcoming through an emphasis on key areas, starting with the MDMP itself.

Units cannot synchronize ISR without conducting proper IPB and staff planning. By that, I mean that the S2 must "sell" multiple enemy COAs to the commander. The staff must build a plan to account for all the COAs, and the S2, S3, and remainder of the staff must develop an ISR plan capable of initiating a friendly branch plan. To have the greatest chance of success, ISR assets need an early start. To have the greatest relevance, ISR assets should be focused as a result of the S2's intelligence gaps and the S3's knowledge of friendly mission and intent. Staffs can help their ISR assets by developing NAIs as a function of time, space, and purpose, and then assigning asset coverage based on capability and compatibility. SORs are the best tools your reconnaissance, intelligence, surveillance, and target acquisition assets have for understanding what's really important. Finally, the staff must manage the process to account for changes in the situation.

Endnotes

1. See "Achieving Mass at the Decisive Point," by Chris Rogers, currently pending publication in *Armor Magazine*.
2. FM 3-90, *Tactics*, page 13-14.
3. FM 101-5, *Staff Organizations and Operations*, page 5-8.
4. FM 3-90, *Tactics*, page 13-16.
5. FM 34-130, *Intelligence Preparation of the Battlefield*, page 1-10.
6. While "engagement area" normally implies the use of multiple weapon system types, I use the term here to help distinguish among the three definite areas involved in planning indirect fires: the tactical trigger, the technical trigger, and the area where the rounds impact.
7. FM 34-2, *Collection Management and Synchronization Planning*.

Know Your Equipment

TYPE 96 MAIN BATTLE TANK, People's Republic of China

Production of the Type 96 main battle tank probably began in 1997, few being available for the PRC's 50th anniversary parade in 1 October 1999 (photo). The People's Liberation Army allegedly ordered 100 type 90 II MBTs without advanced fire control systems. The tank has been previously indentified as the Type 96, 98 or 99, with the export variant know as Types 90 and 90 II.

ARMAMENT

- 125-mm autoloading, smoothbore gun (fires high-explosive fragmentation (HE-Frag), HE antitank (HEAT), and armor-piercing fin-stabilized discarding sabot (APFSDS)
- 12.7x 108-mm Type 54, roof-mounted antiaircraft (AA) machine gun (probably 250 rounds)
- 7.62x 54-mm R Type 59T, coaxially mounted machine gun (probably 2000 rounds)

PROTECTION

The design incorporates modular composite armor. Some photos have shown models with explosive reactive armor (ERA), but the tanks seen in the anniversary parade had no ERA.

PROPULSION

- 1200-hp, 8-cylinder turbocharged diesel allows a maximum road speed of 37 mph (59 kph)

ADVANCEMENTS

The Type 96 incorporates stabilized turret, slaved targeting sight and gun, integrated passive thermal-imaging, and laser rangefinder. The vastly improved targeting systems, crosswind sensor, and increased mobility allow the Type 96 to engage moving targets day or night with an 80-percent success rate for the first shot.

By Mr. John Oakley, 304th MI BN, DSN 821-7781.

Modified Intelligence Synchronization Matrix—
A Technique for Brigade Combat Team Operations

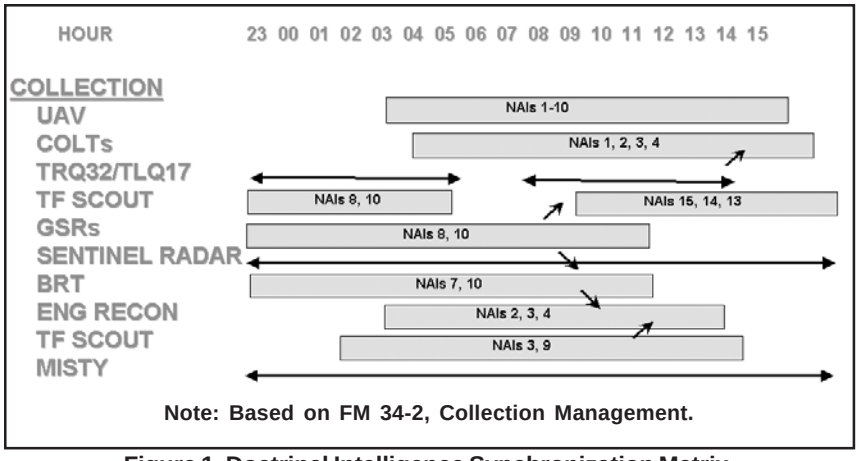
by Captain Tod A. Langley

At the National Training Center (NTC), I have observed a constant downward trend in our Branch's ability to support the warfighter at the brigade level. Reviewing the quarterly trends and executive summaries that my predecessors published, it is apparent that this is not new; however, this is not to say that Military Intelligence professionals who deploy to the NTC are not improving in many areas.

I formerly believed that the primary challenge for MI company commanders was to ensure **asset integration**. The MI company commanders who deploy to NTC today are much more involved and there is a positive, upward trend that shows we are ensuring integration of all of our assets into the brigade's scheme of support. To provide maximum support, however, we must ensure **asset synchronization**. It is not enough to say you discussed every system during the wargame or gave them specific tasks and purposes within the MI company operations order (OPORD). To be effective, MI company commanders must ensure that their schemes of support nest into the brigade combat team's scheme of maneuver. Our failure as a Branch to do this efficiently has resulted in a negative trend in intelligence synchronization, which affects all other aspects of combat operations.

Collection Management and the ISM

In **FM 34-2**, **Collection Management**, the responsibility for ensuring use of assets in a way that makes certain we satisfy information requirements falls on the collection manager (CM). According to **FM 34-2**, the CM is the key to intelligence synchronization. During the wargaming effort, the CM looks at each potential course of action (COA) and determines how to satisfy the information requirements (IR) derived there from with the available assets. The S2 determines the IR at the brigade level. Typically, no one has the established responsibility of collection management within a brigade combat team (BCT). The person in the best position to take on this responsibility is either the MI company commander or the analysis and control team chief (ACT). Most commanders and ACT chiefs that participate in the brigade wargame process come out scrambling to complete Annex T, Intelligence Electronic Warfare, (FM 5-0, annexes B and L) as well as the company OPORD. The doctrinally based tool available that allows MI planners to organize their notes from the wargame is the intelligence synchronization matrix (ISM). With a blank ISM available, the CM can track each asset's task and purpose, assigned named area of interest (NAI), and collection timeline. Once the wargame is complete and the BCT has selected a COA, the ISM serves as the basis for both the Annex T and the MI company OPORD. However, there is much more value added from a modified ISM than what **FM 34-2** describes.



Note: Based on FM 34-2, Collection Management.

Figure 1. Doctrinal Intelligence Synchronization Matrix.

An ISM must comprise the following required data:

- ❑ Time.
- ❑ Decision points.
- ❑ Assets.
- ❑ NAIs assigned coverage.
- ❑ Cueing requirements.
- ❑ Latest time information is of value (LTIOV) (see Figure 1).

Putting the brigade commander's crucial decision points (DPs) on the matrix reflects determination of an intelligence requirement (IR). By looking down the chart at the expected time for making a decision, the CM is able to verify that each asset is attempting to answer an IR tied to the commander's DP. This is a simple tool to ensure overall synchronization; however, it does not include the fidelity necessary to ensure MI assets achieve the necessary objectives.

A Modified ISM

In a modified ISM created during the wargame, the MI company commander should be able to provide the following information to his subordinates:

- ❑ BCT scheme of maneuver.
- ❑ Commander's DPs.
- ❑ Most likely Enemy COA.
- ❑ Focus of fires (including close air support (CAS)).
- ❑ Asset location and assigned NAI(s).
- ❑ Collection focus by intelligence discipline and analytical focus.

Your imagination is the only limitation to the data that you put into the ISM

to make it an efficient tool for your company (see Figures 2 and 3).

If you look at each significant activity within the BCT scheme of maneuver, you should be able to verify the focus of collection assets on support to the brigade. You should also be able to direct your analysts to ensure they are working to answer the IR in a timely manner. When the staff creates this document during the wargame, they have already developed the majority of the MI company's scheme of support. This document can then become part of Annex T and the company OPORD.

An Example of Using the ISM

A specific example appears on the right side of Figure 2. The general scheme of maneuver calls for the brigade's main effort to cross the LD at 0500 hours. The commander expects the main effort to conduct a breach and attack to destroy enemy at the objective by 0700 hours. By 0800 hours, the brigade S2 has estimated that the enemy will commit his local reserves and shortly after that his combined arms reserve (CAR). During this critical time of consolidation and reorganization on the objective, the commander must decide whether to commit the supporting effort task force to continue the fight against the remaining enemy in the main battle area (MBA) or block the attack of the CAR. With this information, the MI company commander should establish a task, purpose, and collection focus for every asset ensuring priority goes to answering priority information requirements linked to the brigade commander's second DP.

The MI company commander's challenge is to find the CAR before its commitment or as it begins movement. Nested in his support plan, the commander has assigned NAI 9 for GSR Team 2 focused on detecting movement of reinforcements toward the MBA. During this phase of the operation, NAI 9 is a secondary route that the CAR might use, so the team is to report the movement of any wheeled or tracked vehicles moving through the NAI toward friendly forces. The S2 focused the TRQ-32 and TLQ-17 on command and control nets that indicate movement of forces toward the MBA. Additionally, the TLQ-17 is to deny the enemy the ability to call for reinforcements or coordinate a counterattack focusing their antennas on NAI 7. The ISM indicates that non-lethal fires

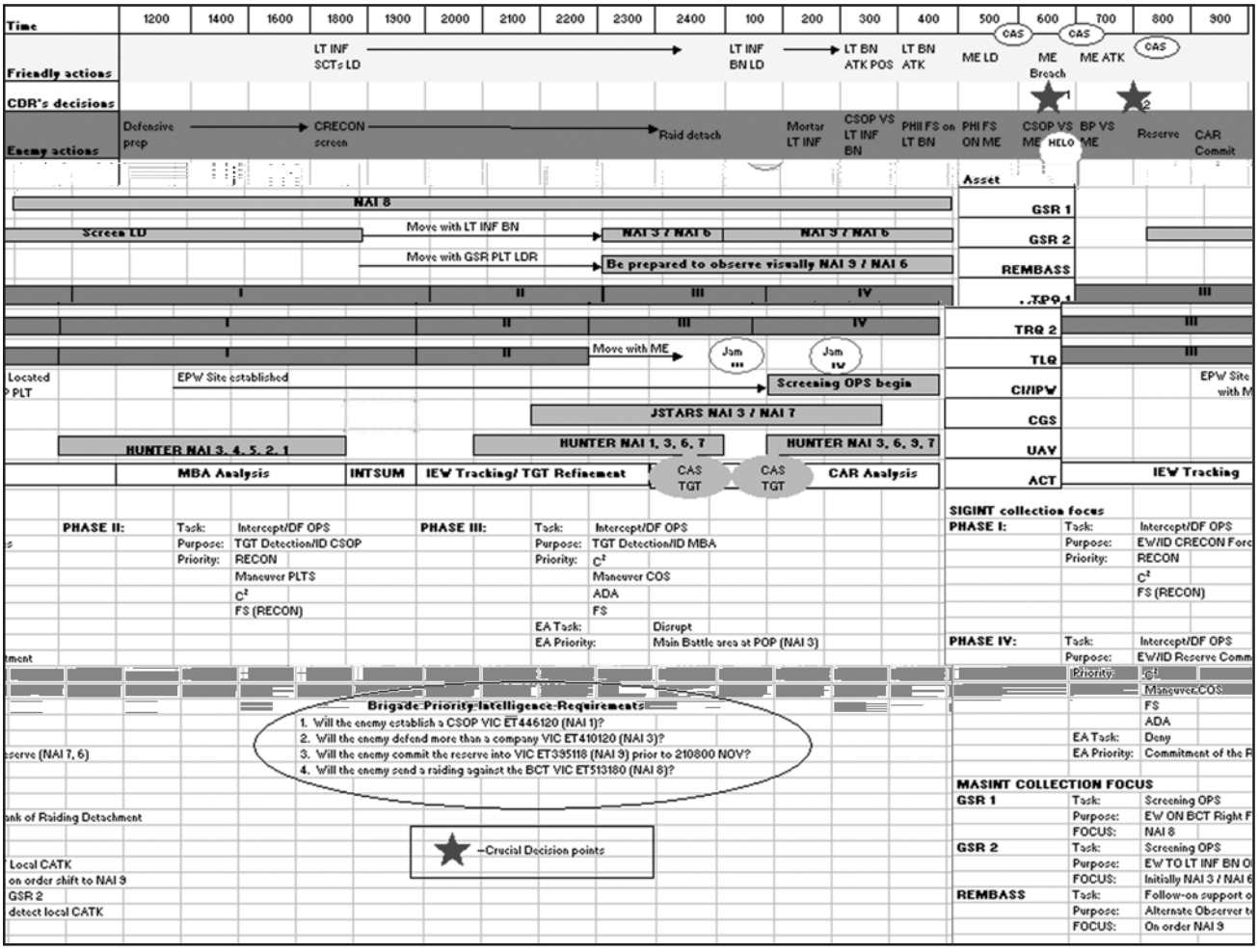


Figure 2. Modified Intelligence Synchronization Matrix.

will be in conjunction with the CAS planned to be on station at the same time as the commitment of the CAR. Joint STARS focus within the Common Ground Station (CGS) is on NAIs 3 and 7 (the most likely route of the CAR toward the MBA). To ensure the brigade has redundant early warning, the UAV concentrates on the CAR in NAI 7. Finally, the ACT's focus is on identifying the location of the CAR, when it will move, and where it will attack. Through the use of the modified ISM, the MI company commander has ensured that he has focused his assets on finding the CAR, the analysts are providing intelligence that will help the commander make a critical decision, and the synchronization of non-lethal fires with lethal fires to ensure maximum effect.

Final Thoughts

The usefulness of the ISM is not just in its ability to synchronize assets during the planning process; the modified ISM should also be useful during the execution of intelligence operations. Each subordinate asset manager or platoon leader should have a copy of the ISM to verify that platforms and soldiers are accomplishing their major tasks and purposes for each phase of the operation. The ACT should also have a copy of the ISM to ensure that their analysis is predictive rather than just reporting the current enemy situation. Finally, the ACT chief and MI company commander should use the ISM to verify that their scheme of support is valid relative to the current friendly situation. Through planning and execution, a modified ISM is a useful tool for MI companies supporting the warfighter. The ISM also allows the brigade commander to see how his ISR assets are working to provide him with the information he needs to make the right decision at the right time.

Captain Tod Langley is currently the Senior Military Intelligence Company Trainer at the NTC. His previous assignments include Commander, D Troop (Surveillance), 1st Reconnaissance Surveillance Target Acquisition Squadron, 14th Cavalry Regiment (the Initial BCT), and Commander, A Company, 125th MI Battalion. CPT Langley earned a Bachelor of Arts degree in Political Science from Purdue University. Readers may contact the author via E-mail at bronco75@irwin.army.mil and telephonically at (760) 380-4443 or DSN 470-4443.

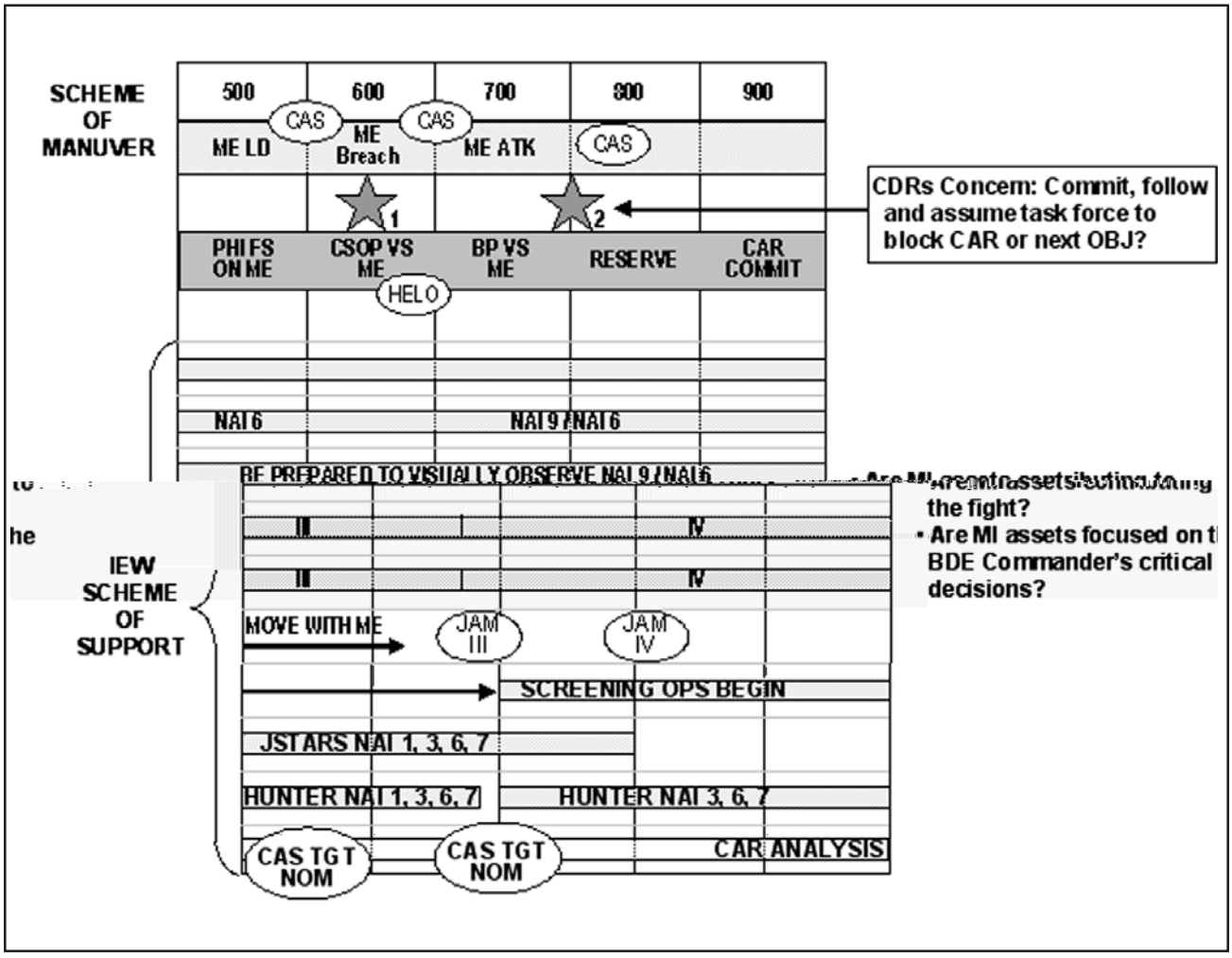


Figure 3. Explanation of Important Areas in Figure 2.

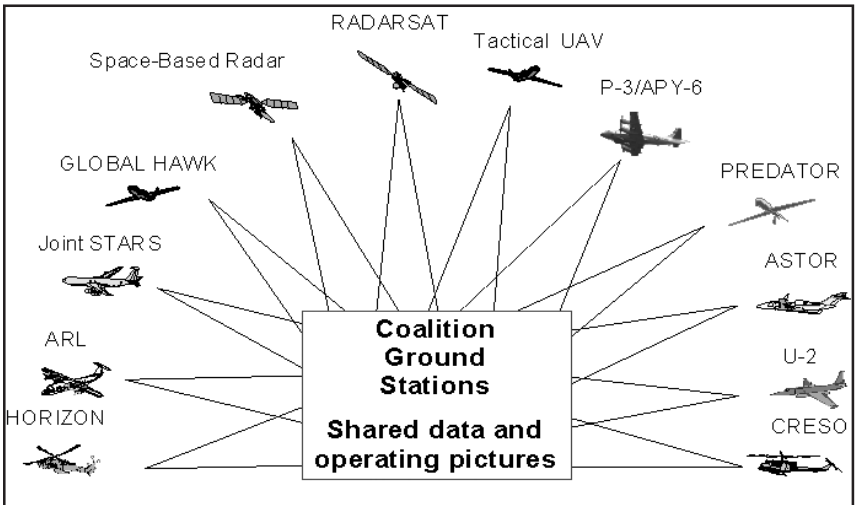
Coalition Aerial Surveillance and Reconnaissance

The CAESAR Project

by Colonel Stephen J. Bond

Coalition Aerial Surveillance and Reconnaissance or CAESAR is an intelligence, surveillance, and reconnaissance (ISR) interoperability project. Seven nations and the North Atlantic Treaty Organization (NATO) Consultation, Command and Control Agency (NC3A) are working the project to integrate, exploit, and share data from ground moving target indicator (MTI) and synthetic aperture radar (SAR) imagery surveillance platforms to the associated coalition ground stations (see Figure 1). The seven participating nations, all NATO members, include the United States, Canada, France, Germany, Italy, Norway, and the United Kingdom. Supreme Headquarters, Allied Powers Europe (SHAPE) has endorsed the project.

The CAESAR Project will maximize the efficient and effective use of high-demand, low-density surveillance platforms and ground stations among the coalition member nations. The Project's goals are to establish interoperability through technical interface, architectural design, and operational standards for employing surveillance platforms and ground stations to support the U.S. and other coalition ground, air, and maritime commanders (see Figure 2). For the United States, CAESAR is an Office of the Secretary of Defense (OSD) Advanced Concept Technology Demonstration (ACTD). The Air Force is the lead Service for the demonstration and provides the technical management for the U.S. participants in the project through the Joint Surveillance Target Attack Radar System (Joint STARS) Program Office, Electronic Systems Command, at Hanscom Air Force Base, Massachusetts. The U.S. Army Intelligence Center (USAIC) provides operational management for the Project. Representatives from all the Services participate with the representatives from the other member nations in coalition working groups. International memorandums of agreement and security arrangements, signed by the participating nations, establish and govern the Project.



The goal of CAESAR is to achieve operational and technical interoperability among ground MTI and SAR assets.

Figure 1. CAESAR Goal.

Project Objectives

The specific objectives for the Project are to—

- Produce interoperable concepts of operations (CONOPs) and tactics, techniques, and procedures (TTP) for use by coalition, joint, ground, air, and maritime commanders for the employment of multinational ground MTI and SAR assets.
- Develop or improve existing technologies to achieve technical interoperability among the participating surveillance platforms and sensors. This includes interchange formats, registration, and exploitation algorithms,

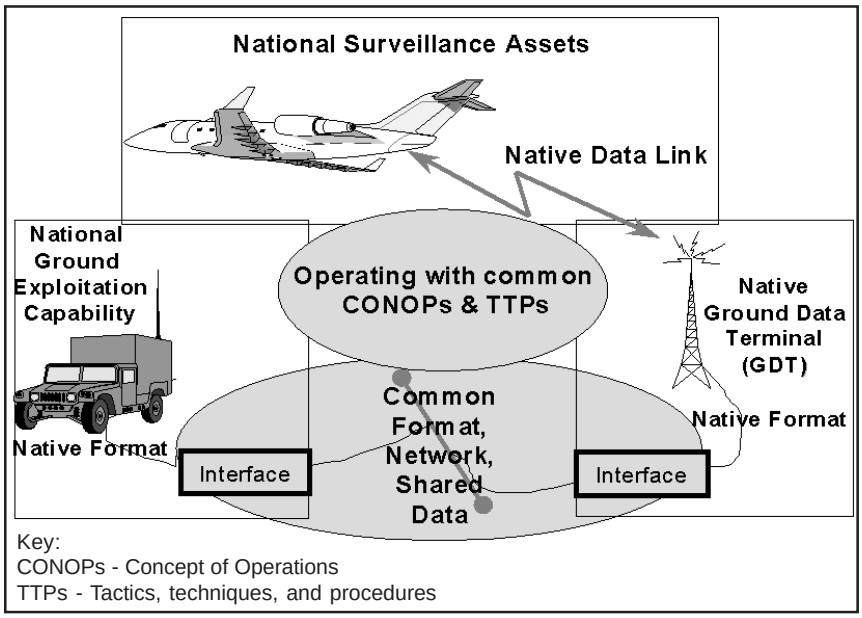


Figure 2. CAESAR Interoperability.

mission planning and tasking tools, and architectures for networked and distributed processing (see Figure 3.). Each ground station is capable of receiving and sharing data in near-real time to provide a common view of the battlefield.

- Conduct annual exercises to evaluate program technology and operational concepts. Integrate these technical and operational capabilities within the supporting commands and architectures of the United States, other coalition nations, and NATO.

Participating Systems

The national platforms participating in CAESAR appear in Figure 4 and a listing of all participants and assets is in Figure 5. The coalition systems participating in the CAESAR Project include the following:

- Canadian Radar Satellite (RADARSAT) system and associated ground stations. RADARSAT 1 is an operational commercial satellite providing 7- to 100-meters resolution SAR imagery, depending on the radar beam mode and incidence angle. RADARSAT 2 is currently in development; when operational, it will provide radar images at better than 3-meter resolution and have an experimental ground MTI capability.
- French *Helicoptere d'Observation Radar et d' Investigation sur Zone* or HORIZON system and associated ground stations. The targeting radar produces ground MTI and its platform is a Eurocopter Cougar AS-532 UL helicopter.
- Developmental German inter- operable imagery workstation to display and exploit ground MTI and SAR information.
- Italian CRESO (*Complesso Radar Eliportato per la Sorveglianza)* and associated ground stations. Installed aboard an Augusta Bell AB-412 helicopter, the battlefield surveillance radar provides ground MTI. The platform has an electronic warfare support measures (ESM) capability.
- Norwegian Mobile Tactical Operations Center (MTOC) for receiving and exploiting ground MTI and SAR information. Norway is further demonstrating and integrating MTI and SAR information within the Norwegian command, control, and information system.
- The United Kingdom is developing the ASTOR or Airborne Stand-Off Radar. This system's platform is a modified Global Express airframe carrying a multimode ground surveillance radar (GSR) capable of both ground MTI and SAR imagery.

The standards under development for interoperability through CAESAR will apply to all U.S. platforms and ground station systems providing, receiving, or processing MTI and SAR data. This includes current and future Army systems, including Airborne Reconnaissance Low (ARL), Tactical Unmanned Aerial Vehicle (TUAV), Aerial Common Sensor

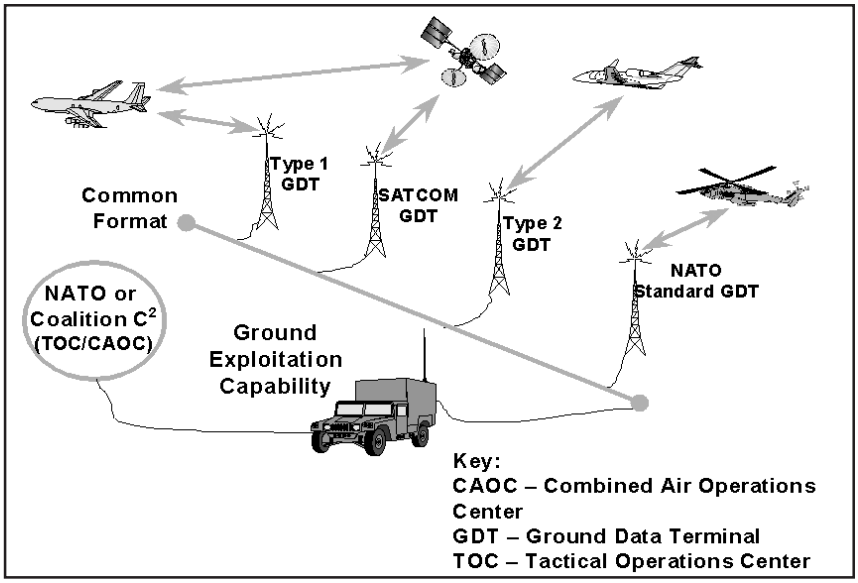
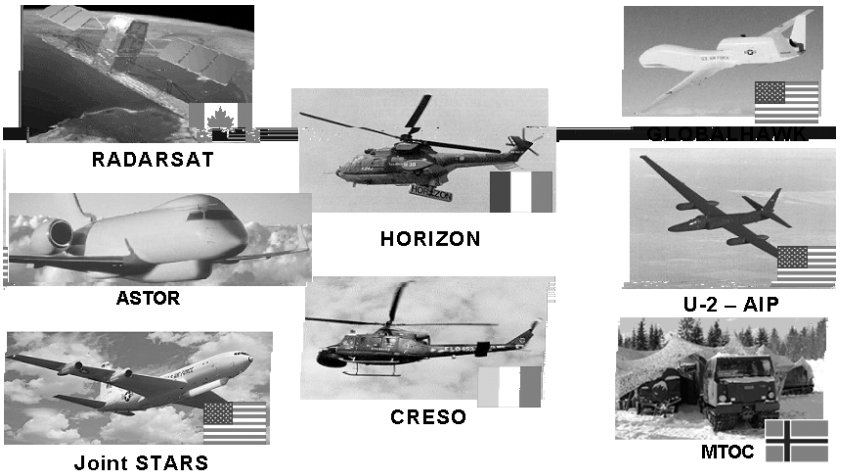


Figure 3. Interoperability Architecture.



The participating surveillance platforms are shown above; additional participants in the CAESAR project include Airborne Reconnaissance Low and the Predator UAV.

Figure 4. Participating Platforms in the CAESAR Project.

(ACS), and the Distributed Common Ground System-Army (DCGS-A). U.S. systems currently participating in the CAESAR Project include—

- E-8C Joint Surveillance Target Attack Radar System (Joint STARS).
- U-2 Advanced Synthetic Airborne Radar System (ASARS) Improvement Program (AIP).
- RQ-4 Global Hawk UAV.
- RQ-1A/B Predator UAV.
- Common Ground Station (CGS) and the Joint Services Workstation (JSWS).
- The experimental Moving Target Indicator Exploitation (MTIX) Workstation.

Project Background

The CAESAR Project has only formally existed since 2000, but efforts have been underway since 1995 to work issues associated with interoperability of NATO member nations' ISR assets. The work began through the efforts of NC3A, located at The Hague, Netherlands. In 1997, France hosted six of the current CAESAR nations in the Paris Interoperability Experiment. At this experiment, one Joint STARS aircraft and a forerunner to the CGS (the Joint STARS Ground Station Module), and two French HORIZON helicopters with two HORIZON ground stations gathered and exchanged data on ground vehicle movement. Both the U.S. Joint STARS and French HORIZON successfully provided surveillance of ground and helicopter traffic in Kosovo in Operation ALLIED FORCE in 1999. However, this operation specifically pointed the need to establish greater interoperability and integration of ISR assets to support coalition military operations.

Since then, CAESAR-related platforms, simulators, ground stations, and crews have participated in and further demonstrated interoperability in three SHAPE-sponsored exercises in Europe. These exercises were:

- JOINT PROJECT OPTIC WINDMILL/CLEAN HUNTER 1999, an Allied Forces North (AFNORTH) theater missile defense (TMD) exercise.
- CLEAN HUNTER 2001, an AFNORTH/AIRNORTH TMD exercise.
- STRONG RESOLVE 2002, an AFNORTH/Joint Command North exercise with CAESAR assets primarily supporting the land component commanders in Norway.

As a result of these exercises and other laboratory simulation tests, technical and architectural interoperability have become a reality. SHAPE- and coalition-endorsed CONOPs and TTP exist today. These documents will become a part of U.S. joint and Service doctrine through on-going coordination with U.S. Joint Forces Command; the multiService Air, Land, and Sea Application (ALSA) Center at Langley, Virginia; Headquarters, U.S. Army Training and Doctrine Command (TRADOC) and USAIC; and the U.S. Air Forces' Aerospace Command and Control, Intelligence, Surveillance, and Reconnaissance Center (A2CISRC) also at Langley, Virginia.

Canada
Space-based radar ground MTI

France
HORIZON and ground stations

Germany
Interoperable exploitation work station

Italy
CRESO and ground stations

Nc3a / shape
Alliance ground surveillance (AGS) simulations

Norway
Mobile Tactical Operations Center

United Kingdom
ASTOR and Ground Stations

United States
Platforms: Joint STARS, U-2, ASARS, Predator, and Global Hawk
Ground Stations: Common Ground Station (CGS)/Joint Services Workstation (JSWS), Moving Target Indicator Exploitation (MTIX) Workstation

Figure 5. CAESAR Participants and Systems for Integration.

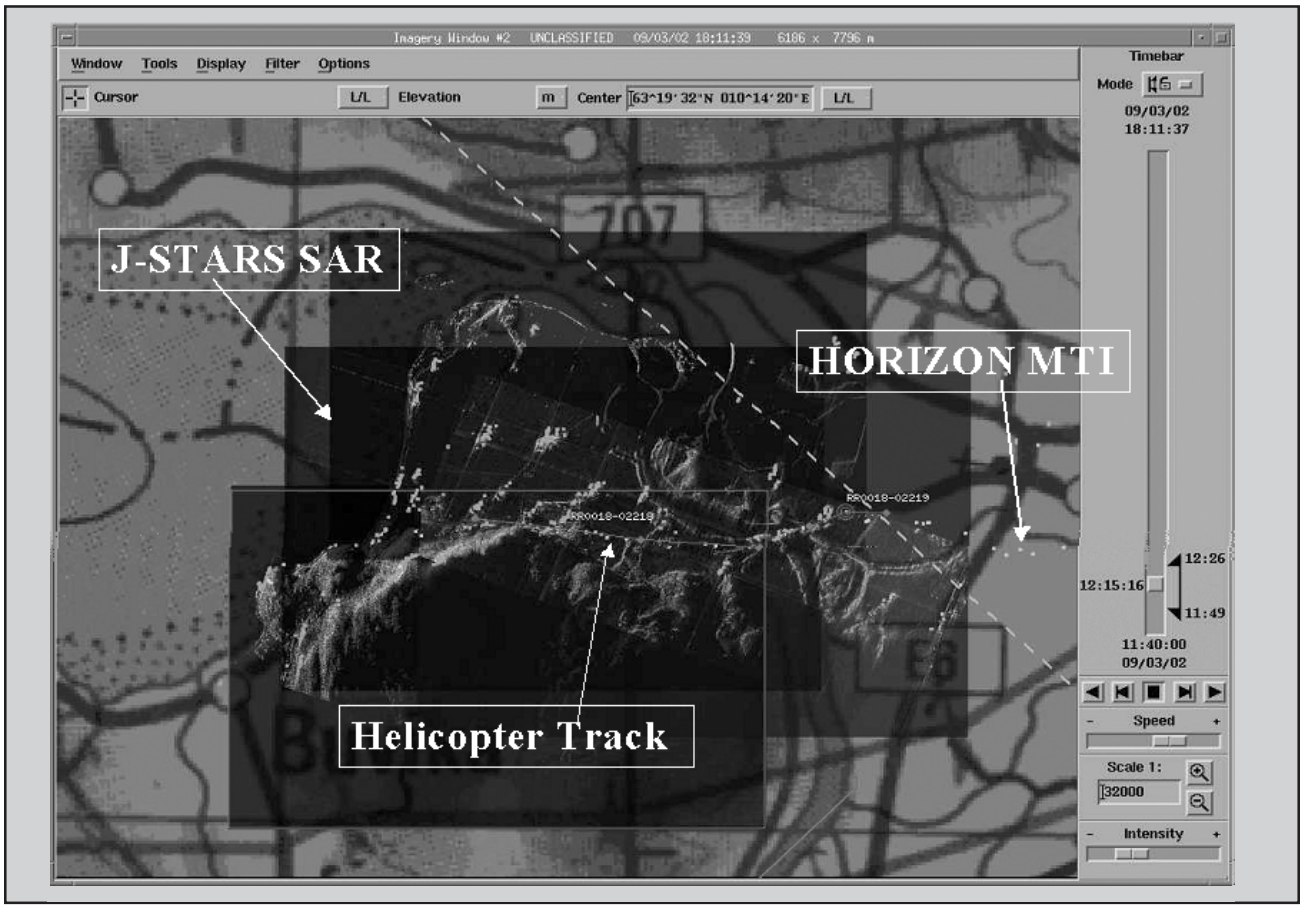


Figure 6. JSWS Displaying Joint STARS SAR and HORIZON MTI.

The CAESAR Project has received numerous awards among the member nations. These include selection in the United States as the Department of Defense's "ACTD Operational Manager of the Year" award for 2001, and the "ACTD Technical Manager of the Year" award for 2002.

The Project has funding as an ACTD through 2005, with supporting major exercises in planning for 2003 and 2004. There are quarterly meetings of the three coalition working groups: operations, technical interoperability, and architecture development. The Project also plans follow-on ACTD and project efforts.

Through the CAESAR Project, a unit with CGS will be able to receive information from the participating coalition surveillance platforms. Coalition commanders operating in the joint operations area with compatible workstations can also receive the same ISR information, nearly simultaneously, from the designated U.S. and other coalition surveillance platforms. When networked through tactical communications, the CGS operators also collaborate with other workstation operators in the coalition network of ground stations and retrieve information from a shared database.

Outlook

Widely considered a Department of Defense and SHAPE/NATO "success story," the CAESAR ACTD and Coalition Project uses the philosophy of practicing before crises; these on-going efforts will allow expanded situational awareness and enhanced capability for targeting. The Project efforts provide commanders from brigade to the operational levels with greater access to ISR assets and enable a sharing of data. These efforts will support future operations and ultimately allow U.S. and other coalition commanders to gain a common perspective and improved understanding of the battlefield. While there is still work to accomplish, efforts are well underway to achieve interoperability with these critical high-demand, low-density surveillance assets.

Colonel Steve Bond is the U.S. Army Training and Doctrine Command (TRADOC) Systems Manager for Joint STARS, Common Ground Station, and Joint Tactical Terminal; he was recently assigned responsibilities for the objective Distributed Common Ground System-Army (DCGS-A). He is also the U.S. Operational Manager for the CAESAR ACTD and chairs the Seven-Nation Coalition Operations Working Group. In recognition for the outstanding work performed by members of the CAESAR Project, Colonel Bond was selected the Department of Defense ACTD Operations Manager-of-the-Year in 2001. He holds a Master of Arts degree in History from the University of Kansas and is a graduate of the U.S. Army War College. Readers can reach him via E-mail at bonds@hua.army.mil.

HORIZON, The ng Tool of French Intelli Assets

by Lieutenant Colonel
Martin J. Renard, French Army

Due to the variety of intelligence assets available to a commander and the nature of terrain and weather conditions in the areas of operations (AOs), commanders and their staffs need to choose the appropriate assets, use them in the most efficient way (location and time), and not "waste" them. In fact, the number of assets available are important for a modern army, but there will never be enough of key intelligence, surveillance, and reconnaissance (ISR) to allow unneeded overlapping.

- **Builder team:** Eurocopter, Thomson-
- **First operational flight:** 1994, (although flew as demonstrator during G
- **In-service in the French Army:** D
- **Rotor diameter/ Length/ Height:**
- **Maximum weight during takeoff**
- **Fuel capacity:** 2,000 liters – 4 hour a
- **Power plant :** 2 Turboméca Malika 1
- **Maximum speed:** 275 km/h in transi
- **Range :** 1,000 km
- **Crew :** 2 pilots, 1 flight engineer, 1 ra
- **Special equipment :** Moving Target (Thomson-CSF), scanning a 20,000 km jamming resistance
- **Major operational capabilities :** of vehicles, boats and helicopters up to protected transmission of data to the gr exploitation. Air deployable ground sta
- **NATO interoperability :** Demonst the US J-STARS part of CAESAR mul
- **French Army inventory :** 4 helico

Figure 1. HORIZON Heliborne Radar Specifi

Some researchers are looking toward software to help with these collection management decisions, but some actual pieces of equipment can also provide a good overview of the AO and therefore assist commanders. The HORIZON[1] heliborne radar used in the French Army performs this function; moreover, combined with an unmanned aerial vehicle (UAV), it probably forms one of the best "teams" resourced by the Intelligence Implementation Center (INTEL IC)[2]. This system will soon become the true unifier of all French tactical intelligence assets. Figure 1 describes some of HORIZON's specifications.

The INTEL IC

In the new Fre
tion 2002, the t
assets are organ
Intelligence Brig
der the direct co
Forces Commar
de la force d'Acti
these assets d
tions, they are r
team tailored by
cated near the i
of the main unit

The INTEL IC f
sions: it develop
sions and manag
(see Figure 2).
around the liais

representing the different sensors and five cells that ensure the management of the intelligence collection assets. The liaison officers are the link between the INTEL IC and the sensors: they turn the collection orders (requests for information) into technical orders for their detachment and exploit the collection results forwarded by their units to answer the requests. The five specialized cells are—

- Intelligence cell synthesizes the information received and steers the sensors.
- Operations cell commands the intelligence units' maneuver according to the evolution of the combined arms maneuver.
- Logistics cell organizes the support of the units in the field.
- Third-dimension cell (or airspace management cell) manages the integration of heliborne assets and UAVs.
- Signal and information systems (SIS) cell manages liaisons with the G6, the frequencies allotment, and the communication network's integration.

Role of the INTEL IC

The INTEL IC is therefore a real intelligence command center that co-

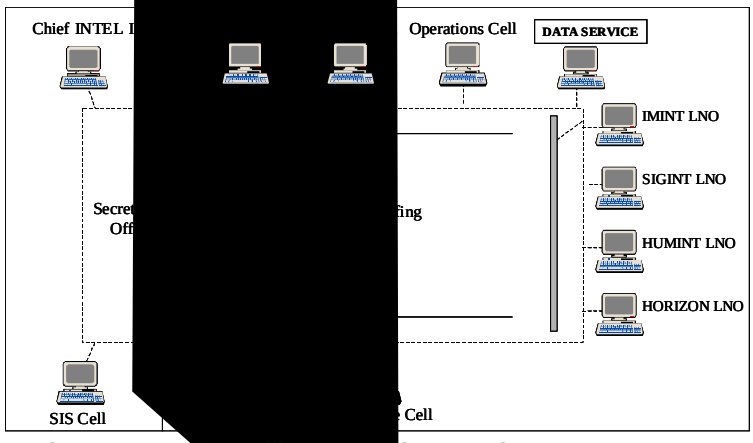


Figure 2. French Intelligence Implementation Center Structure.

ordinates the actions of the human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT) assets and provides necessary support. The INTEL IC's raison d'être is to profit from the complementary nature of the sensors to bring about synergy. The HUMINT, SIGINT, and IMINT assets have complementary qualities and limits. The aim is not only to compensate for the limitations of a sensor by the action of another asset but also to combine them to increase the value of the intelligence obtained. Hence, the INTEL IC has a dual role:

- *Ensure the assets are complementary:* Since the assets managed by the INTEL IC cover the entire spectrum (electromagnetic, visible, and infrared), few enemy elements can go undetected. Each sensor compensates by its abilities for the others' limitations. When the INTEL IC receives a mission from the G2, it chooses the sensor best suited to fulfill it, according to the nature of the target and terrain. It can also use a second sensor to confirm the information gathered by the first one.
- *Make the sensors work in synergy.* The aim is not only to fill in for each sensor's limitation with another sensor but also to maximize the resulting value while conserving the assets. The INTEL IC gives the missions to the collection assets, receives the information, and synthesizes it to produce intelligence of a greater value than the normal sum of the information. The INTEL IC structure allows one to confirm information quickly, and this avoids analytical errors linked to the exploitation of target data coming from a single sensor.

The INTEL IC turns the information received into varied and accurate intelligence in a short timeframe that can be useful to the maneuver unit.

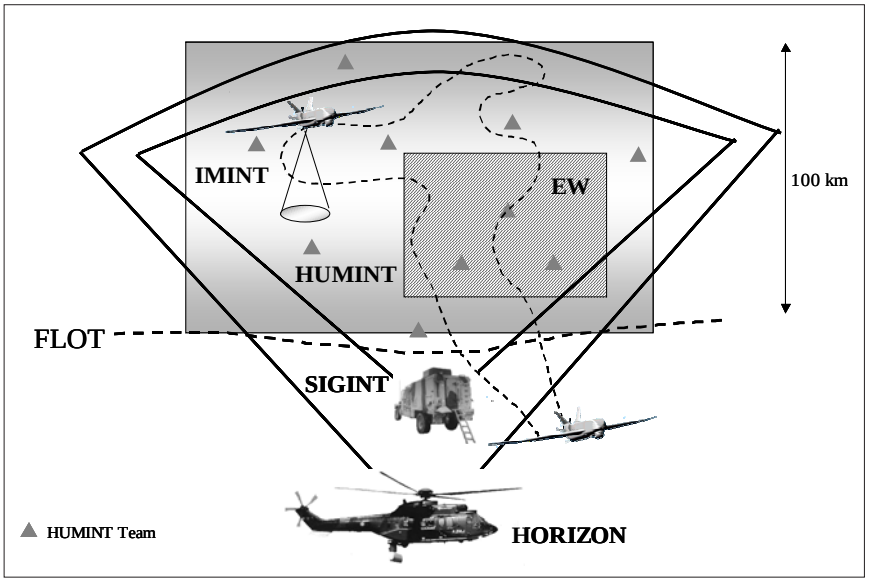


Figure 3. Complementarity of Intelligence Assets and Overall Coverage by HORIZON.

It uses the processed data within the intelligence cycle missions to create and steer the sensors. In this framework, HORIZON serves as a unifying tool, thanks to its collection and detection capabilities.

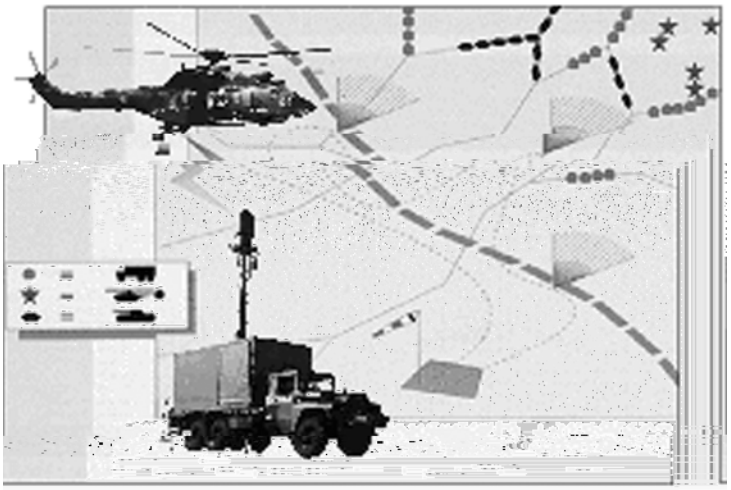
The following are examples of how INTEL IC assets fulfill the missions given by the G2. The INTEL IC steers each of the components according to their capabilities and limitations.

- SIGINT maintains passive and continual monitoring in an investigation area of 900 square miles to detect high-payoff targets like divisional headquarters. The covered zone is large, but redirecting collection toward a new area takes a long time.
- HUMINT allows continual intelligence on points of interest with great stealth, but the number of available teams is limited, the areas covered are not very large, and redirecting also takes time. One of HUMINT's strengths is that it discriminates military personnel and vehicles from civilian ones. This is an indispensable capability in times of crisis, when civilians and military often mingle.
- IMINT is a flexible tool that gains information quickly. The INTEL IC can rapidly redirect it (by dynamic retasking during flight), and it offers an extended range but covers a reduced area. Because of these characteristics, the images serve as either a way to gather initial intelligence or a way to confirm information.
- HORIZON, by its range and field of observation, covers the main unit's whole intelligence area of interest (AOI) while operating at a safe distance. These capabilities allow it to unify and steer the other sensors.

The INTEL IC tries to create the most accurate picture of the enemy maneuver by confirming information and reducing areas without coverage. To do this, it enhances the complementary nature of the collection assets, directs them, and plans their missions. Because of the way the INTEL IC is organized, it obtains a picture of the situation as seen by the sensors. (See Figure 3.)

HORIZON – Middle Altitude Long Endurance (MALE) UAV

In the area of sensor cooperation, the correlation between HORIZON and the MALE UAVs is specific because it plays a major role due to



Mission: Provide information regarding suspicious movements in critical areas

Figure 4. HORIZON's Operating Mode–Tension.

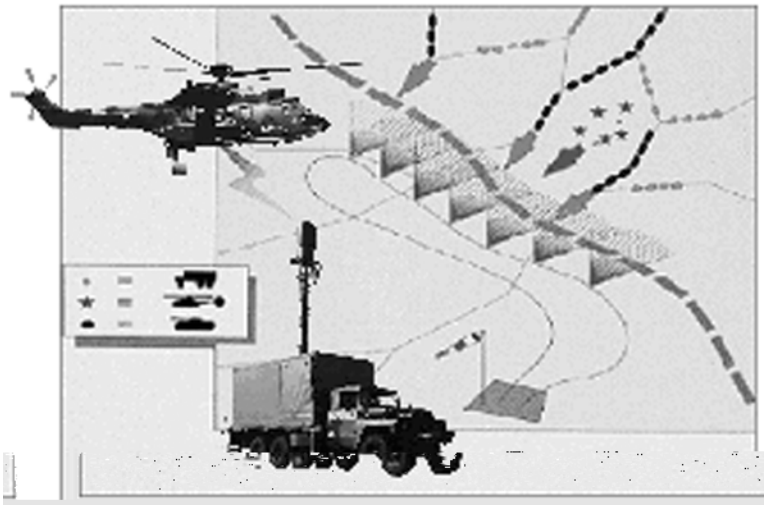
respective capabilities. Information gathered by HORIZON needs a confirmation that might come from any other sensor; however, the MALE UAV, with its range equivalency to HORIZON's and its speed and flexibility, constitutes the favored confirmation asset for information gathered by the heliborne radar.

HORIZON System Capacities. HORIZON can detect any moving vehicle with a speed equal to or more than 6 miles-per-hour from up to 90 miles away, and can cover a 125-mile front. It perceives objects that are moving away and those that are getting closer and displays, through specific symbols, the equipment type (land vehicle, helicopter). It is also able to extrapolate the future position of the detected targets. On the other hand, it cannot identify which specific piece of equipment it is detecting and cannot differentiate between civilian and military vehicles. The collected information needs verification.

In terms of mission capabilities, HORIZON benefits from the performance of its platform, the Cougar helicopter: it is highly reactive and can be retasked in flight. Its work altitude is 12,000 feet, it can reach 93 miles-per-hour during observation, and can fly for 3.5 hours. (Deploying two helicopters per ground station doubles this observation time.)

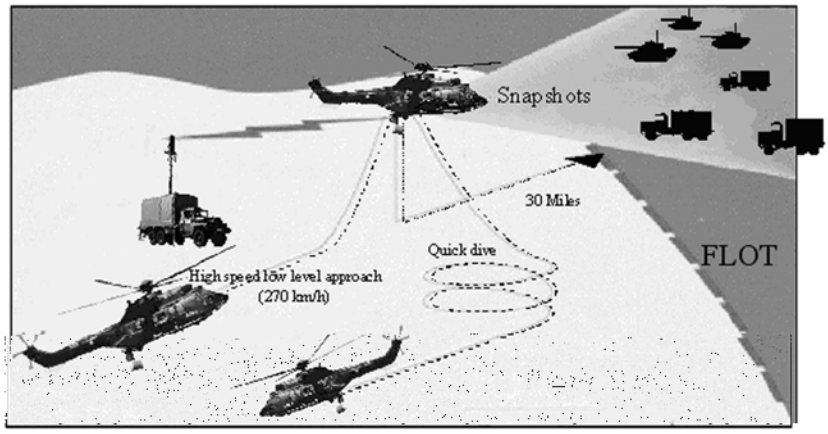
HORIZON can be used in two different modes, depending on the threat: in an airborne warning and control system (AWACS) mode with almost continuous emission, or a succession of two-minute illuminations intermingled with quick climbs and dives so as to protect itself from antiradiation missiles or long-range air defense. According to the various situations, HORIZON will conduct different types of missions and its flight will depend on the context. In any of these cases, confirmation of the information by another sensor is necessary to identify the detected vehicle or to discriminate between civilians and military in a crisis management situation. Some examples are discussed below.

- *Tension Situations* (see Figure 4). HORIZON can fly near the surveillance area and in some situations it can perform penetration flights. With intermittent surveillance, it can detect, pinpoint, and classify convoys and vehicle concentrations as well as helicopters throughout the surveillance area.[3]
- *Crisis Management* (see Figure 5). The flight will take place at a safe distance from the surveillance area, with almost continuous surveillance of hostile activities and ground forces deployments.
- *Armed Conflicts* (see Figure 6). Because of the increased air defense threat, the flight will take place at a safe distance (30 miles away from the contacts) with continuous surveillance or quick highlights of the battlefield. Its detection and localization capabilities will increase to 60 miles beyond the forward line of own troops (FLOT).



Mission: Provide information regarding suspicious movements within critical areas and prepare the commitment of friendly forces

Figure 5. HORIZON's Operating Mode–Crisis Management.



Mission: Provide, in real time to the intelligence and command cells, the information allowing them to ensure force protections during commitment, prepare and conduct operations, commit depth attack assets, guide attack helicopters to their targets.

Figure 6. HORIZON's Operating Mode – Conflict.

- *Peacekeeping NATO.* HORIZON can also participate in peacekeeping activities within multinational operations (United Nations [UN], North Atlantic Treaty Organization [NATO]) by helping to maintain security in the territories and on the borders.[4]

MALE-UAV Correlation: Among all the collection assets used, UAVs are the best suited to confirm information gathered by HORIZON, and among the different types of UAVs, the MALE UAVs are the most complementary, thanks to their endurance and reach. Tactical UAVs like the Crecerelle[5] can also cooperate with HORIZON, but they do not have sufficient range to cover the whole area monitored by HORIZON.

The MALE UAV typically has a range at least equal to 90 miles, which it can double by using a relay plane. This range from the ground station allows the UAV to have a penetration capability equal to HORIZON's on the whole radar front (120 miles). Its endurance of more than 10 hours ensures continuous availability during the HORIZON's mission.

Since it is redirectable in realtime, it can be sent at any moment to confirm a new target and then come back for another mission. This flexibility makes it the ideal confirmation tool for the HORIZON data.

The UAV enables the INTEL IC to reliably identify the type of equipment detected by HORIZON and to give its location with sufficient accuracy to launch a fire mission[6]. The MALE UAV confirms HORIZON information, but also complements its action: the UAV can detect unmoving targets that are undetectable for HORIZON. It does more than double-check the radar's detections.

How the Cooperation Works. The cross-cueing between the two assets, HORIZON and UAVs, is managed by the INTEL-IC. Received in real-time on an imagery workstation, the HORIZON images isolate specific targets that will be the subject of a confirmation request by a UAV to categorize and pinpoint the threat. This confirmation can be done in two ways: either the INTEL IC organizes a mission and totally dedicates the UAV's flight to the HORIZON cooperation, or the UAV's tasking to confirm the target is done in realtime by steering it while in flight (dynamic retasking).

The intelligence cell can establish an intelligence cycle between the HORIZON data and the UAV's confirmations. After detecting suspicious convoys, the INTEL IC sends a UAV for confirmation. Once they cross-check the information, HORIZON can track it, and as many UAV flights as needed can follow for confirmation.

As for the other sensors managed by the INTEL IC, cooperation between HORIZON and MALE UAVs benefits from a complementary, synergistic effect, which magnifies capacities: the UAV compensates for the HORIZON's limitations by identifying the detected equipment, and HORIZON brings a scope the UAV does not have. Synergy has a multiplier effect: the intelligence produced with the HORIZON data confirmed by a UAV is clearly superior to the sum of information gathered by each system independently. In an area 130 miles wide and 60 to 90 miles long, analysts identified the targets detected and tracked by these two sensors, pinpointed them with accuracy, and extrapolated a future position. This intelligence brings aid to both the targeting and to the future maneuver planning processes. By its collection scope and by steering the UAVs' investigations, as well as by the integration of its own capabilities with those of the other sensors, HORIZON gives the INTEL IC greater adaptability to counter the enemy's maneuver.

The Unifying Role of HORIZON and Its Consequences

Maneuver Planning. HORIZON is the only tactical collection asset able not only to cover the entire intelligence AOI but also do it in a single mission and at short notice. Therefore, it plays the critical role in cueing the intelligence-gathering assets.

The data gathered by HORIZON will provide the basis for the other sensors' mission planning. According to the threat evaluation done from this information, the appropriate assets INTEL IC will steer toward the high-enemy-density areas. The other technical or HUMINT-gathering assets will be able to complement and

increase the value of the information gathered by HORIZON by bringing in their own added value.

The detection depth gives sufficient preparation time for the most difficult sensors to be redeployed or reorientated (human research after deployment, electronic warfare) if necessary.

The capability to analyze moving targets and extrapolate a convoy's future positions allows the INTEL IC to maneuver the sensors efficiently and to anticipate the combat commanders' intelligence requirements.

Conduct of Operations: HORIZON permits cueing intelligence-gathering missions in near-real time by regularly refreshing the available picture of the enemy's deployment. The INTEL IC can steer in real time all available sensors it manages.

This unifying role is valid in all spectrums of conflict, ranging from peacetime military engagements to small-scale contingencies to major theater war. The system's vulnerability due to its vector and lack of stealth of its radar radiation is made up by its detection range. This allows the use of stand-off.

By the size of its search area, HORIZON is truly the unifying tool of the French Army's intelligence assets. It has a central role in the decisions made by the INTEL IC for all the other sensors, either to confirm or complement the information it provided. Among the various sensors available, one of the best cooperations will be with the future MALE UAVs due to their ability to confirm and add information to the information provided by HORIZON. This cooperation will be the cornerstone of the future intelligence cross-cueng for French operational ground forces.

Endnotes

1. HORIZON (Helicoptere d'Observation Radar et d'Investigation Sur Zone) is a French targeting radar with moving target indicator (MTI) capability.

2. France has already used UAV and heliborne radar systems in operational situations both during armed conflicts (Gulf War 1991, Kosovo bombing 1999) and peacekeeping operations (Kosovo 1999). In these two operations, the two assets performed without any real cooperation, in spite of their complementary nature. The structure of the INTEL IC allows us today to envision this cooperation.

3. One of the missions the system performed prior to the entrance into Kosovo by the ground forces.

4. For example, HORIZON will also be able to help protect humanitarian convoys by observing their environment, help fight against illegal immigration, and by surveying great areas and possible infiltration spots.

5. Crecerelle is, with the CL 289, one of the two tactical UAVs in use in the French Army. The Sperwer, built by the same company will replace it soon.

6. Later on, those same MALE UAVs will probably be armed and therefore be able to strike themselves, therefore reducing considerably the "sensor-to-shooter" delay.

Lieutenant Colonel Martin Renard is currently the French Liaison Officer at the U.S. Army Intelligence Center and Fort Huachuca in Arizona. As a French Army officer's son, he grew up in France, Germany, and the United States. A graduate of the French Military Academy of Saint Cyras (in International Relations) and the Armor Officers Basic Course in the Armor Branch School in Saumur, LTC Renard joined the French Brigade in Berlin, Germany, where he served as a Medium Tank (AMX 30) Platoon Leader. While on this assignment, he participated in an exchange program organized by the U.S. Commander of the Berlin Brigade and spent six months as the 3d Platoon Leader (M60 A3 tanks) in the U.S. 40th Armor Squadron. He was a Tank Company Executive Officer (XO) during his last year in Berlin Brigade. After serving as an Instructor for the Draftee Officers Basic Course at the Armor Branch School and attending the Armor Captain's Command Course, he became a Reconnaissance Troop XO and then Troop Commander with the French 3d Corps Cavalry Reconnaissance Unit. He was next a Training Battalion Deputy Officer at the Military Academy of Saint-Cyras. Success on a competitive exam to enter the French Command and General Staff College led to his attendance at the CGSC and the French Joint College (in the International Course). After graduation, he joined the Armor Branch School at the Futures for Armor Directorate, where he was in charge of careers definition for all Armor personnel. LTC Renard received the French Defense Meritorious Service Medal (Silver). Readers may contact the author via E-mail at martin.renard@hua.army.mil.

MI Corps Hall of Fame Nominations

The Military Intelligence Corps accepts nominations throughout the year for the MI Hall of Fame (HOF). Commissioned officers, warrant officers, enlisted soldiers, or civilians who have served in a U.S. Army intelligence unit or in an intelligence position with the U.S. Army are eligible for nomination. A nominee must have made a significant contribution to MI that reflects favorably on the MI Corps.

The Office of the Chief, Military Intelligence, provides information on nomination procedures. If you wish to nominate someone, contact the OCMI at U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-MI, Fort Huachuca, AZ 85613-6000, call commercial (520) 533-1173 or DSN 821-1173, or via E-mail at OCMI@hua.army.mil.

MASINT: New Eyes in the Battlespace

by William K. Moore
(U.S. Army, Retired)

MASINT will help us view another dimension of the 21st re5T6vosAther early 1Ys as a means of describing intelligence operations and sources other than the more traditional signals intelligence (SIGINT), human intelligence (HUMINT), and imagery intelligence (IMINT). This "new" source actually represented innovative methods employed to support the oldest and most basic form of intelligence—the process of trying to identify an object or event. One hundred years ago, the "measurement" was often a scout's view of an event occurring in front of his unit. The "signature" identification was the process occurring in his head in which he compared the observed event to his personal "database" or memory of similar events and then identified the activity. Completing this simplistic scenario, he reported the information to a commander or other person who could use it. He detected, processed, identified, and reported. Now and in the future, the Military Intelligence (MI) soldier will take advantage of sources that will provide full-spectrum intelligence, surveillance, and reconnaissance (ISR) to the warfighter. They include—

- ❑ Acoustic.
- ❑ Magnetic.
- ❑ Seismic.
- ❑ Nuclear, biological, and chemical.
- ❑ Radar.
- ❑ Multi-, hyper-, and ultra-spectral.
- ❑ Electro-optic (EO).
- ❑ Radio energy.
- ❑ Olfactory, and other signatures.

MASINT complements the more traditional forms of Army Intelligence by accomplishing the base work of identification, characterization, and location of battlespace entities.

As we move farther into the 21st century, MI faces complexities that will drive our methods and technology in new directions, many of which we can only partially envision today. One of those is the wide availability and dispersion of crucial enabling technologies to every political and military entity in the world. It will become harder to develop intelligence against these forces with traditional methods. MASINT looks at every intelligence indicator with new eyes and makes available new indicators as well. It measures and identifies battlespace entities via multiple means that are difficult to spoof and it provides intelligence that confirms the more traditional sources, but is also robust enough to stand alone. In my opinion, the Army does not treat MASINT as a major intelligence source with the same institutional imperatives as SIGINT, IMINT, and HUMINT. Because of its numerous and widely divergent sources and its long association with the technical intelligence community, it does not receive the visibility of its more "mature" cousins. We have not fully engaged MASINT as an operationally valid contributor to the common operational picture (COP) of the battlespace, but these conditions are changing.

Background

In October 1998, the Army assembled a team of functional area experts to design a MASINT concept of operation (CONOP)i chaired jointly by the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH), the Army Deputy Chief of Staff for Intelligence (DCSINT), and the U.S. Army Intelligence and Security Command (INSCOM). The Army charted this integrated concept team (ICT) to develop a CONOP that both defined and forecasted an "operationalized" MASINT with emphasis at echelons corps and below (ECB). The CONOP included a description of requirements, a basic operational architecture, and an analysis of how Army MASINT would support the Army from the years 2005 through 2025. The ICT's goal was to identify future operational capabilities (FOCs), develop an experimentation plan, and assess the impact of MASINT on DTLOMS (doctrine, training, leadership development, organizations, materiel, and soldiers). The result of this effort was a roadmap that the Army would follow to capitalize on recent developments in training and technology in order to complete the ISR infrastructure for the future.

We are not starting from scratch. The U.S. Army has a fairly long history of involvement with nontraditional intelligence development using MASINT. For example, in Vietnam a system known as "Igloo White" was the mainstay remote-detection program that allowed us to conduct our counter-infiltration efforts. It consisted of acoustic, seis-

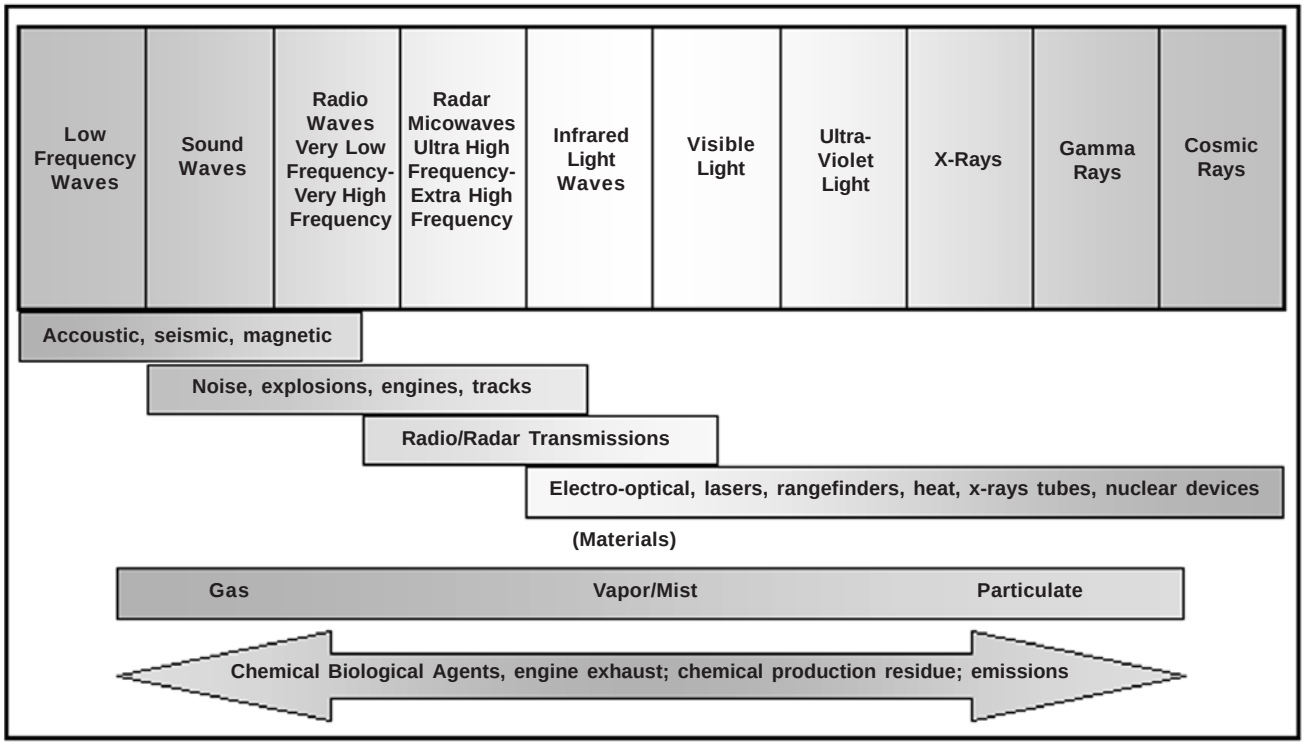


Figure 1. Signature Spectrums (Electro-Magnetic).

mic, and magnetic sensors remoted to a central facility for exploitation. Based on that technology, we have today's Improved Remotely Monitored Battlefield Sensor System (I-REMBASS), the soon-to-be-fielded REMBASS II, and the Prophet system that will bring several intelligence domains together into a single package. Similar programs exist throughout our Armed Forces (for example, Steel Rattler and the Platoon Early Warning Device). We have also developed radar-based MASINT intelligence at the tactical level, which for many years employed our AN/PPS-5 and -15 radars. Today, we derive phased- history data (PHD) from synthetic aperture radars (SAR) and moving target indicator (MTI) radars on the Army's Airborne Reconnaissance Low (ARL) aircraft and are major consumers of Joint Surveillance Target Attack Radar System (Joint STARS) MTI data. Finally, we are actively investing in hyperspectral MASINT (HSM) technology for future applications that will allow us to examine and identify battlefield entities with new sets of discriminating sensor suites. Simply stated, these are all techniques for comparing collected information to stored templates and signatures to identify battlefield entities.

All of these detectors and many others are undergoing improvement today to provide clearer threat definition and, when coupled with extraordinary advancements in database and processing technology, positive identification at the sensor location, not in a laboratory thousands of miles from the operation. This latter feature is what grants relevancy to our warfighters and finds expression in the following types of scenarios.

- ❑ Achieving real timeliness by automatically detecting, identifying, and reporting enemy activity.
- ❑ Measuring the probability of weapons of mass destruction (WMD) effects in the battlespace, such as identifying the presence of biological agents.
- ❑ Detecting and locating minefields.
- ❑ Providing real-time signature data to reprogrammable munitions and sensors.
- ❑ Tagging and tracking enemy equipment of all types through all environmental conditions.
- ❑ Monitoring no-fire and demilitarized zones and detecting violations.
- ❑ Countering enemy stealth technology.

The Future

Tactical MASINT, therefore, is by its very nature based on varied sources, produces a multiple intelligence disciplines-based product, and is well able to support the other, more traditional intelligence sources. More significantly, it has the potential to enrich the COP due to the characteristics that make it unique. Specifically, tactical MASINT provides tireless ISR and target acquisition collection and is most useful in areas in which soldiers cannot deploy but where we have vital interests. It does this by using on-board processors that carry algorithms and signature databases allowing for near- instantaneous characterization and/or identification of battlefield entities. The overarching characteristic of MASINT that ties these disparate

sensing regimes together is the following processing methodology: t**o compare the detected measurement (from whatever source) to a database of operationally relevant signatures to characterize and/or identify and locate battlefield entities.** Tactical MASINT **analysis** will occur at the MASINT Domain (MD) of the Distributed Common Ground System-Army (DCGS-A) and will provide identification for a new, anomalous, or otherwise unidentified battlefield entity. The system then downloads the resultant product to the sensing networks and elsewhere as required.

In this concept, tactical MASINT for the Objective Force (TMOF) sensing suites will be integrated, special purpose, remote detection, and identification devices. They will consist of terrestrially based air- and ground-deployed sensors, processors, and dissemination (SPD) sub-components, interconnected into an information grid that will provide wide-area search and cueing. They will detect, acquire, identify, track, and support the acquisition of targets through network connectivity to DCGS-A and the future Objective Force battle command system. TMOF will support defensive and offensive information operations (IO), ISR, and Target Acquisition (TA) in operations from small-scale contingencies to major theaters of war and will include capabilities for supporting complex urban operations. TMOF will automatically detect, characterize, and identify battlefield entities and cue TA, tracking, and attack options. Tailored TMOF will deploy throughout the battlespace to provide full-spectrum coverage of all activity within the assigned areas. Upon detection, we will characterize a battlefield entity as to type, direction of travel and numbers, friendly, enemy, neutral, unknown and, when possible, identified. If friendly or neutral, we will track the entity while the identification and location from the TMOF network, through common battlefield communications, to the future Objective Force battle command system for both "Blue" and "Gray" update. If enemy, we will track the entity while the TMOF network immediately reports identification and location to the DCGS-A's MD as well as to the future Objective Force battle command system for "red forces" update. If unknown, the entity's characterization will be vehicular (wheeled or tracked), personnel (armed or unarmed), aircraft (fixed or rotary) or ambiguous. We will monitor the unknown entity while pertinent parametrics are recorded at the TMOF network "gateway" for further download to (and analysis at) the DCGS-A's MD, time permitting.

As described in the MASINT CONOP, the measurement could indicate a new mode of operation, which might reflect changed enemy performance data. TMOF will exploit signature processing at or near the sensor to provide full-spectrum coverage of the battlespace. When coupled with other sources of intelligence, this will allow information superiority to build from the forward point of conflict and permeate the battlespace. In combat environments, TMOF will tirelessly examine new and less conventional operational parameters and external indicators for evidence of friendly, enemy, and neutral activity through inherent multiple intelligence collection and data fusion. This data will be crucial for the maintenance of the COP. TMOF will also cue other weapon and sensor systems, maintain the necessary coverage of the expanding, complex battlespace, and allow for high Operational Tempo (OPTEMPO) while minimizing human intervention and workload.

These systems rely on organic intranetted communications and have hub access to the DCGS-A and the future Objective Force battle command system for processing support, analysis, and intelligence dissemination. Joint and coalition forces will access this same information through their connectivity to the future Objective Force battle command system.

Lastly, unattended TMOF must adopt some of the behavior of human scouts when it detects a possible threat. It must adopt low observability and be capable of "hiding" (or relocating), observing, reporting, and protecting itself until the incident is resolved. Additionally, it must be equipped with an anti-tamper capability that is harmless to humans, but self-destructs. TMOF assets will be tailored for split-based and remoted operations featuring connectivity based on the intranetted DCGS-A.

Prognosis

On 19 May 1999, Major General John D. Thomas, Jr., then Commanding General, USAIC&FH, signed the MASINT CONOP. Prior to this, senior personnel from throughout the Army, many of whom actively participated in its construction, had reviewed the CONOP in a series of In- Progress Reviews (IPRs). The approved CONOP emphasizes the following:

- A system that provides answers to the tactical commander based on the automatic, real time comparison of collected information to stored signatures. It further defines the basic requirement for the future development of sensing suites. It requires processing close to the sensing head and the subsequent real-time iconic display of MASINT data to enable the "Now Battle" and influence future plans. The CONOP recognizes there will never be enough bandwidth available to the tactical commander to ensure passage of raw intelligence data; therefore, the future will see sensing suites with dynamic, reprogrammable libraries of regionalized signatures for on-the-spot identification, and a limited anomaly storage capability.
- The employment of terrestrially based (air and ground) collection systems across the spectrum of conflict to include stability operations and support operations, ur-

ban operations and areas not routinely accessible by more conventional collection means.

- Integration of the data available from sensors used by other than MI forces (Army Target Sensing Systems such as the Future Combat System (FCS)) to enhance situational awareness.
- Ability to engage the MASINT expertise at echelons above corps (EAC) and Technical Intelligence Centers to provide direct support to ECB for specialized collection, analytical support, and reprogramming of Army Target Sensing Suites (ATSS). This readiness constitutes a genuine "mud-to-space" construct for intelligence support to the Objective Force.
- The proliferation of automated target recognition (ATR) capabilities, which implies a requirement for adequate pre-deployment signature development and post-fielding signature maintenance support.

Since the CONOP serves as the roadmap for the future of MASINT in the Army, it also acts as the requirements blueprint document. As such, the ICT actively assessed sensor, processor, platform and communications technology, training, and organizational impacts. In August 2000 the Deputy Chief of Staff for Operations (DCSOPS), DCSINT, and USAIC&FH formed an Integrated Product Team (IPT) to focus more on near-term solutions to the requirements outlined in the CONOP.

The IPT sought to identify available and projected platforms suitable for use in support of MASINT operations out to about 2010. Additionally, the IPT explored sensing and processing technology available today to apply to these platforms. This ability coincides with, and conforms to, the Army's Transformation goals and objectives. Work groups dealing with ground, air, Tactical Exploitation of National Capabilities (TENCAP), and processors and display systems were formed and the results released in late 2000. Integration of technical upgrades to existing and near-term platforms and programs will involve a great deal of activity for the next few years.

So What?

Sensing technologies based on the detection of battlefield entities and the comparison of the results to a library of signatures for identification have moved beyond the Intelligence Battlefield Operating System (BOS) and into the combat arms. The FCS will depend almost entirely on its MASINT-based sensing suites. Many of our weapon systems are, and will be, based on embedded threat and terrain signatures allowing ATR; so it is not just MI taking advantage of these capabilities. For the MI soldier and his supported commander the future will hold a toolbox of MASINT collection systems designed with flexibility in mind. Tactical MASINT sensing suites will, in addition to detectors, be processor-centric. TMOF will take advantage of the technical leaps that have occurred in numerous fields over the past 20 years, many of which have never been applied to tactical MASINT suites. Each can be configured with mission-appropriate "plug-and-play" sensor heads. If these components are hand-emplaced, they will also receive necessary long life power supplies and dissemination media. If they are emplaced via a robotic platform, unmanned aerial vehicle, or manned tactical vehicles, they will rely on the host platform for power and communications.

Other sensors organic to the maneuver force to support their targeting and force protection requirements will detect, compare, and report results to their assigned units and to the S2 of the maneuver battalion or brigade (Unit of Action [UA]in Objective Force-speak). These will then be transmitted as required to higher headquarters via tactical MASINT reports (TMRs). Networked TMOF, operated by the supporting MI unit, will help satisfy the commander's intelligence requirements. They would be emplaced to identify the battlefield entities in the Division (Unit of Engagement) or UA commander's area of interest. Detailed, specific results from both organic and non-organic MI sensing suites will be transmitted automatically to the DCGS-A at the UA and unit of employment (UE).

For the field commander, this helps assure timely intelligence support in the most dangerous environments imaginable—frequently environments where soldiers are unable to gain access. These environments will not be amenable to traditional intelligence development. At the maneuver level, available detectors will be battle enablers, allowing the unit to maneuver out of contact, launching operations at the most salient point and time. The commander will have full targeting and force protection sensor suites available to provide early warning and ATR. Tactical commanders and staffs will see the results of this MASINT system in a fully processed format on the DCGS-A displays. Relevant products of national and theater MASINT systems will be available as far down as the maneuver battalion, the UA.

MASINT promises to be an economical enhancement to the intelligence structure of the force because its first objective is entity identification. The results can be useful in the all-source world for confirming intelligence or cueing other sources. We'll ask it to confirm targets. We'll use it in an economy of force role and to prevent surprise. We'll drop it in deep or fly it over our entire area of interest to confirm intelligence preparation of the battlefield (IPB). MASINT, when fully engaged, will enhance and allow full- spectrum dominance and, ultimately, the information dominance of the battlespace.

Summary

To a large extent, the tactical Army is going to play catch-up with the

(Continue on page 48)

LANGUAGE TOOLS

by Kenneth Dunn

The Army has always had a need for soldiers with language skills, and soldiers with the ability to speak foreign languages are in demand now more than ever. Unfortunately, the Army has never been able to maintain the number of linguists it needs, particularly in the hard-to-fill, low-density languages. The Language and Speech Exploitation Resources (LASER) Advanced Concepts Technology Demonstration (ACTD) is working to provide much needed automated assistance to linguists, while providing rudimentary translation devices to those who cannot speak a foreign language.

The LASER ACTD is a cooperative effort among some of the most language-dependant organizations in the U.S. Government. With the Army as the lead, the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) provides the technical manager for the program, with the U.S. Army Intelligence and Security Command (INSCOM) and U.S. Army, Pacific (USARPAC) serving as "co-operational" managers. This all-star team also includes the Central Intelligence Agency (CIA), Federal Bureau of Intelligence (FBI), National Security Agency (NSA), Defense Advanced Research Projects Agency (DARPA), and the Army Research Laboratory (ARL), among others. This powerful combination of researchers, scientists, linguists, analysts, and intelligence professionals creates a blend of technical expertise and practical knowledge that helps the entire team rapidly hone in on the best technology available for our soldiers today, while helping to steer developments to meet the future needs of soldiers.

The LASER ACTD is actually an expansion of some technologies demonstrated in the Human Intelligence Counterintelligence Support Tools (HICIST) ACTD. According to Lieutenant Colonel Kathy J. Debolt, Technical Manager for both the HICIST and LASER ACTDs, "*Language translation was just one portion of HICIST, but the soldiers found these tools to be such timesavers and so useful that we felt we should continue to work on languages as a separate ACTD*." Several such tools exist to include—

- ❑ FALCon, the Forward Area Language Converter, which translates documents from foreign languages into English, that began as a HICIST initiative and will continue.
- ❑ A multilingual chatroom carried over from HICIST.
- ❑ FORUM, which allows commanders and others to enter information in their native languages and have it instantaneously translated into multiple other languages.
- ❑ The document explotaition (DOCEX) Suite, a DOCEX package that enables operators to process multitudes of captured enemy documents quickly in order to recover documents of operational value to the commander rapidly.
- ❑ The Phraselator, a speech-to-speech machine translator from English to Arabic, Dari, Pashtu, and Urdu currently in use in Afghanistan, began as a DARPA initiative and will continue under the LASER, ACTD. (See the article on the Phraselator in this issue of ***MIPB***.)

A major challenge facing any attempt to develop language translation

(Continued on page 41)

Advanced Concept Technology Demonstrations

Advanced Concept Technology Demonstrations (ACTDS) allow users to gain understanding of proposed new capabilities for which there is no user experience base. Specifically, they offer the warfighter an opportunity to—

- ❑ Develop and refine his concept of operations.
- ❑ Exploit the capability under evaluation fully.
- ❑ Evolve his operational requirements as he gains experience and understanding of the capability.
- ❑ Operate militarily useful quantities of prototype systems in realistic military demonstrations and on that basis, assess the military utility of the proposed capability.

The Department of Defense (DOD) initiated the ACTD program in 1994 to help expedite the transition of maturing technologies from the developers to the users. The ACTD program was to help the DOD acquisition process adapt to today's economic and threat environments.

ACTDs emphasize technology assessment and integration rather than technology development. The goal is to provide a prototype capability to the warfighterand to support him in the evaluation of that capability. The warfighters evaluate the capabilities in actual military exercises and at scale sufficient to assess military utility fully.

For more information about ACTDs, please see the following internet web site: http://www.acq.osd.mil/actd/index.htm

Tactical Source Profiling and Indicator Analysis

by Chief Warrant Officer Three Gregory M. Garcia

Human intelligence (HUMINT) collectors and counterintelligence (CI) agents visualize a different battlefield than do other military intelligence (MI) collectors and analysts. In particular, our battlefield and consequently our areas of operations (AOs) are among concentrations of people. In such an environment, the HUMINT collectors and CI agents can easily become inundated with the number of potential sources. Tactical source profiling and indicator analysis is a process that helps the collectors narrow their collection focus and a means whereby the collectors can target the best available potential sources with the greatest degree of success. This analytical process clears up an otherwise "muddy" picture of the population centers allowing the HUMINT collectors and CI agents to visualize their battlefield better.

Often referred to as the oldest intelligence discipline, HUMINT is evaluated and collated information obtained from human beings. U.S. Army HUMINT collectors train in questioning methodologies and support the military decision-making process by developing and reporting timely and accurate information. The collectors serve in military areas of concentration and occupational specialties 35F (Human Intelligence), 351E (Human Intelligence Collection Technician), and 97E (Human Intelligence Collector), while the CI agents are in 35E (Counterintelligence), 351B (Counterintelligence Technician), and 97B (Counterintelligence Agent). While performing differing intelligence missions, both the HUMINT collectors and CI agents support many of the same collection operations; additionally, they employ many of the same methodologies in performing their missions. In this sense, it is quite common for both types of collectors to collect information from human sources, albeit for different end states. This article will focus on tactical HUMINT collection operations although the source-profiling process applies to both HUMINT collectors and the CI agents.

Doctrinal Note: This article includes the terms "information" and "intelligence" and alludes to an analytical process conducted by HUMINT collectors on the information they have collected. The collectors generally describe and report their "thoughts" regarding this collected information as a paragraph on the intelligence information report (IIR) as "**field comments**." For the purpose of this article, the reader should use the following definitions:

- *Information*. **FM 101-5-1**, **Operational Terms and Graphics**, states that "information" is the meaning that a human assigns to data by means of the known conventions used in their representation.
- *Intelligence*. **FM 101-5-1** states that "intelligence" is information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
- *Field Comments*. The assumptions, opinions, or conclusions reached by the HUMINT collector regarding the information he or she has collected, source information, or comments on reliability or credibility.

Missions of HUMINT Collectors

HUMINT collectors perform a variety of missions to satisfy the intelligence requirements at all echelons of command. Although HUMINT plays a significant role in strategic planning, this article addresses the collection missions in the tactical environment. The HUMINT operations performed in the tactical environment include—

- Screening operations.
- Interrogation operations.
- Debriefings and interviews.
- HUMINT contact operations.
- Document exploitation (DOCEX) operations.
- Liaison operations.
- Open-source information operations.
- Support to force-protection (FP) operations.
- HUMINT analysis.

U.S. interests in areas such as Haiti, Bosnia-Herzegovina, and Kosovo have seen a steady deployment of military forces to environments heavily laden with noncombatants. As a result, HUMINT collectors are a hot commodity in short supply. Local nationals, refugees, host-nation officials, nongovernmental organizations (NGOs), partisans, foreign military organizations, and paramilitary organizations are just a few of the groups that U.S. military forces encounter while performing their missions. HUMINT collectors view each group as a potential source of information, and as such, execute their missions by interfacing and communicating with them.

As the target of intelligence collection efforts, human beings provide unique challenges and opportunities. Specifically, the collector must deal with the variables of human behavior, thought, cultures, relations, and languages. Because these vary from

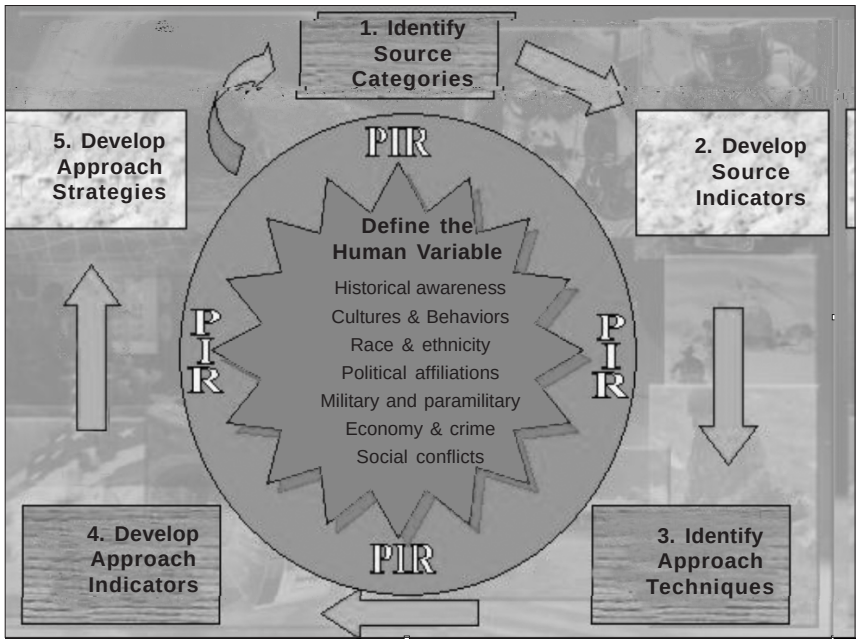


Figure 1. Source Profiling Developmental Process.

one society to another, HUMINT collectors **must** achieve increased understanding of the target area and the human variables with which they plan to interact. Effective collection demands a thorough understanding of a country's history, social structure, culture, demographics, religions, education, internal and external conflicts, economics, and politics.

Population centers—such as cities, villages, camps, way stations, and base-camp clusters—coupled with the human variables create a unique operational condition for the collector. HUMINT collectors must examine and analyze their battlespaces fully. Therefore, HUMINT collectors must devise analytical methods to examine the human variables and to enhance their ability to identify, assess, and exploit their sources successfully. Source-profiling and indicator-analysis tools assist team leaders in conducting tactical mission planning.

Source Profiling

Source profiling is a developmental and analytical process (see Figure 1) that groups potential source types by category and according to a particular set of attributes and exploitable characteristics. Once they have categorized the source types, HUMINT collectors can analyze their characteristics to identify exploitable strengths and weaknesses. Timely and accurate HUMINT collection operations rely on the teams' abilities to identify and familiarize themselves with the AOs' pools of potential sources. Source profiling provides the detailed analysis of these sources, and helps to paint mental pictures of potential sources. It prepares the collectors for encountering their sources. In many respects, this form of analysis represents a cross between a psychological profile and stereotyping. In essence, source profiling serves as a foundation or starting point for collection operations, and it is an easy way to instill confidence in the less experienced or more junior HUMINT collectors.

The most important part of the developmental process is research. Study of a country's target audience (the population) lies at the center of the profiling process and sets the stage for all follow-on procedures. This research is crucial for successful collection operations. The commander's priority intelligence requirements (PIR) not only drive the collection efforts, but also focus this research effort, since the collectors accomplish each step of the profiling and indicator process by focusing on the PIR. Without this focus, the HUMINT collectors operate in a vacuum and the scope of the collection mission is too broad to be effective. Collectors' knowledge extends beyond what is available in country study briefings, deployment briefings, and the intelligence annex of an operations order. Although good starting points, the information contained in these briefings will not provide the level of detail that HUMINT collectors require to analyze both the strengths and weaknesses of the categorized sources. One can only conduct this form of analysis through dedicated research efforts. By combining the PIR with research, the HUMINT team is prepared to begin the developmental process.

Source-Profiling Developmental Process

Step 1: Identify Potential Sources and Develop Categories

Although referred to as Step 1 in source profiling and indicator analysis, developing source categories is not a new idea. For many years, our HUMINT collectors have categorized prisoners of war and captured enemy documents during screening, DOCEX, and interrogation operations. The **North Atlantic Treaty Organization (NATO) Standardization Agreement 2033**, **Interrogation of Prisoners of War** and **FM 34-52**, **Intelligence Interrogation**, mention the idea of source categories. However, categorizing prisoners of war and captured enemy documents in this sense prioritizes the exploitation process. When applied to the source-profiling and indicator-analysis process, the purpose of source categorizing is to develop lists of potential sources for possible exploitation.

Instinctively, HUMINT collectors identify the obvious belligerent cat-

Source Categories Enemy Military Force	Civilians on the Battlefield	Belligerent Groups
1. Special Purpose Forces: PIR # 1, 3, 4, 5, 6 Indicator 1: Individuals captured conducting unconventional warfare missions, special reconnaissance, special direct action missions, etc. Indicator 2: Individuals captured training or operating with insurgents or civilians Indicator 3: Individuals captured with specialized weapons, equipment, or uniforms A. Primary Approach: Emotional Love of Comrades Indicator 1: Expresses concer for individuals captured with him Indicator 2: Source asks to communicate with members of his unit Indicator 3: Source maintains close contact with other sources in the holding facility B. Secondary Approach: Pride and Ego Down Indicator 1: Source captured under embarrasing circumstances Indicator 2: Source exaggerates about the circumstances of capture in an attempt to cover up feelings of inferiority Indicator 3: Source displays an arrogant or prideful attitude; tries to vindicate himself from responsability	1. Host-Nation Officials: Indicators 1-3: XXX A. Primary Approach: Indicators 1-3: XXX B. 2nd Approach: Indicators 1-3: XXX	1. The NLA Insurgency: Indicators 1-3: XXX A. Primary Approach: Indicators 1-3: XXX B. 2nd Approach: Indicators 1-3: XXX
2. Aircrew Members: PIR # 3, 4, 6 Indicator 1: Individuals captured with aircraft Indicator 2: Individuals captured in flight uniforms Indicator 3: Individuals captured with associated technical documents A. Primary Approach: Fear-Down Indicator 1: XXX Indicator 2: XXX Indicator 3: XXX B. Secondary Approach: Incentive Indicator 1: XXX Indicator 2: XXX Indicator 3: XXX	2. Civilian Populace: Indicators 1-3: XXX A. Primary Approach: XXX Indicators 1-3: XXX B. 2nd Approach: XXX Indicators 1-3: XXX	2. Criminal Organizations: Indicators 1-3: XXX A. Primary Approach: Indicators 1-3: XXX B. 2nd Approach: Indicators 1-3: XXX
3. Intelligence Personnel: PIR # 5, 6 Indicator 1: Individuals captured with intelligence collection systems Indicator 2: Individuals captured with classified documents Indicator 3: Individuals who speak foreign languages A. Primary Approach: Fear-Up Indicator 1: XXX Indicator 2: XXX Indicator 3: XXX B. Secondary Approach: Emotional Love of Family Indicator 1: XXX Indicator 2: XXX Indicator 3: XXX	3. NGOs: Indicators 1-3: XXX A. Primary Approach: XXX Indicators 1-3: XXX B. 2nd Approach: XXX Indicators 1-3: XXX	

Figure 2. Source Profile Table.

egories of potential sources—enemy prisoners of war (EPWs), insurgents, terrorists, and members of criminal organizations. However, collectors must give careful consideration to categories of nonbelligerents, who quite often are more readily available and can provide a wealth of information. These types of sources include host-nation officials, local nationals, NGOs, refugees, and displaced persons. Identifying and categorizing potential sources is a matter of familiarity with the target country and populace. The greater the familiarity, the easier it is for the collectors to identify the potential sources they will encounter in the villages, on the roads, in the refugee camps, and in the holding facilities.

These lists of potential sources can easily become very large and difficult to manage. For this reason, the collectors need to focus on two things: **placing the source types into manageable categories** and **synchronizing the list with the commanders' PIR**.

Manageable Categories. Categorized individuals possess several characteristics in common. For example, Figure 2 lists the category of **belligerent groups** as a potential source of information and useable intelligence. Common characteristics of these belligerent groups may include individuals that—

- ❑ Display hostile intentions toward U.S. interests in the AO.
- ❑ Possess the means to engage U.S. soldiers or allies.
- ❑ Have demonstrated their willingness to attack U.S. interests to accomplish their agendas.

In our example, members of the "national liberation army (NLA)" (used generically) insurgency and members of organized crime are in one category despite the fact that they may not have any contact or affiliation with each other. The only

thing that might bind them together is common characteristics.

Synchronizing the PIR with the lists of sources. Second, the HUMINT collectors must ensure that they synchronize the lists of potential sources with the commanders' PIR. They review the source list and determine which PIR the sources most likely would be able to answer. For easy recollection, the collector should list these PIR next to each source type. If it appears unlikely that a source could reasonably be able to answer a PIR, then collectors should eliminate that source type from the category list. Remember, source profiling and indicator analysis provide a starting point for collection operations. In the event that HUMINT collectors discover during the course of collection operations that a particular source type proves valuable, they can add it to the category lists.

Step 2: Develop Source Indicators For Each Source Group

When combat arms units prepare to deploy in support of military operations, they expend a large amount of time learning how to identify the enemy they plan to engage. Developing source indicators is the HUMINT collectors' method for identifying and recognizing the potential sources they hope to encounter; these indicators are a series of determinants that help them to identify the type of source encountered as well as to provide collection focus.

FM 34-2, **Collection Management and Synchronization Planning**, explains the purpose of indicators as they relate to PIR. When applied to the source-profiling process, indicators are distinguishing actions or events that help to confirm which type of source the collector has encountered. In this sense, indicators may represent individual or group characteristics, mannerisms, methods of operation, or given sources' distinguishing attitudes. As the HUMINT collectors encounter individuals who portray one or more of these identifiable indicators, they can identify the type of source encountered. Recognizing the type of source is a critical element for successful collection operations. It allows collectors to focus and tailor their thought processes on source characteristics, help establish a collector-source rapport, and expose the source to exploitation. In Figure 2, the HUMINT collector identified the source category of "enemy military forces." By reviewing the commander's PIR, the collector has narrowed this category down to the three primary source types that have the greatest potential of answering the PIR:

- ❑ Special purpose forces (SPF).
- ❑ Aircrew members.
- ❑ Intelligence personnel.

These source types represent the greatest potential of all enemy military forces for answering the PIR. Continuing with the source-profile table, the HUMINT collector has displayed the primary source indicators for each type of source. These are the distinguishing characteristics, actions, and events that reveal which of the three types of enemy military forces the collector may encounter. In our example, if the collector encounters a member of the enemy military forces in the holding facility captured with specialized weapons, leading insurgent forces, or conducting unconventional warfare operations, the collector can ascertain that this source is a member of the enemy SPF. Thus, the collector knows this type of source can potentially answer PIR numbers 1, 3, 4, 5, and 6. Source indicators prove extremely critical in the final steps of the source-profiling process.

Fluid analytical process. Source-profiling and the indicator-analysis method are parts of a fluid. Collectors continually add or delete source types and categories from the process and lists of source indicators may expand and change as collectors meet with and gather intelligence from their sources. If the initial profiling is wrong or the characteristics of a source group change, the table can change to meet the new identifiable circumstances. Source profiling is an ever-evolving and adapting analytical tool.

Step 3: Select Primary and Alternate Approach Techniques

In a perfect world, all HUMINT sources cooperate completely and are truthful with the collectors. Realistically, the collectors will engage in activities with the sources to gain their trust and cooperation and to gather information. The collector's ability to establish open communication with the source is crucial, and it reflects the collector's ability to be attentive to the actions and mannerisms of the source. Collectors employ approach techniques as a way to establish rapport, maintain control, and manipulate the sources' emotions to gain their cooperation. Identifying which approach to employ is the responsibility of the collector conducting the questioning; however, collectors will often rely on recommendations from screeners, supervisors, or previous source reports.

The collector bases the process of selecting the primary and alternate approaches for each source type on the prior analysis of the source groups and these approaches serve as starting points for gaining a source's cooperation. Obviously, identifying an approach based solely on research without the benefit of seeing or screening a source will not be 100-percent accurate. However, the purpose of this process is to develop a starting point for the collector. These selected approaches represent the likely methods for gaining a source's cooperation and establishing rapport. The amount and accuracy of the research the collec-

tors conduct preceding deployment correlates directly to their success.

Under *enemy military forces*, for example, Figure 2 illustrates the primary and alternate approaches considered most likely to be effective for the three source types. The collector determines that SPF are most susceptible to the "emotional love of comrades" and the "pride and ego down" approaches. It is important to realize that the collector does not select these recommended approaches arbitrarily, rather the HUMINT collector recommends these approaches based on sound analysis and research. In our example, the collector has determined that SPF show a strong degree of espirit de corps, display an attitude of arrogance, and possess a genuine concern for members in their organization. This makes them susceptible to the aforementioned approaches.

HUMINT teams, operational management teams, and interrogation operations elements should maintain statistics on successful approach techniques. This is a method for feedback and allows the collector to make any necessary adjustments. For example, perhaps in the past two months, HUMINT collectors have interrogated eight SPF soldiers. Four of these soldiers cooperated on an "emotional love of comrade" approach, two cooperated on the "pride and ego down" approach, and the last two were susceptible to a "futility" approach.

In this example, the collectors begin to recognize a trend indicating that half of the SPF soldiers are cooperating when they employ an "emotional love of comrades" approach. It also reveals that 25 percent of these source types are susceptible to the "pride and ego down" method. More importantly, the collectors are aware that the "futility" approach is proving successful. This is an approach that they did not identify during the initial analysis. As a result, the collectors should continue to monitor its usefulness and rate of success with these types of sources. In the event that a "futility" approach continues to be advantageous, the collectors can add it to the selected list of approaches. It should also be noted that these approach recommendations are not all-inclusive; if at any time screeners or collectors perceive that they should try a different approach, then they must rely on these indicators. This process does not eliminate or take the place of screeners' recommendations, the collectors' instincts, or planning and preparation. We encourage exceptions and additions.

Traditionally, collectors have associated approaches with interrogation operations; however, I submit that approach techniques are applicable to all HUMINT collection operations. During liaison operations, it may be necessary to use a "pride and ego up" approach or even offer "incentives" to gain cooperation. During "local employed persons" screenings, the collector may orchestrate a "love of family" approach to garner the cooperation of the local nationals with whom they are communicating. Our HUMINT collection operations should always apply these techniques and analytical tools. Their purpose is to help focus the collection effort of the HUMINT assets.

Step 4: Develop Approach Indicators

This step serves a purpose similar to that of Step 2 (develop source indicators). In the event collectors must employ an approach, it is imperative that they quickly ascertain which approach will be the most likely to gain the sources' cooperation. The proper selection of an approach combined with a believable orchestration is critical in developing rapport and gaining the sources' cooperation. This skill set directly correlates with the collectors' experience level and their ability to recognize the indicators a source presents. By developing their approach indicators, collectors can identify some likely recognizable actions, statements, or characteristics that help them select one approach over another. Approach indicators provide examples of determinants, and collectors base them on research and a study of the source type's emotional or habitual strengths and weaknesses.

Returning to our example, Figure 2 presents a list of approach indicators for the primary and secondary approaches that represent the leads for helping the collector select an appropriate approach. During a meeting with the source, the collector would begin to recognize several of these indicators: first, the capturing unit indicates the source surrendered without a fight and second, the source appears arrogant and extremely self-assured. These two indicators fit the profiling process and prompt the collector to orchestrate a "pride and ego down" approach for this source.

Approach indicators assist in developing the source's psychological profile. Undeniably, the collector finds approaches and indicators are normally associated with the individual source and, as such, the psychological profile differs for most individuals. However, in the source-profiling process, we attempt to analyze groups or types of sources, which allows for quicker and easier management. Collectors can select successful approach techniques with their corresponding indicators for groups of source types. Sociological studies often contain a profiling flavor. In particular, these studies examine the characteristics of individuals based on race, ethnicity, political affiliation, geographic location, religion, age, and so forth. Common characteristics or mannerisms are threads that connect individuals together into recognizable groups; for the HUMINT collector, these common attributes, characteristics, mannerisms, and attitudes represent some of the source type's exploit-

able strengths and vulnerabilities. In short, the approach indicators are the evidence that points the collector to a known "weakness" and one the source exhibits at a given point in time. Collectors who take the time to conduct this form of analysis will benefit from increased awareness, confidence, and ease of collection.

Step 5: Orchestrate Approach Strategies

Orchestrating the approach strategies represents the crux of the source-profiling process. The greatest benefit of developing these strategies is that it instills confidence in the collectors of their abilities to perform the collection operations and run the approaches to gain the sources' cooperation. The development of approach strategies permits HUMINT collectors to practice approaches that have a good chance of success before they actually meet the source. I refer to this as "rehearsal." It allows leaders to mentor and evaluate their subordinates on their techniques.

Quite often, collectors discover that different source types are susceptible to the same approach technique. However, the collector must orchestrate different approach strategies (or methods for employing that approach). For instance, the collectors may determine that members of a particular insurgent organization and a group of displaced persons are both susceptible to the "fear up" approach. While both are susceptible to the same approach, it is important for the collector to comprehend the basic underlying reasons why the insurgents and refugees are afraid. In this sense, the collector selects the same approach but must orchestrate each approach differently.

During the Gulf War, Iraqi soldiers were afraid of the U.S. soldiers. Specifically, their leaders informed them that if they were captured, the U.S. personnel would execute them. Additionally, Kurdish refugees who inhabited the refugee camps on the Turkey-Iraq border also had a fear—they were not afraid that the U.S. solders would execute them but that if they were forced to return to their cities, they would again face Sadam Hussein's persecution and devastation. Obviously, a collector who intends to talk to these source types would have to orchestrate carefully the different approach strategies. Although organize approaches appears redundant, senior collectors must resist the temptation to cut out this important final step as it provides closure to the process and serves as the end product.

Conclusion

HUMINT collection operations are an invaluable asset and an essential tool in the intelligence cycle. However, unlike other intelligence collection systems, the behavioral and cultural variables inherent in a specific society greatly influence these operations. HUMINT analysis provides a means to deal with these variables. Collectors' abilities to understand the sources, their behaviors, attitudes, and the environment will determine the effectiveness of their collection operations. Source profiling is one method that supports tactical mission planning and the successful implementation of HUMINT and CI methodologies.

References

Headquarters, Department of the Army, **FM 34-52**, **Intelligence Interrogation**, 28 September 1992.

U.S. Army Intelligence Center and Fort Huachuca, **ST 2-22.7**, **Tactical Human Intelligence and Counterintelligence Operations**, April 2002.

Headquarters, Department of the Army, **FM 34-2**, **Collection Management and Synchronization Planning**, 8 March 1994.

Appointed as a Warrant Officer in 1993, Chief Warrant Officer Three Gregory Garcia is currently the Course Manager for the Warrant Officer Basic Course Phase I and the 351E certification track in the 304th MI Battalion at Fort Huachuca, Arizona. His prior assignments include Regimental HUMINT Technician in the 66th MI Company, 3d Armored Cavalry Regiment; Interrogation Operations Officer in Charge in the 125th MI Battalion, 25th Infantry Division (Light); Group Interrogation Technician, 10th Special Forces Group (Airborne); and Translator/Interpreter, 1st Psychological Operations Battalion, Special Operations Command (Airborne). Readers may contact CW3 Garcia via E-mail at gregory.garcia@hua.army.mil and telephonically at (520) 533-3479 or DSN 821-3479.

LANGUAGE TOOLS

(Continued from page 28)

tools is the language itself. We must develop assistance packages for each language individually, a very labor-intensive and time-consuming task. Some of the lower-density languages in critical demand by the Armed Forces today have no translation programs at all. Because these languages are not commercially viable, it is up to projects like LASER to fund and nurture these programs to a usable level.

As LASER enters the second year of its five-year run, the pace of activity will only increase. We will thoroughly test and evaluate the upgrades and enhancements to current projects as well as new developments during Military Utility Assessment (MUA) exercises. During these exercises, soldiers will use the equipment exactly as they would in wartime, giving the product a thorough testing before it is accepted for deployment into the Army inventory. Sometimes, though, real-world events can overcome the timeline for evaluation. In a perfect world, we would like to run all of our products through a full exercise schedule but when we have a product that can help a soldier complete his or her mission, we will get it to them immediately.

VISualization of Threats and Attacks (VISTA) in Urban Environments

by Frederick J. Diedrich, Kathleen M. Carley, Jean MacMillan, Keith Baker, LTC Jerry L. Schlabach, and LTC J. Victor Fink

VISualization of Threats and Attacks (VISTA) in Urban Environments. Traditionally, the military intelligence analyst has been able to focus on a known enemy within situations that are relatively comprehensible. Uniforms, military vehicles, equipment, and communications patterns, to name a few, could identify the enemy and help to clarify the situation. The natural terrain shaped maneuvers and gave the analyst a framework to view the battlefield. Predicting the enemy's course of action, while never easy, could at least be attempted using traditional Major Theater of War (MTW) terrain analysis tools.

Today there is a new battlefield and a nontraditional enemy. Although this was true before 11 September 2001, the events of that day have put this challenge at the very center of our national military policy. Intelligence analysts must face an enemy that does not use a standard uniform, does not travel in military vehicles, and does not use the natural terrain exclusively. Many of the battles of today and of the future will be fought in urban environments—populated areas filled with objects constructed by humans.

The complexities of such urban environments create a variety of challenges for the military analyst. These complexities were apparent, for instance, during the summer of 1999 when North Atlantic Treaty Organization (NATO) deployed a multinational military force, known as the Kosovo Force (KFOR), into the city of Pristina, the capital of Kosovo, to bring peace to the warring factions and end ethnic cleansing by the Serb Army. Upon entering the city, KFOR faced a multitude of problems that included, but were not limited to—

- The mass movement of ethnic Albanian and Roma refugees.
- Newly displaced Serb civilians.
- An active international humanitarian community.
- Armed combatants comprised of the Serb military and the Kosovo Liberation Army.

Faced not only with the task of quickly grasping the "on-the-surface" situation, intelligence analysts soon realized they also needed to provide their commanders with an understanding of Pristina's "landscape"; an urban intelligence preparation of the battlefield (IPB) that assessed communications and social networks, the "tempo" of the city, and the major perceptions and predispositions of its inhabitants. While a large volume of information was available to these analysts, trying to understand how seemingly unrelated events might combine to create the next catastrophic event was nearly impossible. For example, how would they assess the return of displaced ethnic Albanian refugees to their homes? Besides ensuring that the combatants were identified and isolated, they needed to consider environmental factors such as weather, available power and drinking water, movement constraints from destroyed roads and emplaced minefields, and the composition and attitudes of the refugee group. Likewise, it would have been problematic to understand the relative impact of inserting friendly forces at various locations. In short, it would have been difficult, if not impossible, for an analyst using the tools available then to fully understand the potential for seemingly unrelated conditions to cascade into significant events.

Much of this problem remains today. What is needed is a system that promotes understanding through visualization and analysis of the sudden, nonlinear, emergent events that characterize complex systems like operations in urban settings. In one sense, the problem is much like trying to understand and visualize severe weather events such as tornadoes that depend on a myriad of interrelated factors. Although the weather remains a complex problem, it is increasingly possible to predict the likelihood of a tornado within a certain time and vicinity. In other words, it is possible to determine when "conditions are right." Similarly, what is needed for military analysts is a system that enables the determination of when "conditions are right" for emerging threats. Given a certain set of conditions–and a way to visualize the consequences of multiple interacting factors–an analyst may be able to "forecast" possible scenarios.

Note, however, that the urban problem differs from the weather problem in at least two important ways. First,

unlike the weather, the urban situation can be influenced (for example, by inserting forces in particular locations, the chance of future threats may be altered). Second, the urban situation is purposively dynamic (for instance, the actors are constantly adapting). Over time, the "landscape" of the urban operational setting changes and, consequently, the likelihood that "conditions are right" changes as well. In the KFOR example, some Serb Army garrisons, weapons cache sites, and government municipal buildings have since been taken over by Albanian and United Nations organizations–radically changing the landscape. To cope with this complexity, the analyst needs a tool that enables visualization of potential outcomes given hypothetical conditions and probable changes. One such tool is now under development.

Under an (SBIR) contract with the Army Research Laboratory, Aptima©, Inc., is currently working with the Center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University to design a prototype tool for VISTA in urban environments. The U.S. Army Battle Laboratory and TRADOC Systems Manager All-Source Analysis System (TSM ASAS), Fort Huachuca, are providing subject matter expertise. Ultimately, the tool promises to facilitate "forecasting" of potential events by enabling exploration by manipulation of conditions. By enabling exploration of various actions and outcomes, the system will allow an analyst to visualize the types of events that are possible, the likelihood of those events given certain conditions, and ways to maximize the likelihood of certain types of outcomes.

The VISTA Model. The VISTA model is based on complex systems theory, sometimes referred to as the science of chaos, which is a perspective for conceptualizing nonlinear dynamical systems.[1] Complex systems are typically characterized by a large number of interacting elements that combine to produce emergent behavior–the behavior is not prescribed ahead of time, but rather, arises from interactions between the system components (self-organization).

Multi-agent models are often used to examine adaptive behavior in complex systems.[2] Multi-agent models represent system components as agents that interact. For instance, in the area of intra- and inter-organizational dynamics it has been found that the coupling of multi-agent models with networks leads to a powerful toolset for growing and analyzing the complex behavior of diverse entities.[3] Using a multi-agent network approach it is possible to describe and predict potential emergent properties for networks of friends and enemies such as those that one is likely to encounter in an urban or counter-terrorism situation.[4]

In particular, the VISTA model rests on a multi-agent network approach[5] that incorporates multiple interacting and adaptive elements (agents) that represent enemy entities and different regions of a given city. Each city sector agent reacts to events depending on its characteristics, history of having been threatened, and its connectivity with other regions. The enemy agents generate threats and respond to the city sectors depending on their characteristics, history, and connectivity to other enemy agents. The model focuses on how these agents, friend and foe, interact and learn. System behavior emerges in a self-organized fashion from this interaction.

Figure 1 shows the conceptual framework for the model, which specifies at a high level how the system works. There are several key components to VISTA:

- A database with background information on historical events related to urban operations (Historical Database). These events will include information on incidents like those in Hue City, Mogadishu, and Kosovo.
- A database containing information on the city being evaluated, both in general and by region or sector within the city (City Database). This will include information such as the size of city, population density, poverty levels, and locations of key infrastructure, based in part on categories of information addressed in items such as FM 3.06, [Urban Operations], [6] and MCIA-1586-005-99, [*Urban Generic Information Requirements Handbook*], [7] This database and the historical database will focus on critical aspects of urban operational environments that can feasibly be captured in the model.
- A database containing information on typical threat and non-threat agent characteristics (Enemy and other Players Database).
- The City Threat Evaluator that judges the likelihood of a threat and its potential severity by relying on data about the city of concern, including items such as the physical, political, economic and demographic layout, as well as social structure characteristics (as captured in the above databases). Similarly, for each sector (region) in the city, the system uses sector level characteristics and threat agent characteristics as captured in the databases. Based on this collective input, the city evaluator uses a multi-agent network engine to predict the potential for threat on each sector by each enemy for different types of threats (for example, bombings, riots, assassinations).
- The Future Event Evaluator that is used to ask "what-if" questions about specific events of interest, either friendly actions such as the movement of troops or aircraft, or possible actions

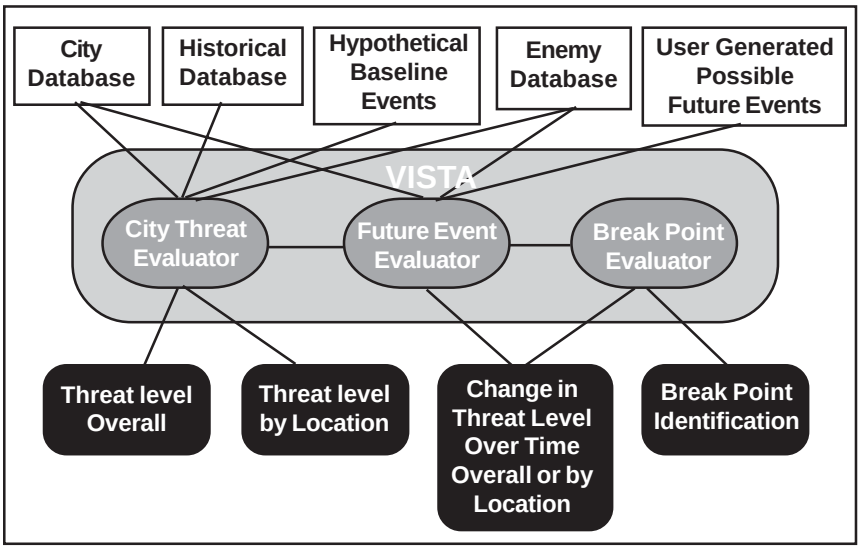


Figure 1. Conceptual framework for the VISTA system.

that are not under friendly control, but are considered likely enough to be of concern (for example, the explosion of a bomb in a populated area). The analyst specifies possible future events, and based on the complex interactions, this module predicts dynamic changes in threat level by time and location, based on the time and location of the events specified by the analyst. The Future Event Evaluator consists of a multi-agent network that uses data on the city in question, a set of hypothetical events, and the historical database to initialize a set of agents who then proceed to act out possible future threat scenarios. Threats and responses to those threats are "grown" as agents, friend and foe, which continue to interact. The model uses an analytic technique to produce results that are statistically analyzed to evaluate the likelihood and severity of threat given a particular scenario, both by geographical location and over time. These agents are dynamic in that they learn, adapt, and respond to other agents. The output of the system reflects the patterns that emerge from the interaction of these agents and represents the likelihood of attacks.

- The Break Point Evaluator will run a variety of "what-if" analyses and determine the relative impact and likelihood of different threats under different response conditions. This aspect of the system will provide the possibility of surprise by threat and weakness by threat mapping, thus creating the ability to systematically explore and represent classes of different actions, events, and outcomes. As a result of this analytic function, the commander's staff will be able to identify and wargame friendly courses of actions (COAs) that best neutralize threat actions and constructively reshape the actions of non-threat players such as international charities.

Ultimately, the system parameters and output will be tuned to data on real-world equivalents to ensure realistic estimates and processes, and the system will be tested against known data from historical events of interest (for example, those in Pristina). Model elements will support a wide range of "what-if" analyses that reflect the complexities of urban environments and that enable forecasting of when "conditions are right" for emerging events.

The VISTA Visualization Tool. The two primary modes of use for the VISTA tool will be data entry and threat analysis. A user might perform data entry when there is a need to add a new city, a need to modify parameters reflecting certain city sectors, or a need to change the overall characteristics of a city. Within threat analysis, the VISTA tool will provide guidance in a variety of ways. First, the analyst will be able to explore the likelihood of threats in various sectors of the city or overall.

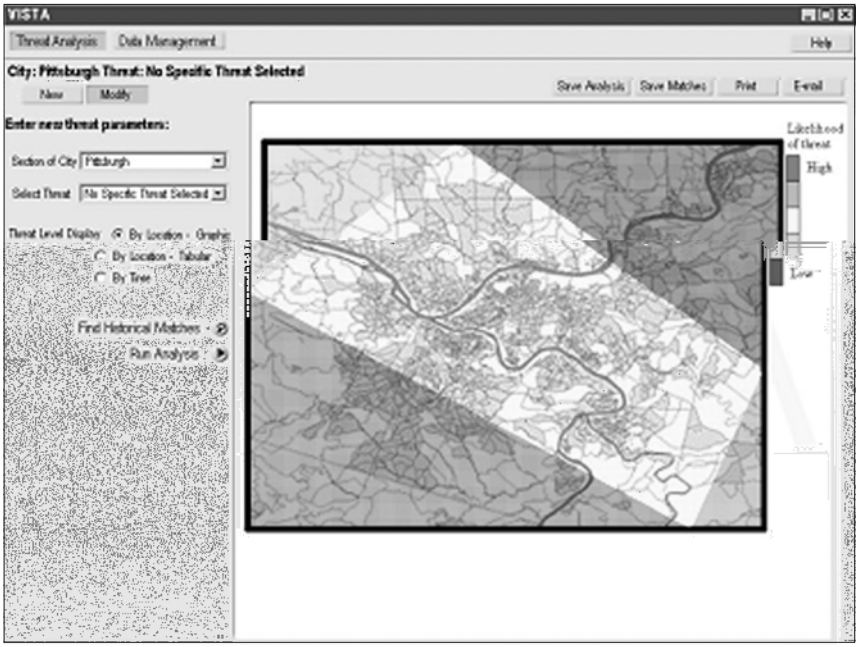


Figure 2. Prototype of the VISTA visualization tool showing threat analysis by city sector where color represents the likelihood of threat.

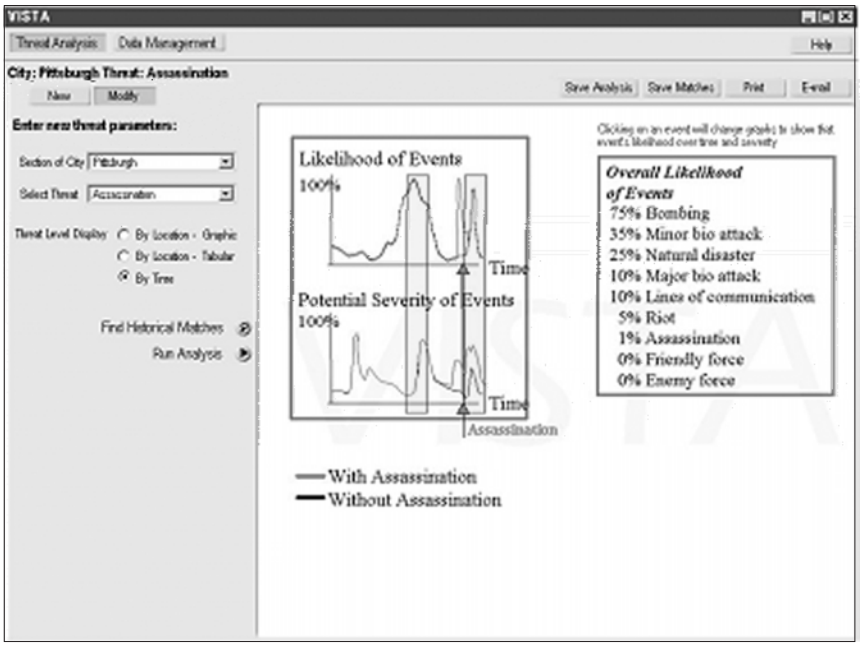


Figure 3. Prototype of the VISTA visualization tool showing threat analysis by time reflecting the consequences of a hypothetical assassination leading to increased threat levels.

Second, it will be possible to use VISTA as a "what-if" decision aid to think through the possible consequences of various types of attacks, actions, or events. This corresponds to interaction with the Future Event Evaluator. Third, with VISTA the user will be able to create an overall map of the relative impact of different types of events (via the Break Point Evaluator).

Taking the example of a threat analysis, Figures 2 and 3 show the types of output and interfaces that will ultimately be available to intelligence analysts using the VISTA tool. In Figure 2 results are displayed graphically by overlaying different colors, corresponding to different threat levels, on the city. In this hypothetical case, the southwest region shows the highest levels of threat, thus supporting rapid identification of problem regions.

Figure 3 shows output over time, presented as a time series (black line). This example illustrates the output of a "what-if" analysis involving a hypothetical assassination leading to shifts and elevations in threat levels over time (the red trace). The system specifies the relative likelihood of different types of events, thus supporting the visualization of a variety of possible outcomes.

Conclusions. VISTA can be thought of as a "social-infrared" system for visualizing the urban battlefield. It is a computational system for forecasting and visualizing the potential threat on complex urban environments. Like night-vision goggles, VISTA will use an underlying model to make visible threats that might otherwise remain hidden by the opacity of the complexity inherent in urban environments. System predictions will reflect the patterns of interaction among the agents in the model that will be based on data about the characteristics of the city sectors and enemies in question. Of course, given the nature of complex systems, the VISTA tool will not enable the precise prediction that a particular type of attack will occur at a certain time and place. Nevertheless, the VISTA system will enable the "forecasting" of conditions and the exploration of possible outcomes given certain events and actions.

TSM ASAS has already begun investigations to determine the appropriateness of integrating a VISTA-like capability as a module within the ASAS-Light, which is a tactical intelligence analysis system that operates on a lightweight, portable workstation. KFOR is currently testing an upgraded ASAS-Light that begins to provide analysts a basic toolset optimized for conducting non-traditional intelligence threat analysis. This initial tool advances IPB and the management of intelligence, security, and recon (ISR) in a stability or support environment. The next step, however, is to leverage COA development models that not only facilitate deeper visual insight but also prompt rapid, decision-focused analysis. Thus, the combination of ASAS-Light and VISTA will result in a powerful and cutting-edge analysis suite that will help analysts to focus collection and track asymmetrical threat factors with greater specificity.

Endnotes

1. Prigogene, I., & Stengers, I. (1984). *Order out of chaos: Man's new dialogue with nature*. New York: Bantam.

Waldrop, M. M. (1992). *Complexity: The emerging science at the edge of order and chaos*. New York: Simon & Shuster.

2. Carley, K. M. (1991). A theory of group stability. *American Sociological Review*, pages *56*, 331-354.

3. Carley, K.M., Lee, J.S. and Krackhardt, D. (2001). Destabilizing Networks. *Connections,* pages *24*, 31-34.

4. Ibid

5. Carley, K.M. (1999). On the Evolution of Social and Organizational Networks. In Steven B. Andrews & David Knoke (Eds.), *Research in the Sociology of Organizations: Networks In and Around Organizations*. JAI Press, Inc. Stamford, CT.

6. United Sates Army. (1979). *Military Operations on Urbanized Terrain*, FM 90-10.

7. Marine Corps Intelligence Activity. (1998). *Urban Generic Information Requirements Handbook,* MCIA-1586-005-99.

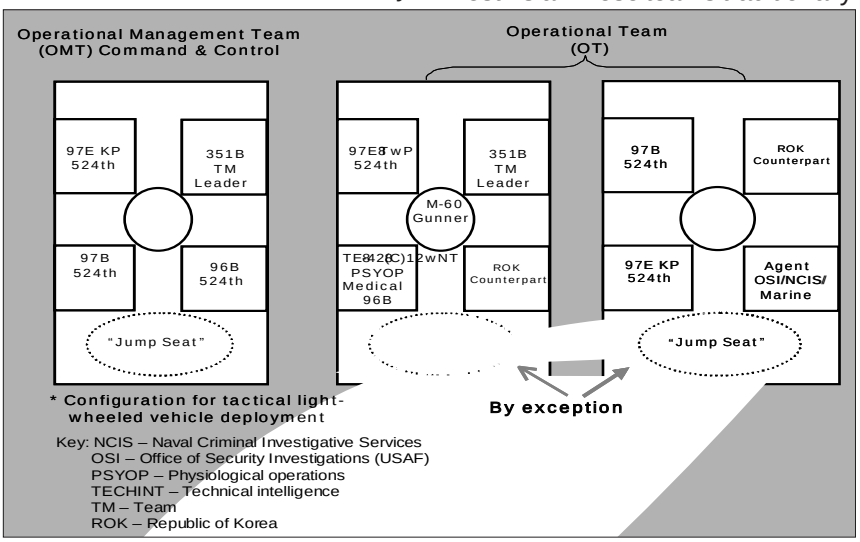
Carley, K.M. (2002), "Intra-Organizational Computation and Complexity." In J.A.C. Baum (Ed.), *Companion to Organizations*. Blackwell Publishers.

Combined Go Team Transformation in the Republic of Korea

by Captain Alan G. Rogers

Transformation—the core of the Army Chief of Staff's initiative to redefine the way our Army will meet future challenges—is driving military intelligence visionaries to rethink our current force modernization and force structure in the continental United States and abroad. Recent Army methods has evolved into the combined tactical "Intelligence Go Team" concept.

Admittedly, the concept of Go Teams is not a unique one. Army CI/HUMINT teams have deployed to various locations across the globe, from Bosnia-Herzegovina and Macedonia to Thailand and Southwest Asia. These teams traditionally deploy with a warrant officer as the team leader, a noncommissioned officer (NCO), and a small "slice" of CI agents; required linguist support comes from organic HUMINT collectors or Defense Language Institute-trained CI agents. However, the 524th MI Battalion is experimenting with the next logical progression: fully combined Go Teams (see Figure 1). The augmented team will contain its full contingent of U.S. Army CI agents and HUMINT collectors, but will also include their Republic of Korea (ROK) counterparts. The intent is to integrate wartime CI and HUMINT operations fully into the combined campaign plan. The hope is that this broader, combined effort will provide a more complete picture of the battlespace.



…perations
…al Team.

counte
intelli
Kore
trine
fyin …ys to
furnis …rmation
to thea… …ers.

The 524th Military Intelligence (MI) Battalion provides operational CI and HUMINT support to the Korean theater of operations. Subordinate to the U.S. Army Intelligence and Security Command's (INSCOM) 501st MI Brigade, the 524th Headquarters and Headquarters Company and its two operational line companies have the mission under armistice and in wartime to supply timely CI and HUMINT support to the theater's warfighters. One of the Battalion's transforming

Photographs courtesy of Captain Alan Rogers

Camp Humphreys MI Detachment (B/524th).

Go Team member with equipment.

tive area of operations. The MIDs conduct the full spectrum of the CI and HUMINT mission:

- Robust liaison program with our ROK counterparts.
- All personnel security investigations.
- Threat statements and assessments coupled with conducting security awareness briefings.
- CI investigations and force protection (FP) reporting.

In wartime, the MIDs continue their FP mission but take on an additional responsibility of deploying integrated tactical CI-HUMINT Go Teams in support of the three Republic of Korea Army (ROKA) commands. The 524th MI Battalion command and ROK-U.S. combined staff planners developed the Go Team concept jointly to better meet the mission capabilities required by the theater operations plan.

The South Korean Peninsula comprises three distinct military areas. The First ROKA (FROKA) and Third ROKA (TROKA) cover the northern area while the Second ROKA (SROKA) covers the combined rear area. The Capital Defense Corps is responsible for providing coverage to the greater Seoul area where more than 25 percent of the Peninsula's citizens reside. The 524th MI Battalion's operational line companies strategically align with their respective ROKA counterparts. Over the past year, the Battalion has successfully validated the tactics, techniques, and procedures of this transforming Go Team vision in a proof of concept demonstration in April 2001. That Ulchi Focus Lens (UFL) exercise demonstrated a robust combined, Go Team operation across the entire Peninsula further validating the Go Team vision.

Figure 2 depicts the architecture of the Battalion's Go Team. The Team is a CI-HUMINT incident response element that can deploy on short notice from its MIDs located across the Peninsula. The teams are tailorable to meet different mission requirements and deploy rapidly to any threat area. When a terrorist or Special Operating Forces (SOF) incident occurs on the Peninsula, the Combined Forces Command (CFC) CI-HUMINT control element will notify the Brigade and subsequently the Battalion to deploy a Go Team to a given location where the team would link up with its ROK counterparts. Within a short period, the designated MID can supply a rapidly deployable Go Team in support of the operation.

Once the Operational Team (OT) arrives at the incident site, the team members quickly set up security, assess the on-the-ground situation, set up the CI/HUMINT Automated Tool Set (CHATS) and provide timely information to the Operations Management Team (OMT) cell via satellite communications (SATCOMs). The SATCOMs give the OT the capability to transmit and receive spot reports via both secure and unsecure means. Perhaps the most significant feature of the 524th MI Battalion's Go Team is that they require no external power source to conduct satellite and CHATS operations. Each team has commercial-off-the-shelf (COTS) generators that run for a long time and quietly for extended operations. The Team quickly and easily transports this equipment in a small suite of transit cases.

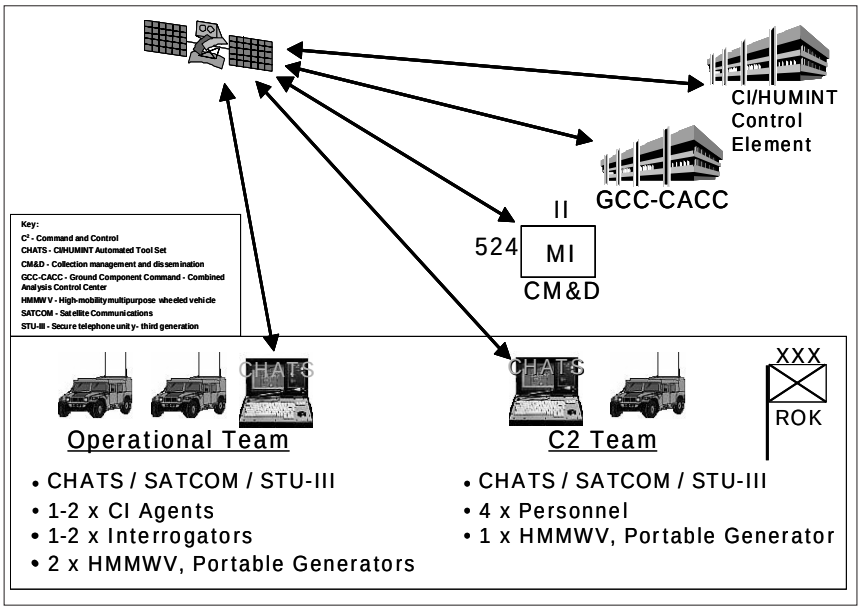


Figure 2. Go Team Architecture.

The OT transmits its spot reports to the next higher echelon. That echelon, the OMT—which usually colocates with a ROK command and control center (CCC)—then transmits the spot report traffic to the Company Operations Cell via the same SATCOMs architecture. They, in turn, quickly transmit the information to the theater CI and HUMINT control element and the Ground Component Command-Command and Control Center (GCC-CACC), The theater CI and HUMINT control element disseminates the information electronically to a myriad of tactical intelligence and operational consumers.

During UFL 01, the C2 of the CFC asked the Battalion to expand its Go Team configuration by an additional layer. While an OMT deployed to a specific ROK division headquarters, another element—the Combined Counterintelligence Section (CCIS), deployed to a ROK corps headquarters. The ROK 9th Corps Commander, Lieutenant General Cho, Young-Ho, recently articulated during UFL his pleasure that U.S. MI was working hand in hand with the ROK Army. He said that the Korean and U.S. assets "*provided a combined intelligence capability that could not be broken.*" Lieutenant Colonel David J. Clark, Commander of the 524th MI Battalion, echoed the same sentiments saying that it is critically important that the 524th remains at the "tip of the spear" in identifying creative ways to work with our Korean allies.

As the Battalion continues to train to its tactical Go Team concept, its future focus will include continued integration of Reserve Component WARTRACE[1] augmentation into the theater's CI and HUMINT architecture, as well as continuing with faster innovative methods for transporting Go Teams to hot spots on the Korean Peninsula (such as through sling-load operations—see the photographs). The early Spring 2002 Foal Eagle (FE) and Reception, Staging and Onward Integration (RSOI) exercise will provide yet another forum for CI and HUMINT elements to identify creative ways to meet the Brigade's goal in providing timely, accurate, and predictive intelligence to the theater's warfighters. By transforming for these future operations, the 524 MI Battalion pledges its commitment to the MI Corps motto—ALWAYS OUT FRONT!

A/524th MI Batalion soldiers practice sling-load operations with 17th Aviation Brigade to enhance the rapid response capability of the Go Teams.

Endnote

1. The WARTRACE Program aligns, organizes, and integrates Active and Reserve Component (AC, RC) Army units under wartime gaining commands. It provides units with detailed information concerning their wartime missions.

Captain Alan Rogers is currently serving as the Commander of Bravo Company, 524th MI Battalion, in the Republic of Korea. CPT Rogers served as the Squadron S2 of 1-6 Cavalry, Camp Eagle, Korea. He has a Master of Business Administration degree from the University of Phoenix, and a Bachelor of Liberal Arts degree from the University of Florida. He has attended the Combined Arms and Services Staff School, the Military Intelligence Captain's Career Course, and the Army's Counterintelligence Course. Readers can reach him at rogersa@seoul-501mi.korea.army.mil.

MASINT

(Continued from page 34)

technology advances that have occurred since the fielding of the original REMBASS and the AN/PPS-5/15 radars were fielded. However, it is something that must happen if we are to gain dominance in this arena. The quality of our soldiers and current technology allow the Army unparalleled opportunities to exploit, in real time, battlefield information that in the past has gone unused. Furthermore, processing techniques will enhance our ability to identify battlefield entities at the sensor and chip capacity will solve huge data storage and manipulation problems of the past. Power management techniques have extended the life of collection systems extraordinarily. Display technology has greatly enhanced the utility of MASINT collection. Our challenge is now to develop the materiel, training, and force structure requirements necessary to exploit this capability. The Army's intelligence leadership has taken the initial steps towards using MASINT in the tactical Army. Now it's up to the rest of us to bring the concept to life.

Bill Moore is a former G2 and battalion commander and is currently a Department of the Army Civilian in the Concepts Division, U.S. Army Intelligence Center and Fort Huachuca. He wrote this article while employed by a contractor in support of the MASINT Requirements Team, USAIC&FH. Readers can contact him via E-mail at william.moore@ hua.army.mil and by telephone at (520) 533-7212 or DSN 821-7212.

Civilians on the CTC Battlefield—Threat, Opportunity, or Distraction?

by Captain Matthew J. Morgan

Civilian presence in the area of operations (AO) is an important factor in visualizing the battlefield and one that we occasionally overlook. The Center for Army Lessons Learned (CALL) reported that *"little thought is given to intelligence collection from…civilians on the battlefield*" in Afghanistan.[1] Following three visits to Fort Polk, Louisiana, last year, I was impressed with the realistic integration of civilian role-players enriching the battlefield scenario at the Joint Readiness Training Center (JRTC). These visits provided me with the opportunity to make a number of observations that I wish to share. I hope they will be useful for military intelligence (MI) professionals both in the regular combat training center (CTC) training challenge and in the small-scale operations that are more common in today's Army. They form the basis of JRTC's small-scale contingency (SSC) experience. After learning about JRTC's practices and lessons learned from an intellectual viewpoint at Fort Polk's Leader Training Program, I was able to see JRTC from the "inside out" as an opposing force (OPFOR) augmentee before returning on my unit's regular "Blue Force" (BLUFOR) rotation. These experiences helped me understand the integration of civilians on the battlefield (COB) and how some units do not sufficiently prepare for this aspect of an operation.

Civilians as Threats

Civilians can play several operationally significant roles. They are perhaps most importantly a threat. At JRTC, civilian-clothe's OPFOR act as members of the Leesville Urban Group (LUG), a low-level insurgency group that provides intelligence across the battlefield and conducts small-scale raids or demolitions. Traveling across the "box" during the day, the LUGs are able to identify BLUFOR high-payoff targets early in the rotation. Without incriminating identification or other indicators, the LUGs blend with other civilians on the battlefield who have a real-world need for access to the lines of communication because they have a finite workday and do not stay in the "box" overnight. The LUGs also leave the box, returning to the OPFOR headquarters where they are debriefed and given new assignments. Especially in the SSC phase of operations, preventing civilian insurgents from accomplishing their reconnaissance and surveillance mission becomes very important. Failing to stop them leaves the OPFOR tactical operation center (TOC) with a complete picture of the enemy (BLUFOR) disposition with a minimal expenditure of collection effort.

Photograph by Sergeant Todd M. Roy, U.S. Army.

Sergeant Mark Pelaez and Specialist Robert Bergdorf broadcast crowd control messages using a loudspeaker while soldiers from A Company, 3-187th Infantry, 101st Airborne Division (Air Assault), maintain security and conduct a sensitive site exploration in the eastern central Afghan village of Hesarak, outside Kabul. The mission is part of ongoing operations in support of Operation ENDURING FREEDOM.

Civilians Provide Opportunities

Civilians can present an opportunity in this counterintelligence (CI) endeavor. This would first presuppose the success of the civil affairs (CA) and psychological operations missions. Failure to win the support of the populace would for the most part preclude their positive involvement in the collection effort. However, if the locals want to help, they would probably be good sources of information on civilian-clothe's enemy as well as uniformed OPFOR. Another concern that must arise is the prospect of neutral or unaffiliated civilians transforming into threat collection assets. Averting this problem should be a joint responsibility of CA and CI.

Challenges in Exploiting COB

One problem with the exploitation of civilian opportunities is the limited amount of available collection assets. The devotion of human capital to collection and organization of information on and from the local populace may have a low payoff. On the other hand, current and future operations may already provide overwhelming tasks. This is also true for operations and command channels. Commanders, executive officers, or other important leaders with pressing demands can allow themselves to become embroiled in civil-military relations concerns that lower levels should ultimately resolve without difficulty. Unfortunately, the opposite may also be true—critical events may hinge on CA, requiring the experience and authority of senior leaders for their positive resolution. This dilemma resembles the problem facing MI professionals. When is it worth the effort? What constitutes battlefield intelligence and answers to the commander's critical information requirements (CCIR) versus what comprises information overload is a sensitive delineation.

Photograph by Specialist Marshall Emerson, U.S. Army.

U.S. Army Major Dave Young of the 401st Civil Affairs meets with a village elder to discuss villagers' concerns during Operation Mountain Sweep.

Assessing the COB

Circumstances will suggest whether a need exists to involve civilians in a collection plan based on the "read" of the enemy's intent and operations. If the threat is staging operations from a local population center, then of course civilian intelligence sources would be more critical. Similarly, in SSC or support operations and stability operations, civil-military concerns have a higher priority. However, in cases where there is no reason to suspect that enemy operations are in the vicinity of a population center, or if preparations of high-intensity conventional operations are underway, then civilians have the potential to become a significant distraction. This distraction can consume valuable planning time and temporarily remove essential staff and leaders from the operation. Under such circumstances, operational channels should focus on appeasing any CA concerns of civilian officials as expeditiously as possible while intelligence channels should focus on protection of essential elements of friendly information (EEFI). Figure 1 illustrates the changing possible operational impact of civilians across the spectrum of operations.

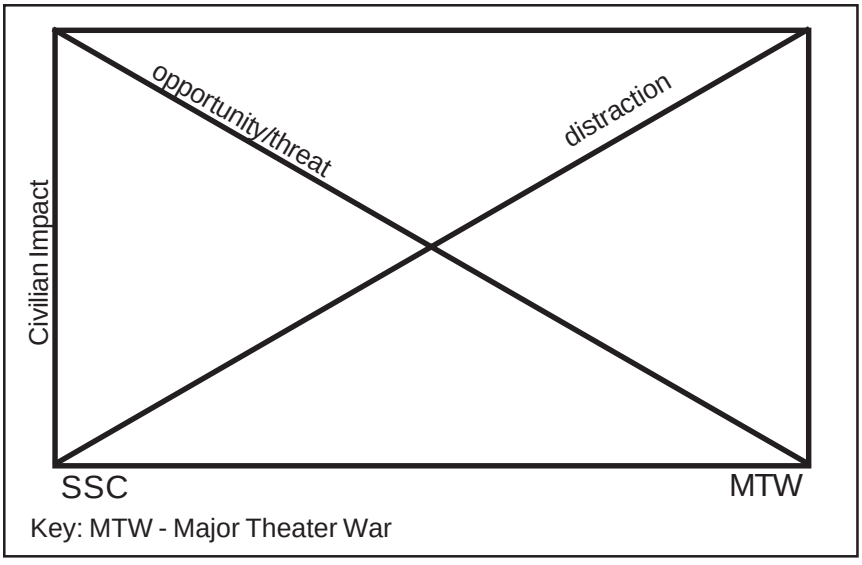


Figure 1. COB impact Depends on the Level of Conflict.

In developing a useful visualization of the battlefield, it will also be productive to consider collection and analysis methods to address the threat and opportunity offered by COB. What analysts must remember is that we may receive quite a lot of information that is of little intelligence value. Therefore some S2s at the battalion task-force level may not find it worthwhile to pursue collection and analysis efforts on COB. What exacerbates this problem is that all **relevant information** may not reach a battalion S2 staff trying to develop the civil-military affairs situation. Other battalions may not track or report the information if it is not a priority for them, resulting

Photograph by LT Scott Hocutt, Assistant S1, 3/4 Cavalry.

The Aviation Task Force occupied Self Airfield for the last phase of JRTC Rotation 01-01; here the commander is negotiating with the villagers. They were led by the village mayor and owner of the airfield. He was upset with us for "ruining the beautiful lawn in front of the court house and for the noise from the helicopters."

in the intelligence work done by the brigade combat team's (BCT) human intelligence (HUMINT) assets never reaching the battalion staffs. With its larger staff and wider-ranging collection assets, the BCT S2 element may be able to implement these techniques better than the battalions.

We have already developed pattern-analysis wheels, association matrices, and other tools in conjunction with SSC scenarios where people can be "key terrain." However, the information they provide may not be adequate to meet the challenge in the CTC environment. For instance, if the JRTC's LUG is locating high-payoff targets during the day and conducting terrorist attacks at night, pattern analysis would assist the S2 in advising the commander on the times during which crucial assets will be most vulnerable to threats. However, a form of pattern analysis that connects people, events, and locations would be of even greater value. For example, we could identify the pickup truck containing two or three men (with military style hair cuts) that observes friendly critical assets during the day by associating the identification of people (the suspicious pickup truck), activities (inconspicuous drive-by observation), and locations (high-payoff targets). In addition to the analysis effort, this association would require alert collection on the part of security forces as well as effective communication between the units across the battlefield. Additionally, tracking organizations as well as individuals on the association matrix may help intelligence professionals determine who is contributing to the threat. All of these efforts obviously require the support of available CI and HUMINT assets as they conduct CFSO (CI force-protection source operations) development.

Conclusion

Civilians on the battlefield are well integrated into the CTC scenarios, and this realistically represents the importance of civil-military considerations in contemporary and future U.S. Army operations. As MI professionals, we must be able to react to this aspect of the battlefield for which conventional models may not adequately account. This will require a broader visualization of the battlefield than conventional tactical intelligence customarily provides. Recognizing the threat, opportunity, or distraction that local citizens represent is necessary to the intelligence professional.

Endnote:

1. Center for Army Lessons Learned (CALL), **Operation Enduring Freedom Tactics, Techniques, and Procedures Handbook**, Number 02-8, 27 June 2002, from the section on the Intelligence battlefield operating system (BOS) in military operations on urban terrain (MOUT).

Captain Matt Morgan is currently serving as the S3 Operations Officer for the 125th Military Intelligence Battalion, Schofield Barracks, Hawaii. He has served as the Assistant S2 of 3d Squadron, 4th Cavalry Regiment and as a Collection and Jamming Platoon Leader and Company Executive Officer in the 125th MI Battalion. Captain Morgan holds a Bachelor of Science degree in Management from the U.S. Military Academy and a Master of Education from Chaminade University. Readers may contact him via E-mail at morganmj@schofield.army.mil and telephonically at (808) 655-8204.

Evaluation of the Enemy Situation
The Role of the G2 in the German Military Decision-Making Process (MDMP)

by Rob Trabucchi

The views expressed in this article are those of the author and do not reflect the official policy or position of the U.S. Army, Department of Defense, or the U.S. Government.

***Note**. Although the term "Bundeswehr" encompasses the entire armed forces, I will use it here in reference only to the German Army. To keep this simple, I generally use U.S. Army doctrinal terms to describe their German counterparts when they are sufficiently alike.*

Introduction. Getting "back to basics" now and then is important in any profession. It provides perspectives with which we might have lost touch in the day-to-day grind of non-mission taskings and other distractions. Such a perspective reminds us of the essential tactics, techniques, and procedures (TTP) which we learned the hard way. Another perspective is to compare our own TTP with those used by other military powers. This comparison can provide enormous insight into our strengths and weaknesses as well as provide us with a rare outlook from abroad. Although we frequently debate various aspects of our own profession and processes, we often do so completely from within the limits of our own experiences. Comparing our TTP to those employed elsewhere offers us the opportunity to identify new lessons learned. It is my hope that the comparison of the Military Decision-Making Processes (MDMP) and the role of the G2/S2 sections in the U.S. Army and the German Bundeswehr will be enlightening and maybe even interesting!

The Environment. We can all agree that getting a handle on the "big picture" before diving into the details is essential to understanding any situation. On that note, just a bit of relevant background on the Bundeswehr.

First and most central, there is no professional Military Intelligence (MI) Corps in the Bundeswehr. This should pique our interest as a profession because it focuses on the often-debated issue of whether or not professional MI officers are needed at the battalion and brigade levels. We know and understand the place and mission of the S2 within the U.S. Army's combat battalions. This situation is very different within the Bundeswehr where the S2 position is often given to a young Lieutenant who may not have had much (or any) experience as a platoon leader, certainly none as a company commander. One might argue that U.S. battalion commanders would never do this because they respect the need for good tactical analysis too much. That respect, however, comes in part from the existence of a professional MI Corps that gains institutional experience over the span of careers that are focused on the intelligence business. Further, the U.S. Army MI officer develops related TTP, incorporates this experience into doctrine, and then teaches that doctrine in order to improve the entire profession and lay a foundation for the cycle to continue.

In the Bundeswehr, some officers unofficially "specialize" in intelligence. Unlike the U.S. Army, this is generally a matter of personal preference and is not institutionalized or officially tracked by their personnel system. For those who choose to pursue multiple assignments in intelligence, there are a few professional courses that focus on specific intelligence issues, such as signals intelligence (SIGINT) collection. There is also the Bundeswehr's Strategic Reconnaissance Command where an officer can gain experience working with SIGINT, human intelligence (HUMINT), and some satellite-based imagery intelligence (IMINT) collection.

There is a limit, however, to an officer's ability to continue with purely intelligence assignments, mainly because the Bundeswehr's personnel system lacks any intent to promote a focused intelligence track. At the end of each tour, a German officer would have to maneuver himself into intelligence assignments. This is difficult because, by modified Table of Organization and Equipment (TOE), all intelligence positions (including brigade-level) must be filled by graduates of their highly competitive General Staff Course. Graduates of this course are among the top 10- to 15-percent of each year group and are also required for G3, G4, Chief of Staff, and Command positions. Their ideal career path includes service in each of these areas as well as on higher-level German and North Atlantic Treaty Organization (NATO) staffs. They seriously risk jeopardizing their careers if they attempt to work purely in the intelligence field.

Further reducing the influence of the G2 is the fact that tactical intelligence collection is conducted by a variety of units in different branches. SIGINT is executed by the Signal Corps while the Artillery fly unmanned aerial vehicles (UAVs) and drones. It is interesting to note that the German Army distinguishes between drones and UAVs; it uses drones for the G2 and UAVs strictly for artillery targeting. Although reconnaissance and other HUMINT assets support the G2's collection plan, Bundeswehr dispersion of collectors

throughout the many branches robs them of a community focused on providing intelligence. In fact, mottos like "Intelligence is for the Commander" are largely unheard-of in the German Army. The overall effect is profound at the noncommissioned officer (NCO) level, where there is no system to develop senior NCOs who have experience on G2 staffs and/or in intelligence units.

The second essential background element is that the German MDMP is designed to be "quick & dirty." The process focuses on the essentials of making a decision and not getting wrapped-up in detailed analysis. Timelines for staff estimates are compressed, with the Chief of Staff personally involved in order to facilitate rapid development of courses of action (COAs). The German system places strict time limits on briefings, and under combat conditions the G2/S2 (division to battalion) usually gets about 4 to 5 minutes in a situation update or COA decision brief. All staff members are taught to focus on "Recommendations" in their briefings; if the Commander wants background information, he will ask for it. Otherwise, a staff officer's recommendations are trusted as having been fully analyzed (and checked by the Chief of Staff before a briefing).

This system seems to work for the Bundeswehr, at least in exercises; its success is generally attributed to their adherence to *Auftragstaktik* (Commander's Intent or Results-Focused Orders), which grants maximum freedom of maneuver and decision to the subordinate commander. Such a system reduces the expectation of highly detailed and synchronized plans. Faithful adherence to the higher Commander's Intent is considered sufficient synchronization among subordinate and supporting units. This vastly reduces planning time because wargaming COAs, synchronization drills, and detailed intelligence preparation of the battlefield (IPB) are not part of their process.

There are other differences between the two armies. Within the Bundeswehr, deep operations are not conducted at the division level, and only rarely at the Corps level, again reducing the need for the level of synchronization to which U.S. forces are accustomed. It is another, much larger study entirely to determine the pros and cons of the Bundeswehr's system. For the purpose of this article, the reader should be aware that the detailed analysis by the G2, which U.S. commanders expect and which is required by the "intelligence drives operations/Commander drives intelligence" philosophy, simply does not occur.

The German Military Decision-Making Process. The following is a brief description of the G2 actions in each step of the German MDMP. These actions are based on what is taught at the General Staff Course and what students, instructors, and small-group tutors describe as common practice in the Bundeswehr. There is no specific MI doctrine, just a 10-page chapter in the document manual on the MDMP and Command and Control.

The Situation Update Briefing

- ❑ Purpose: To enable and initiate staff work and to inform the staff of the current situation. The situation update briefing is conducted as soon as possible if not immediately upon return from the higher headquarters operations plan (OPLAN) or operations order (OPORD) briefing.
- ❑ G2 Actions: The G2 regurgitates those elements of higher headquarters enemy situation report that are relevant to his own unit. Any analysis the G2 has conducted during the return to his own command post (or while awaiting arrival of the Chief of Staff if he did not attend, which is often the case) may be presented but extremely succinctly.

Situation Assessment Part 1

- ❑ Purpose: Equivalent to U.S. Mission Analysis.
- ❑ G2 Actions: Predict enemy plan for operation in the unit's area of interest (AOI). One enemy COA is sufficient; the most probable focus here is on predicting the enemy's main effort and objectives. Units one level down are displayed with their task organization annotated. The primary order of battle (OB) factors are composition, disposition, and strength. Less emphasis is given to the threat's tactics, combat effectiveness, and logistics. It should be noted that the G3, NOT the G2, is responsible for terrain and environment analysis. The G3 also will often discuss terrain effects on the enemy, just as a U.S. G2/S2 would discuss effects on friendly COAs.

In-Progress Review (IPR)

- ❑ Purpose: To "fuse" staff recommendations (from the Staff Estimates) in round-table discussion and to propose and develop COAs. The Chief of Staff (often with the G3) generally develops those friendly COAs proposed by the G2 and G3.
- ❑ G2 Actions: The G2 presents enemy COAs with focus on conclusions for conduct of the friendly operation and provides a recommended location for the "Main Effort of Intelligence Collection."

Situation Assessment Part 2

- ❑ Purpose: The G2 assesses the feasibility of COAs based on combat power ratios and the ability of each combat function to support proposed COAs. He will discard any COAs which are not supportable nor feasible.
- ❑ G2 Actions: The G2 supports G3 development of combat power ratios and develops details of

timing as they pertain to the enemy plan. This includes (at a specified time) the enemy's forward trace and the locations of his main body and reserve at moments critical to the execution of the proposed friendly COAs. The G2 also supports planning the timing of friendly operations; for example, counterattack, reserve. He also develops the collection plan and identifies "reconnaissance areas" (usually 20- to 100-square kilometers) which are intended to locate and target the enemy, not to confirm or deny enemy COAs.

Decision Briefing

- ❑ Purpose: To gain a decision (COA) from the commander. Supporting this objective each COA is presented on its own merit and then compared against one another based on combat power ratios and criteria selected by the Chief of Staff. The battle staff officers then explain their plan to support each COA they prefer and why. (Unsupportable plans have already been thrown out.)
- ❑ G2 Actions: The G2 provides the enemy situation update, repeating what was presented at the IPR because the commander has not yet heard the G2's assessment of the enemy COA. The "collection plan" is usually presented in a limited fashion, the G2 recommending to the commander the "main effort of collection." Selected reconnaissance areas are usually presented on a map overlay. A matrix supporting this effort is usually prepared but not briefed to the commander.

Once the commander approves a COA, the OPORD and Annexes are prepared and disseminated electronically. When time allows, an OPORD Brief may be conducted. More common, however, is the electronic transmission of information (digital), coupled with a frequency modulation broadcast of the essentials (key changes to situation, new mission, or Commander's Intent). There is no Intelligence Annex per se. The enemy situation is described in Paragraph 1 of the OPORD, and a collection plan and an overlay of the enemy COA are attached.

One Foreigner's Observations. Little is taught on the concept of "intelligence homework." The Bundeswehr's training of General Staff Officers does not emphasize the IPB-focused research performed by a U.S. G2 analysis and control element (ACE). The U.S. G2 conducts the research prior to a deployment and disseminates it to the respective G2 and S2 sections before a deployment or operation. As these General Staff Officers are the future G2s, G3s, chiefs, and commanders, it is likely that this emphasis does not exist in the units to the same degree it does in the U.S. Army. This is further reinforced by the emphasis on speed of decision-making at the expense of details. While this system has the advantage of increasing a unit's agility and responsiveness in combat (by reducing the time required to plan and decide), it also increases the tendency to "fight the plan and not the enemy."

There is also little emphasis and no training on the complete cycle which the U.S. Army identifies as "continuous IPB." Under the U.S. system, within the IPB process the situation templates drive the event templates which are used (through named areas of interest and time phase lines) to confirm or deny predictions that were based on the situation templates. Within the Bundeswehr this cyclic linkage of products is not taught as part of the G2's method for fulfilling his responsibility of tracking the enemy, largely because there is no doctrine specifying such products. One small-group tutor at the General Staff Course described the "estimate of the enemy situation" conducted by most Bundeswehr's staffs to be like an informal "coffee table" discussion of possibilities in comparison to the methodical, structured IPB process used by the U.S. Army. When the two systems are compared, then the price paid for speed in the MDMP becomes clear. Within the German system it is acceptable to intentionally ignore elements of the environment and enemy which do not significantly influence friendly conduct of the operation. The danger in this approach is that small details indicating a significant change to the enemy's plans could easily be missed. Other observations include—

- ❑ There are no priority intelligence requirements in the German system, which is odd considering its emphasis on focusing the G2's analysis on only critical aspects of the enemy plan.
- ❑ The G2 has comparatively little influence in the Staff (even less for the S2 at battalion level).
- ❑ Intelligence does not drive operations to the degree which it does in the U.S. Army.

Conclusions. Although IPB still carries some limits from the Cold-War era conditions of its conception, it is an effective system which has two qualities highlighted in comparison to the German system. First, IPB is supported by a professional corps of Intelligence Officers who spend the early years of their career using it, struggling with its limitations, and locally adapting it to their needs. Through these experiences they learn the fundamentals of how and why it works and from these lessons can develop improvements which they can then disseminate through professional publications, individual mentoring, teaching at the schoolhouse, and documenting as doctrine. Without those experiences as a young Lieutenant and Captain on battalion

(Continued on page 57)

Unit Intelligence Staff for Small Armies (or for Small Deployments from Big Armies)

by Major Phil L. Hughes,
New Zealand Intelligence Corps

The views expressed in this article are those of the author and do not reflect the official policy or position of the NZ Intelligence Corps, NZ Army, NZ Defence Force, or the NZ Ministry of Defence.

A "Big Army" like the United States Army must view the New Zealand (NZ) Army in a similar manner to which an Ivy League university might consider a country school. While the ideals and outcomes of both institutions remain philosophically the same, the differences in size appears to render the two so far apart as to make any commonality remote. However, if size can be overlooked, the similar essence of the organizations should be considered closely. Recent developments in the functional aspects of NZ Army intelligence provide some disclosure of its tactical essence.

The NZ Army has just completed what is considered a massive undertaking in deploying and sustaining a Battalion Group to East Timor (1999-2002). This deployment meant that, at any given time, one quarter of the Army was serving in East Timor, one quarter was preparing to deploy, one quarter was undergoing post-deployment administration and training, and one quarter was providing the sustainment and training base in NZ. This was a staggering rate of effort proportionally for any Army, but, in reality, was a small military deployment. However, as Operation Enduring Freedom has demonstrated, the essence of the rate of effort has distinct similarities with that of the U.S. Army. Like the NZ Army, the size of Special Force units in larger armies rarely goes beyond brigade size, and maintaining a sizeable "sabre" element overseas places significant pressures on what are proportionally small formations. Similarly, national force commitments to United Nations (UN) contingencies tend to be of expeditionary[1] size (battalion and brigade), regardless of the size of the donor national force (with, of course, notable exceptions). The lessons learned by the NZ Army during operations in East Timor, Bosnia, and other far-flung places under UN direction, have led to significant reflection regarding the staffing of the Battalion Group.

The Battalion Group, the key deployable Force Element in the NZ Army, integrates an infantry battalion with artillery, engineers, and other combat support (CS) and combat service support (CSS) elements into a cohesive and self-contained infantry-heavy force. Central to this development is the assumption that, as a UN expeditionary force the Battalion Group must "fight as it is" with limited or absent support and direction from the conventional brigade framework. Beginning in 2004 the New Zealand Army's Battalion Group will employ the LAV III (Light Armor Vehicle and also known as STRYKER) as its primary combat vehicle. Acquisition of the LAV III is driving increased deliberations regarding changes in the Battalion Group's staffing.

A motorized battalion gains significant maneuver and fire advantages over a light infantry battalion. However, as the Battalion's area of influence grows, so too does the size and nature of its area of interest (AOI). It also becomes a target of greater significance and visibility than its foot-bound counterpart, albeit with a decrease in overt vulnerability to enemy fires. Corresponding enemy threats must be recognized and identified at greater ranges because the higher operating tempo and closing velocities of the opposing forces. Because of this, NZ forces demand quicker and more intuitive maneuver to counter and prevail.

The NZ Army has recognized this debate within its developing Battalion Group structure. The issues are complex and include addressing the integration of the reconnaissance, surveillance, and fires functions into the battalion system. The organizational structure changes the hierarchy between the reconnaissance and surveillance (R&S) Commander and the S2, and must include the establishment of a targeting officer (TO). All of the staff supports the collection plan that is managed by the S2. The collection plan, by establishing a systematic approach to collecting against the Commander's priority information requirements (PIRs), supports his battlefield decision-making effort. The collection plan remains the overarching battle-management tool, integrating all sources and agencies available to support the Battalion Group. The information collected, followed by the S2's analysis, helps guide the employment of fires, decisive maneuver, and the R&S redeployment.

The change to employment of LAV III-equipped Battalion Groups will, however, force changes on how the unit operates and is staffed. Within the Intelligence Battlefield Operating System (BOS) the R&S organization has been expanded from the "traditional" platoon to a company. The R&S company will incorporate reconnaissance, surveillance, and sniper platoons, and integrate vehicles and other equipment commensurate with the battalion's mobility and acquisition needs. The R&S commander will continue to task and manage the company assets that support the S2's reconnaissance plan (derived from the collection plan) and supporting surveillance and target acquisition plan.

This staffing change, however, affects the Intelligence function. Traditionally, the R&S platoon commander acted as the Assistant S2, a hierarchical method of integrating the R&S assets into the collection plan. The R&S company commander is usually senior to the S2 (a Captain) which raises questions as to whether the S2, a specialist in the intelligence field, will be subordinated in effect if not in fact to the R&S commander, a specialist in an important but somewhat unrelated field.

The question of S2 subordination has wider implications as other specialized R&S elements are either allocated to the Battalion Group or integrated into its collection plan. These other R&S units are diverse in their mission focus and equipment and include air liaison officers, intelligence specialists, special operations teams, engineer reconnaissance teams, and artillery forward observer groups. Intelligence specialists clearly understand these R&S assets serve as their primary information collection tools and that that most effective tasking is when all are integrated into supporting the collection plan. The question arises, however: Does the R&S commander have the same perspective and degree of understanding as the S2? If not, then by rank and position will he override the S2?

Another element of this issue addresses the integration of fires within the Battalion Group. Primarily this is achieved by the allocation of a Field Artillery Battery to provide close support for the Battalion and is managed by the Fire Support Coordination Centre (FSCC). A recent appointment to the Battalion Headquarters is the TO who plays a critical role in ensuring that fires are delivered when and where required. "The TO, 'an experienced artillery officer,' is essential in the sensor to shooter link."[2] The TO will convert the course of action (COA) analysis, the commanding officer's direction, and the S2's explanation of high-value targets (HVTs) and high-payoff targets (HPTs) lists and target areas of interest (TAIs) into tangible and detailed weaponeering and develop the FSCC's attack guidance matrix. The TO is, therefore, a critical procedural link between the S2 and the FSCC as an enhancement to, or in the absence of, higher formation fires.

What remains to be seen is how the relative distribution of responsibility within the Intelligence BOS and between the Intelligence and Fires BOS will be coordinated with the allocation of seniority and tasks in the Battalion Group Headquarters. The S2 currently remains a mid-level Captain on his first staff appointment although following a series of postings to combat arms units where he was able to gain regimental and intelligence collection experience.

Key to improving the future Battalion Group's functionality will be an acknowledgment of the parity of key Headquarters staff. The executive officer (XO) (S3) and S1/S4 are Majors, which seems at odds to the S2 whose advice and staff work will fundamentally guide battalion planning and operations. This is especially true in the NZ scenario of UN quasi-independent battalion deployments. BOS and staff parity suggests that the S2's rank should parallel that of the other staff officers. This would provide a more responsive and appropriate structure within the battalion's R&S community and eliminate some problems associated with rank, not position.

As a Major, the S2 would be senior to the R&S commander and the TO, thus allowing the S2 the functional lead in the battalion's R&S planning. The S2, with a subaltern A/S2, would have a deep and close battle management division of labor much as the XO has with the A/S3 (adjutant) and would gain an equal staff officer profile with the XO, although without his battalion executive authority. Overall, this would enhance the battalion's planning and maneuver ensuring integrated S2 input, product, collection planning, and R&S management.

There is also a need to review the integration of intelligence personnel and intelligence courses into the wider army career management. This is highlighted by key "bench-marking" understanding of the nonlinear behaviour and thinking required in the Intelligence arena. By its very nature, linear planning can cause intelligence to be reactive, as analysis of enemy of critical courses, especially those that address command and tactics, which the intelligence staff must equally understand. To ensure conformity of understanding, the intelligence culture requires an understanding of the wider Army while other staff should have an equal intentions and means becomes "goal-driven" rather than "data-driven".[3] Intelligence staffs should be prepared for nonlinear enemy actions, and amend processes accordingly. It should be noted that nonlinear, nondoctrinal approaches not only require a lateral thought ability in applying and analyzing intelligence products but also place greater emphasis upon

intuition, empathy, and subtlety in developing effective analysis and assessment. Apparently insignificant information may reveal an opponent's intentions. While this nonlinear approach is effective within the Intelligence BOS, it has never sat comfortably within the structured and linear culture of the wider Army.

What does the future hold? The NZ Army Battalion Group will most likely operate as part of a wider coalition force and must look upwards to gain experience in the higher command and control architecture. Acknowledging this fact also recognizes the experience and training deficits that a small army must live with. Small armies need the support and mentoring of larger armies to develop interoperability in training and operations, which in turn validates unit-level structures and development. This is critical for a small army seeking to fully develop its tactical and operational intelligence skills. Therefore, the NZ Intelligence Corps, as well as the NZ Army, must support and rely on inter-Army exchanges, exercises, and courses to widen its operational environment, experience, and exposure of its personnel.

The lessons learned, however, are not all "small army" oriented. Recent operations conducted by the NZ Army have revealed a number of intelligence-related lessons that apply for "Big Armies". They reveal how effective and responsive intelligence support can be integrated into Special Force or expeditionary operations, which are usually conducted by independent and isolated small units. Continuous improvement and operational excellence remain the core effort of the Intelligence BOS. The experiences of Operation Enduring Freedom and East Timor, coupled with the imminent arrival of the LAV III, are providing a unique opportunity for armies of all sizes.

Major Phil Hughes is currently assigned as Directing Staff (Operations) to the New Zealand Defence Force Command and Staff College. His intelligence experience has been gained in postings as S2 to infantry battalions, brigades, and Special Forces, with an operational intelligence tour to Bosnia at Division level. He was recently Chief Instructor at the New Zealand Army School of Military Intelligence and Security.

Endnotes

1. For expenditonary operations, the Author subscribes to the views of General Sir Jack Deverell in "Coalition Warfare and Expenditionary Operations," *RUSI Journal* Feb 2002, UK, pp 18-21, wherein he described expenditionary operations has having characteristics of extended lines of communications, insecure rear areas, a purpose in line with national interests rather than national survival, mixed national and coalition support, and will not necessarily receive the total focus of military resources.

2. Capabilities Analysis and Doctrine "The NZ Motorized Battalion Group Doctrine: Developing Doctrine, " Wellington: Army General Staff, 2001, p. 39.

3. I. Wing, "Chaos Theory and Intelligence Analysis," ADF Journal, December 1995, p. 24.

Evaluation of the Enemy Situation

(Continued from page 54)

and brigade staffs, this process would stagnate at the tactical level, continuing only in divisions and above.

Second, IPB links products throughout the IPB process, specifically between the situation and event templates (and beyond IPB to the collection plan). This is the foundation of continuous IPB and a focus for sorting through the mass of information which flows into the tactical operations center.

What can we learn from the Bundeswehr system? Probably the most important learning point is to keep the estimate process short by focusing only on those elements of the enemy situation and environment that will directly impact the development of our plan. A good rule of thumb is if you cannot make a clear one- or two-sentence recommendation to the staff based on a piece of analysis, then the analysis is probably a waste of time at the battalion level and maybe even at brigade level. There is an exceptional strength in their system, especially at the brigade and battalion levels. As we increasingly face information overload in small S2 sections, elements of the German system may become increasingly attractive.

My conclusion is, however, that there are many more strengths in the more complete U.S. system, the most important being the way IPB focuses our collection on confirming or denying our understanding of the enemy's plan and intent and of warning us of changes to it while an operation is underway.

Major Rob Trabucchi has served as an Assistant Brigade S2 in Korea, Battalion S2, Platoon Leader and Division Collection Manager at Fort Bragg, North Carolina and as the V Corps Collection Manager in Heidelberg, Germany. He has served as a Company Commander and staff officer in the 108th MI Group, U.S. Army Intelligence and Security Command. He is currently a student at the German Armed Forces Staff College.

THE BATHTUB THAT DOESN'T HOLD WATER

by Collin A. Agee

The views expressed in this article are those of the author and do not reflect the official policy or position of the U.S. Army, Department of Defense, or the U.S. Government.

If there is truly a revolution in military affairs (RMA), staff officers have reason to believe that the revolution entails the PowerPoint™ Domain of War. This article addresses a PowerPoint slide. One PowerPoint slide!

The "bathtub slide" (which got this nickname from its appearance) (Figure 1) has become pervasive in Military Intelligence (MI) circles. It has penetrated the Pentagon. It has infused the Intelligence Center. It is present within the Program Executive Office (PEO) Intelligence and Electronic Warfare and Sensors (IEW&S). It has even touched tactical units.

Why has the bathtub slide become popular?

- ❑ It briefs well.
- ❑ It is easily constructed in PowerPoint.
- ❑ It is symmetrical.

Despite its visual appeal, in the serious business of designing intelligence for a transforming Army, the slide is misleading and conveys dangerous perceptions about the role of organic intelligence versus that accessed via Intelligence Reach. Here are the problems with this slide; each number corresponds to a point on what I believe is the real relationship, as depicted by Figure 2.

1. At the risk of stating the obvious, organic assets have not yet deployed during the Predeployment Phase. Thus, organic collection begins at absolute zero on the Y-axis. There may be deviations from this starting point if a contingency evolves over a period of time that includes the introduction of U.S. troops, or if there is a permanent U.S. presence, such as in South Korea.

2. Because organic assets are not in place, initial collection totally depends on Intelligence Reach, even as organic analytical elements begin using externally derived infromation. This low level of effort reflects the nominal level of attention paid to the entire Earth during peacetime, for an Army with a true worldwide mission.

3. As it becomes evident that a crisis is looming, national, theater, and other collection and analysis assets place increased emphasis on the area of interest (AOI).

4. Unit assets arrive in theater according to the time-phased force deployment data (TPFDD) and are placed into operation. Analytical nodes become operational and connectivity is established, both within the theater and with Intelligence Reach assets. Some collectors, such as human intelligence (HUMINT), incrementally become effective, while technical collection assets gain effectiveness as their operators become accustomed to the operating environment and tactical problem.

5. If the crisis evolves into a combat phase, the theater and national assets will surge in support of the warfighter. "Persistent Surveillance," informally known as "Intelligence Stare," connotes the focus of assets and analysts in providing 24-hour, detailed coverage of selected named areas of interest (NAIs) in support of the commander's priority intelligence requirements (PIR). This part of the original slide in Figure 1, depict-

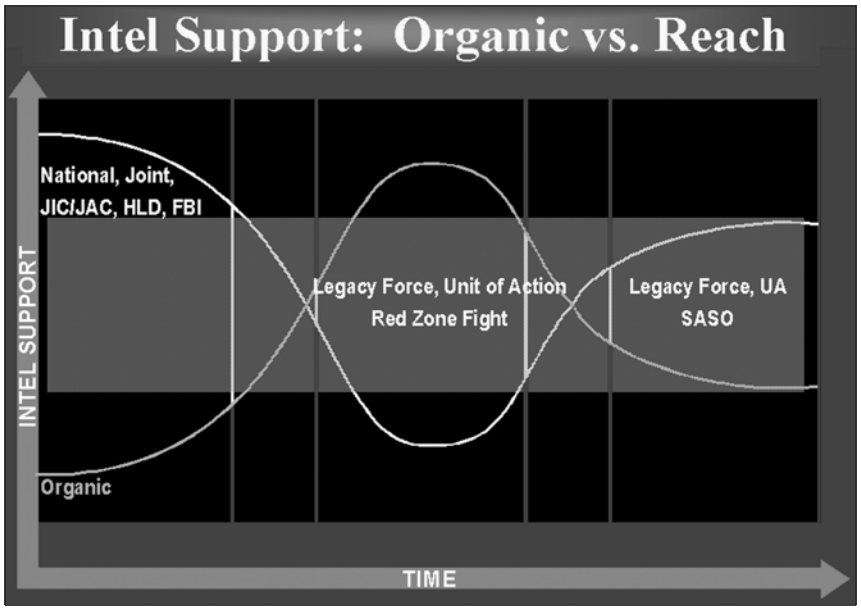


Figure 1 . The HSOC and UE1/UE2 Reach During Phases of the Operation. (All echelons are dependant upon one another to provide intelligence at critical times to develop the intelligence picture.)

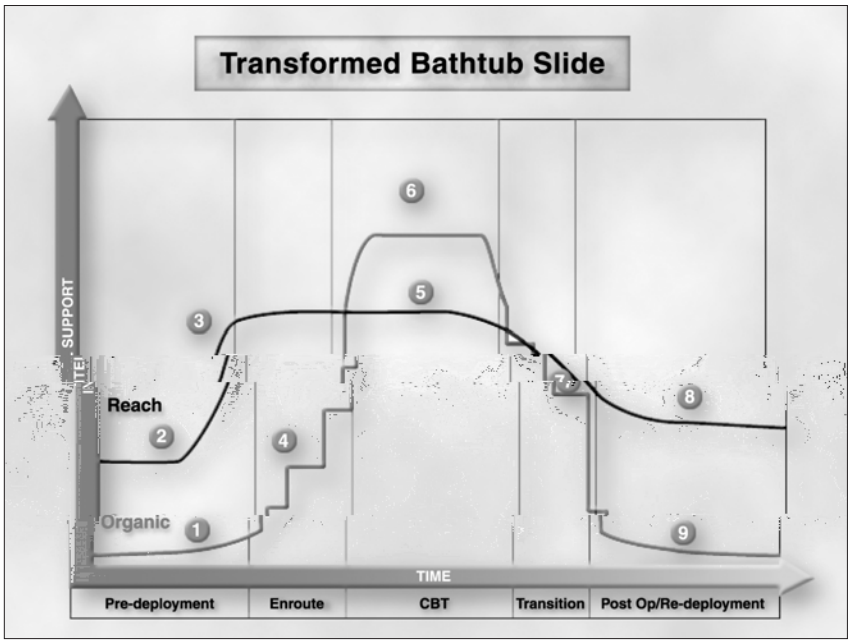


Figure 2. Transformed Bathtub Slide showing the Real Relationship Between Organic Intelligence Accessed Through Reach.

ing external support at its absolute nadir during combat operations, is perhaps the most misleading and dangerous part of the slide. MI is promising the Objective Force unprecedented Situational Awareness (and more importantly, Situational Understanding), made available via the Common Operating Picture (COP). In keeping with the Objective Force imperative of Minimum Footprint Forward, much of that support will come via Intelligence Reach. And yet, the original Bathtub Slide conveys that external support will be least available when it is most needed. Intuitively, and by our training and combat experiences, we know that all assets—internal and external—are maximized during combat operations. If anything, this becomes more imperative for Intelligence Reach assets in the Objective Force.

Operators and Intelligence professionals alike envision a measure of autonomy for Units of Action (UA). In part, this recognizes that combat entails closing with the enemy, attacking him based on sensors that are a part of the engaged weapon system, and sensor-to-shooter links, when the one who fires first survives.

In part, it is based on worst casing: giving the UA the wherewithal to survive and prevail if external links are lost. We must be careful not to design a system only for the worst case, sub-optimized for normal operations. If we are to adopt a warfighting strategy based on decision dominance and rapid decision-making—Battle Command—then we must maximize the contributions of Intelligence Reach during all phases of operations.

The Combined Arms Center (CAC) at Fort Leavenworth is developing the Home Station Operations Cell (HSOC) concept, with input from Army G2 and the Intelligence Center. This concept seeks to maximize the support provided from outside the theater, reducing the "footprint," logistical and force protection requirements for deployed forces. In just a few years, this concept portends that most analytical work will be accomplished at Home Station in the continental United States. In today's parlance, it is the equivalent of leaving the analysis and control element (ACE) behind when you deploy, connected via a virtual electronic tether to the deployed command and his forces. In the terms of the Bathtub Slide, the lines of the graph begin to blur, as analysis will be conducted by organic elements, but those elements will not be in theater.

6. The original slide, if aggregated, is a flat line. Intuitively, we know this is not true; all assets will surge during combat operations.

7. Unit capabilities decrease in quantum steps during redeployment as individuals, systems, and assets are removed from operation.

8. External collection and analysis is likely to be higher during the post-combat phase than the nominal level, as these assets remained sensitized to the crisis area.

9. When unit assets redeploy, they cease collecting.

In summary, the relationship between organic collection and analysis and Intelligence Reach is an important consideration as we envision, design, and bring to life the Transformed Army. Scrutiny of the traditional Bathtub Slide demonstrates flaws in logic. If taken literally, these distortions will have undesired and dangerous effects on the planning for Intelligence Reach for the Objective Force—and the planning for UA to fight largely without the help of Intelligence Reach when it matters most.

What to do with the old Bathtub? Get rid of it. It doesn't hold water!

Lieutenant Colonel (U.S. Army, Retired) Collin Agee, completed an MI career as the G2 of 10th Mountain Division. He currently works as a contractor in support of the Army G2. He can be reached at Collin.Agee@hqda.army.mil.

by Stacie Taylor

The modern digital battlefield is marked by one distinctive change from those of previous eras: this is in the amount of data that can be collected by literally thousands of sensors. So information-rich is this new operating environment that for the Intelligence analyst it can be overwhelming. Today's Intelligence analyst needs accurate, timely, and reliable information from a trusted source, a critical element in successful mission completion and one that may ultimately impact his own survival. One tool that may assist in this effort is now under development. SIREEL is an Internet web site that allows soldiers to see how different enemy vehicles look under normal conditions, to include green and red infrared imaging. SIREEL gives today's soldier a tool to train other soldiers quickly and easily without a lot of supervision.

What do threat vehicles look like under different weather and terrain conditions? What are the differences between an Iraqi T-72 and the Chinese-produced T-90-II, a derivative of the Soviet T-72? What do they look like at 1000 hours while it is raining? These are important questions, and the SIREEL web site provides users with visual answers with the click of a mouse button. The soldier does not have to risk life and limb to reconnoiter his enemy. Instead, he can "virtually deploy" using the latest in simulation software.

The National Ground Intelligence Center (NGIC) supplies this powerful tool. SIREEL is a password-protected web site accessible through the unclassified Internet. It is intended for soldiers, gunners, pilots, and mission planners required to view the world through a Forward looking infrared (FLIR) sensor or thermal sight. SIREEL's vehicles are divided by countries or regions. It displays the thermal signatures of target vehicles according to the terrain and conditions found in those countries or regions. The thermal signatures are a combination of static imagery and video footage, so the soldier can view threat vehicles on both the defense and offense.

When observing a threat system through thermal optics, warfighters must be aware of a variety of conditions affecting thermal imaging, including time of day and year, terrain, prevailing weather, and a vehicle's operational status (see Figure 1). SIREEL is a process in which infrared measurements and predictive models are used to produce infrared signatures of threat vehicles and scenes to simulate these conditions.

The **SIREEL** process is extensive, the following expansion of the acronym below help to reveal the level of detail. One aspect consists of Simulation and modeling. Simulation, using thermal predictive codes, complements NGIC's empirical data and fills gaps where measured data may not be available. Actual calibrated InfraRed signature data are used to validate the models. Earth Environment combines our vehicle models with a thermal scene prediction. This simulation provides a view of the entire scene, integrating vehicles with terrain and environmental conditions. The process and its results on the website combine to form the Lab. With higher fidelity infrared signature models, simulation results are more realistic and accurate.

This means that you tell the web site the time of day, type of weather, vehicle, and the location you want. All of this is done with just a few

(Continued on page 64)

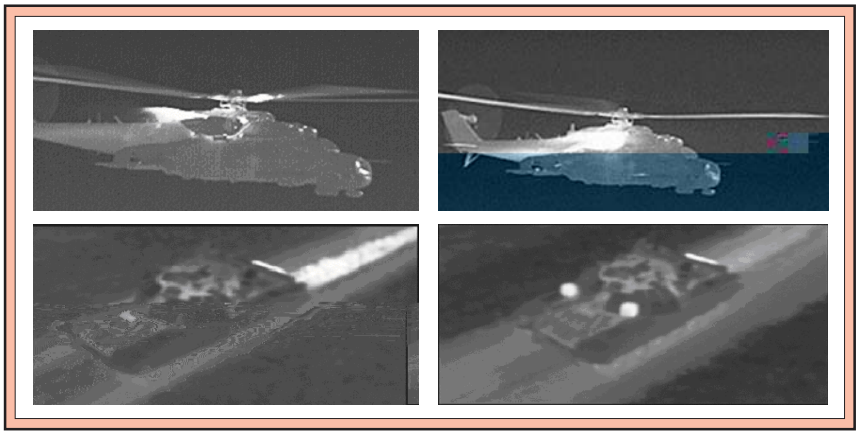


Figure 1. Thermal cues: the operational status of a vehicle is crucial. A vehicle in a silent watch mode may be more difficult to detect than one idling or accelerating. An active protection system is easily detectable when turned on, and identifying a suppressed vehicle may assist your mission planning.

TUAV "Video" Data Can Support Numerous Missions

John Dugan, Ph.D., and Donald Wurzel

The most common missions described for tactical unmanned aerial vehicles (TUAVs) are in support of situational awareness and targeting. The principal sensor developed to provide data to satisfy these needs on low- to medium-altitude-endurance unmanned aircraft is the video camera. Video cameras can provide very useful *movies* of areas of particular interest that are crucial for observing the surroundings and for manually detecting and tracking targets of high interest. The newsprint is replete with stories of their utility in support if intelligence, surveillance, and reconnaissance (ISR) missions.

Example UAV systems and products being developed by the U.S. Army have been described by Colonel Knarr, et al, in a recent article in the ISR Journal.[1] In almost all tactical-level systems developed and fielded to date, the video data are reviewed manually by a human operator, and targets of interest are detected unaided by computer processing. Such processing, when coupled with an enhanced onboard navigation capability, could dramatically increase the accuracy of UAV-derived data for improved precision targeting support and provide additional battlefield preparation data as well.

The navigation subsystems on present and near-future small UAVs are designed primarily as an aid to safety of flight. They do not provide sufficient navigational accuracy to exploit available digital imagery. That is, the data are not very useful for mensuration of the imagery onto a geodetic grid, which is essential for determining Global Positioning System (GPS) coordinates for precision-guided munitions (PGMs). Good examples are the current Air Force *Predator* and the Army *Hunter* UAVs which do not provide accurate, digital metadata for mensurating the imagery. They provide a good picture, but GPS coordinates cannot be derived from the video. The navigation shortfalls inherent in the *Predator* and *Hunter* include inaccurate measurements of both the camera location and attitude during the collection of any particular image frame. If these measurements and the range to the target were known accurately, the geo-position of targets in the imagery could be calculated precisely. The best accuracy that can be achieved on operational systems today is hundreds of meters in three dimensions. Such poor accuracy does not enable the new family of small PGMs that all the Services are developing or producing, nor does it enable other important mission products discussed herein.

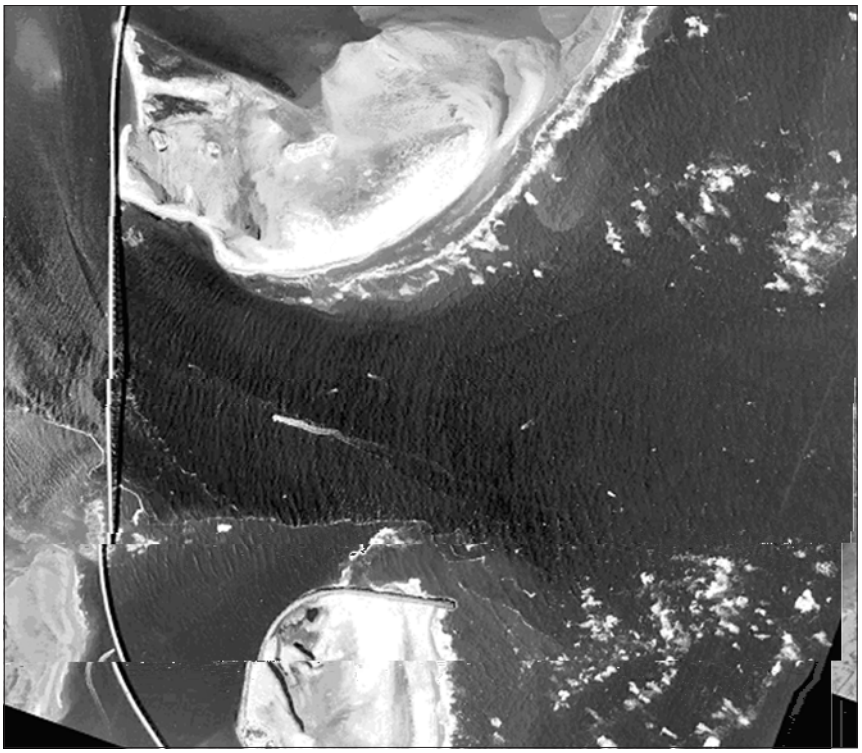


Figure 1. Image from a sequence collected at an ocean inlet on the North Carolina Outer Banks. The sea is to the right and sound to the left. Numerous small targets such as buoys and fishing vessels can be seen, as well as surface waves and foam patches.

There are a number of possible techniques that could be employed to establish the accuracy needed for better precision targeting. One could use a high-accuracy inertial navigation system (INS) and a laser-range finder, wherein the target location is calculated directly from measurements of the camera location and attitude and the range to the target. This approach is called *direct georeferencing*. It is expensive for a tactical UAV, presents laser eye-safe issues, and has not yet yielded desired accuracy. Another current alternative would be to calculate the geo-location of a manually detected target by positioning it relative to ground control points (GCPs) which are recognizable features in the image, and then find these GCPs in a

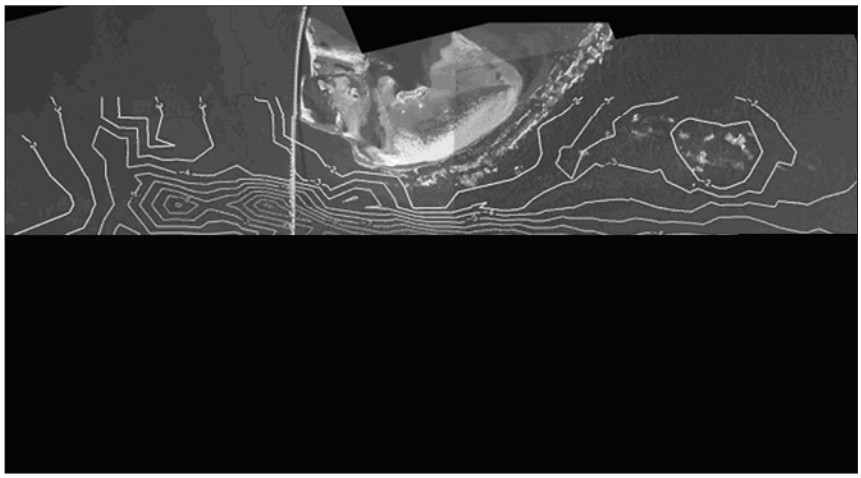


Figure 2. Water depths retrieved from an algorithm that utilizes a sequence of geodetically mapped images and uses characteristics of the propagating waves.

reference image that is geodetically correct.

This approach currently is being developed for Joint Service Imagery Processing System (JSIPS) workstations. Unfortunately, the relationship between the video-derived image and the reference image is not always one-to-one because of changes that may have occurred between the times that the two were collected (for example, winter versus summer, new construction, battle damage) or changes in the relative viewing geometries of the source platforms. In addition, there may well be circumstances where suitable reference images simply are unavailable.

Finally, this is not a rapid process, so it does not address the time-critical strike issue. There are other techniques that have emerged recently that have been successfully demonstrated on imagery from surrogate UAVs, although they have not yet transitioned beyond the Science & Technology (6.2/6.3) stage of development. These approaches key on inexpensive commercial-off-the-shelf (COTS) technologies and a specific mix of hardware and software wherein good geodetic positioning of the camera and advanced processing algorithms are used to calculate the camera attitude and the relative target position. Thus, this approach can be considered a variant of direct georeferencing.

This approach uses a rather inexpensive INS that provides good camera positioning via augmented GPS techniques, but relatively inaccurate attitude solutions due to the use of inexpensive inertial-measurement units (IMUs). The higher noise levels in the COTS IMU can be compensated by one of several techniques being developed under Office of Naval Research (ONR) support. These techniques recalculate the onboard estimates of camera-attitude angles by one of several different algorithms. One technique even takes advantage of features in the images, and it is perhaps of higher risk because it is so unique, but it potentially provides significantly higher payoff because the accuracy of the results, in principle, are independent of the stand-off range. This technique has been applied to imaging data collected during fleet exercises using the Airborne Remote Optical Spotlight System (AROSS), also developed under ONR support. Absolute positioning accuracies of better than 5 meters from 3-kilometer range have been demonstrated, which are adequate for targeting of today's and near-future weapons. Which one of these many approaches will be the best for tactical systems has not yet been determined, and this topic of geodetic referencing of the imagery remains a fundamental one for resolution by further research and development.

However, a primary point of this paper is that the ultimate capability of small, tactical UAVs employing video cameras is much wider than the presently planned and conducted missions for situational awareness and targeting. No matter how this geodetic referencing is accomplished, it enables a number of additional mission products, some of which are particularly relevant to the littorals and, therefore, especially interesting for applica-

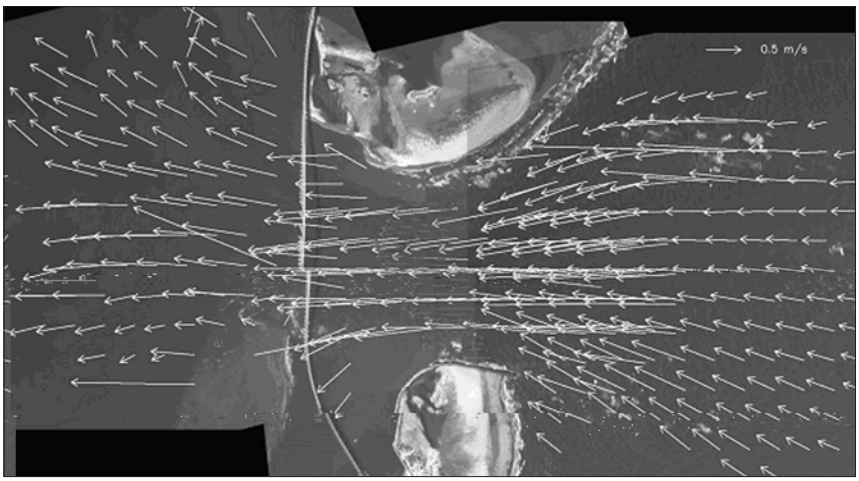


Figure 3. Water current vectors, retrieved by the same algorithm as the water depths in Figure 2. The current speeds are indicated by the length of the vectors (the scale is in the upper right hand corner), and red vectors are *ground truth* collected by sensors in the water.

Figure 4. A small part of a single image of the beach defenses observed at KERNEL BLITZ 2001, including a tank trap, anti-personnel and anti-vehicle obstacles, and a landmine field. The beach is on the lower right, the upper portion is a large topographical obstacle, and the beach exit zone is protected by the barriers.

tion to U.S. Navy and U.S. Marine Corps littoral warfare missions. These products fall under the general classification of battlespace environmental assessment, and they specifically are enabled by further data processing using advanced physics-based algorithms. Examples include retrievals of maps of the environment (digital terrain elevation data [DTED], water depths, water currents, wave heights, surf characteristics); construction of 3-D models of a scene to enhance mission preparation and rehearsal; and detection of small, faint targets such as surface mines.

Amphibious assault planning, for instance, requires accurate estimates of water depths, currents and surf characteristics located at the beach of interest. Multi-image, geodetically correct images of the waves as they shoal and break can be used to calculate these environmental parameters. This is accomplished by detecting and tracking the waves, and fitting a theoretical physics-based model for the wave kinematics to the measured wave spectrum. Figure 1 shows a single image from a sequence that has been collected along the North Carolina Outer Banks. This shows a tidal inlet, where there are unknown topography, water depths, and currents. The top-level questions are: Where is the navigation channel and how deep is it? How strong are the currents? Where are the navigational hazards such as shoals? Figures 2 and 3 are the retrieved water depth and current vector maps. These are overlaid on the single image so that the user can instantly understand the relationships between the land features and the hydrographic maps.

Another example, shown in Figure 4, is a single image from an airborne sequence of a defended beach during the amphibious training exercise KERNEL BLITZ 2001. The extensive tank trap and the vehicles parked behind the bluff are obvious, and would likely be seen by any tactical UAV equipped with a video camera. However, the image sequence can be used to derive a high-resolution topographic map to calculate the height of the ridge of sand and depth of the trench constructed for the tank trap. In addition, the large field of land mines is much less obvious, but these might be detected by mapping each image frame to the WGS84 geodetic coordinate system as above, and then applying an ad-

Figure 5. Single image taken from a sequence of images as seen from a fly-through of a group of buildings. The fly-through was generated from images of all sides of the buildings collected by AROSS as it flew around them.

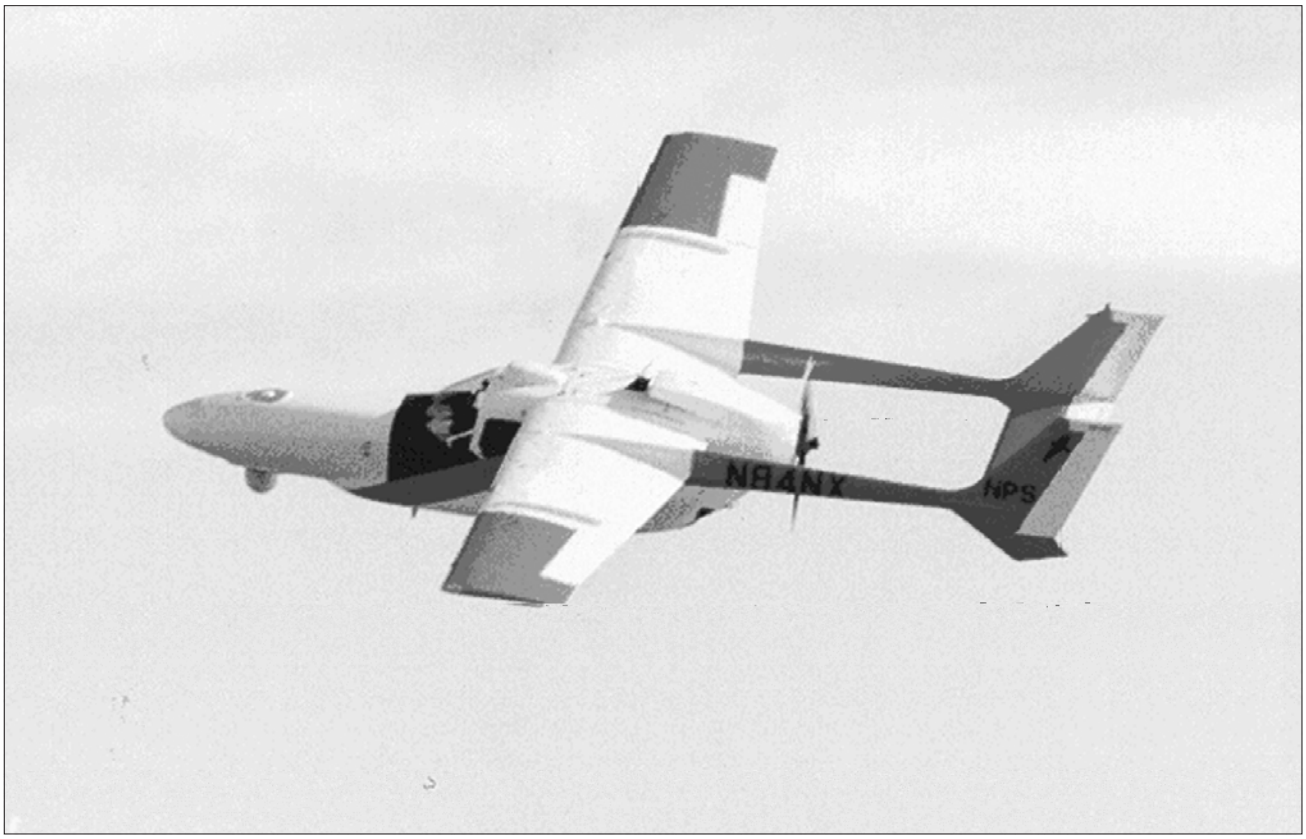


Figure 6. The AROSS turret mounted under the nose cone of the CIRPAS *Pelican* aircraft. The aircraft acts as a surrogate UAV for testing purposes, but in this case, the pilot and an AROSS operator were onboard.

vanced processing algorithm that detects the mine field by their occasional sun glints.

A final example is the use of the multi-image data to construct 3-D models of buildings and other objects. Advanced processing algorithms can provide the data to mensurate the objects and provide video-loop fly- or walk-throughs of the objects and terrain, thereby enabling a more accurate assessment of the impact of physical features (especially in an urban environment) on mission planning. An example image from a video-loop fly-by of a re-constructed group of buildings is shown in Figure 5.

These examples of multi-image data are just a few of many applications of such data and processing algorithms. They were demonstrated on digital images collected by a surrogate TUAV (the modified Cessna 01-A called the *Pelican* that is flown by the Naval Postgraduate School's Center for Interdisciplinary Remotely Piloted Aircraft Studies, or CIRPAS) carrying the AROSS imaging system mentioned previously (see Figure 6). The digital camera was installed along with an inexpensive INS in a *Predator* turret that was mounted under the nose cone, and trained on the targets for these demonstration products.

It is clear that motion imagery can be accurately geo-referenced and subsequently exploited for many more tactically important and mission-relevant products than have been explored thus far.

Endnotes

Knarr, W.M., S. Haskins and T.P. Mouras, 2001, Army Transformation and the Tactical Unmanned Aerial Vehicle (TUAV) System, MIPB, pages 2, 27, 50-55.

SIREEL

(Continued from page 60)

clicks of the left mouse button and you are there. The soldier chooses his time and place to train. It is that easy.

So do not be shy! Get on board with this program by getting your account at https://sireel.ngicarmy.org SIREEL offers capabilities and unique perspectives you can not afford to miss.

Stacie Taylor is a physical scientist in the Measurement and Signatures Division of the National Ground Intelligence Center, Charlottesville, Virginia. She has a Math degree with a strong background in optics and physics. She began her career at the Kennedy Space Center as a software engineer in the Math Modeling Group simulating various shuttle systems. She has been with NGIC for 14 years measuring IR signatures of foreign ground vehicles and helicopters for customers ranging from the warfighter to smart munitions programs.

Enduring Freedom

Extract From Operation Enduring Freedom Lessons Learned and Observations Afghanistan: 19 May 2002–12 June 2002

by Sergeant First Class Robert J. Ehrlich
CALL@JRTC

Editor's Note: *This article is an extract from a Center for Army Lessons Learned (CALL) publication and reflects two intelligence-related lessons learned from operations conducted in Afghanistan.* **MIPB** *thanks SFC Ehrlich and CALL for sharing this information.*

Observation 9: Theater Maps

Discussion. The unit deployed with insufficient maps of the area of operations (see Figure 1), especially those of 1:50,000 scale. The unit installed software program Falcon View on all of the TOC and TAC computers before departure. A tremendous asset, Falcon View was employed for the duration of the operation. With it, the unit could quickly and easily add graphics to a map, boundaries, and other information then simply print a color map of area they were going into. A 1:50,000 scale map of the area was not available for download to Falcon View and that used by MCS Lite was incompatible with Falcon View.

Editor's Note. *Falcon View is an integral part of the Personal Flight Planning Software (PFPS). This software suite includes Falcon View, Combat Flight Planning Software (CFPS), Combat Weapon Delivery Software (CWDS), Combat Air Drop Planning Software (CAPS), and several other software packages built by various software contractors. Falcon View is a Windows 95™ and Windows NT™ mapping system that displays various types of maps and geographically referenced overlays. It supports many types of maps, but the primary ones of interest to most users are elevation and aeronautical charts and satellite images. Falcon View also supports a large number of overlay types that the user can display over any map background. The current overlay set is targeted toward military mission planning users and is oriented towards aviators and aviation support personnel. Additional information can be found at http://www.falconview.org/contacts.htm.*

DTLOMS Implications:

Doctrine. Doctrine must include digital mapping and planning software functions as these can significantly assist in the military decision-making process (MDMP).

Training. Training in various software programs must occur in the schoolhouse and home station to allow staff soldiers to use the equipment and tools properly, and make the most of the programs available to assist in planning and combat control.

Materials. Software packages must all include a commonality in maps, either by being able to import the various formats used by other programs, or by using a common format. All DOD map programs must have a commonality in exporting and importing map sheets. If not, DOD

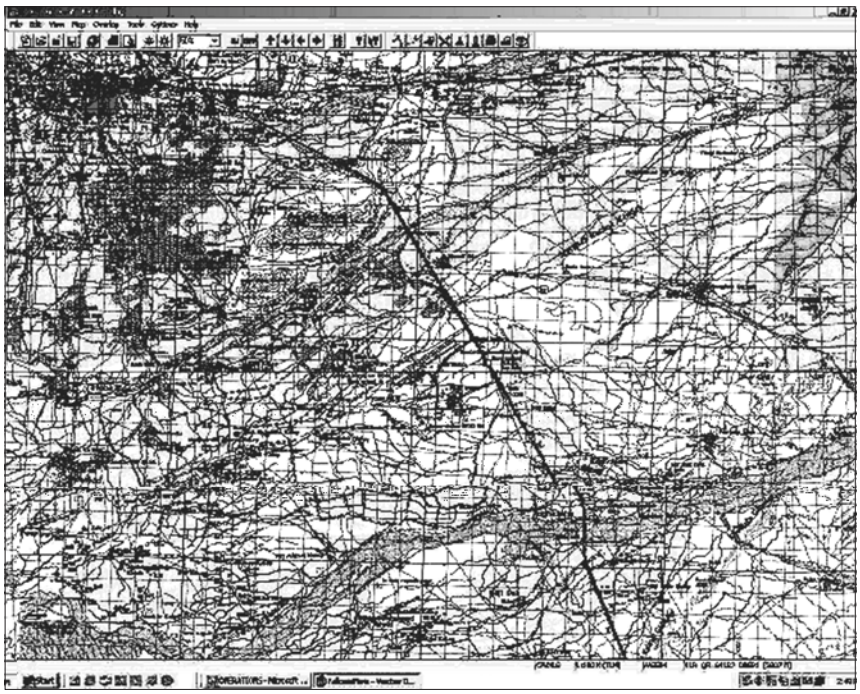


Figure 1. Map of Area of Operations.

must support each authorized program with all (map) sheet scales for download.

Observation 14: Falcon View or MCS Lite.

Discussion (Extract). The 3d Battalion S2 was very forthright in comparing Falcon View to MCS Lite. He favored Falcon View because it—

- ❑ Was much easier to learn and use than MCS Lite.
- ❑ Allowed you to develop a plan quickly, lay it out, then if required, change it without having to delete and redraw a boundary.
- ❑ Allowed "printed to scale" without the hassles of putting together map sheets, acetate, alcohol pens, and the like.
- ❑ Allowed you to download icon pallets or create your own.
- ❑ Allowed conduct of fly-through rehearsals in support of air assault missions. In this use, it allowed us to "see" exactly what we had templated along the flight route.
- ❑ Allowed a change in the magnification (zoom).
- ❑ Allowed rotation of the view using only a few simple keystrokes.
- ❑ Allowed easy updating to other users by sending databases via the LAN, E-mail, or by disk. This was important because it allowed everyone use of the same graphics.

Recommendation. Relook program software for simplicity of use and compatibility across platforms. The digital TOC must be something that has simple-to-learn functions, but be robust enough to handle task such as those explained above.

DTLOMS Implications:

Doctrine. Doctrine must include digital mapping and planning software functions as these can significantly assist in the MDMP.

Training. Training in various software programs must occur in the schoolhouse and home station to allow staff soldiers to use the equipment and tools properly, and make the most of the programs available to assist in planning and combat control.

Materials: Software packages available to soldiers must all include a commonality in maps, either by being able to import the many formats, or use a common format.

Soldiers: Soldiers assigned to staff positions must be computer-literate and seek training for the operating systems and programs they will use. They must be self-starters and before being assigned to a staff, all must be competent in all aspects of their military occupational specialties (MOSs). Assignment to a staff position should not hinder the soldier's chance for advancement; rather, it should make them stand them out as being the highest qualified.

Observation 23: Brigade Intelligence Analysis

Discussion. During operations, the brigade Intelligence section was severely understaffed and underequipped to handle the volume of information coming in during actual combat operations. Part of the problem was that although each higher headquarters had a Secure Internet Protocol Router Network (SIPRNET) information page, they had not been maintained. Many pages were outdated but even those shown in the CAAT were more than 3 weeks old and some pages were more than month old. Neither SOF nor TF 11 reported through standard intelligence channels, even on areas the Rakkasans were targeting. When SOF or TF 11 came in from a mission, the S2 shop attempted to capture a quick intelligence snapshot of the area. Otherwise that data was lost to the soldiers about to go into the area. Additionally, during the course of the MDMP, areas of interest changed with almost every FRAGO.

Digital Imagery. NIMA teams arrived to update digital imagery but their responsiveness was mixed. The first team was very responsive and cooperative in updating data. The second team was not, forcing the third team to attempt to make up for them. Falcon View served as the easiest, most efficient means in updating maps and providing maps and overlays to units and commanders.

Other Observations

- ❑ Training: A common comment was, "that at JRTC you know how the enemy fights. Here (Afghanistan) it is random chaos but our training was directed at the threats present at JRTC. To train for here one needs to go to Los Angeles and get into the barrio and pin on a badge during a drug or gang war."
- ❑ All home station training should include SALUTE and SALT information formats.
- ❑ Soldiers under duress fail to submit spot reports to higher that provide a good picture of what is happening.
- ❑ UAV / Predator utilization and taskings do not help. Predator TV must be analyzed to be effective; it requires a collection plan, not just hip-shoot taskings for an area. Hours of tape were shot, but no one had a focus or the time to sit down and analyze the footage for validity of operations.
- ❑ During the MDMP, CA and PSYOP issues were often pushed to the S2 to work out, even those with a CA and PSYOP team.
- ❑ Scouts and long-range surveillance (LRS) were not used effectively. Rather, they became additional shooters since there was no clear task or purpose for implementation or usage of the teams.

(Continued on page 76)

Wireless Phrase-Recognition PDA Deployed to Afghanistan

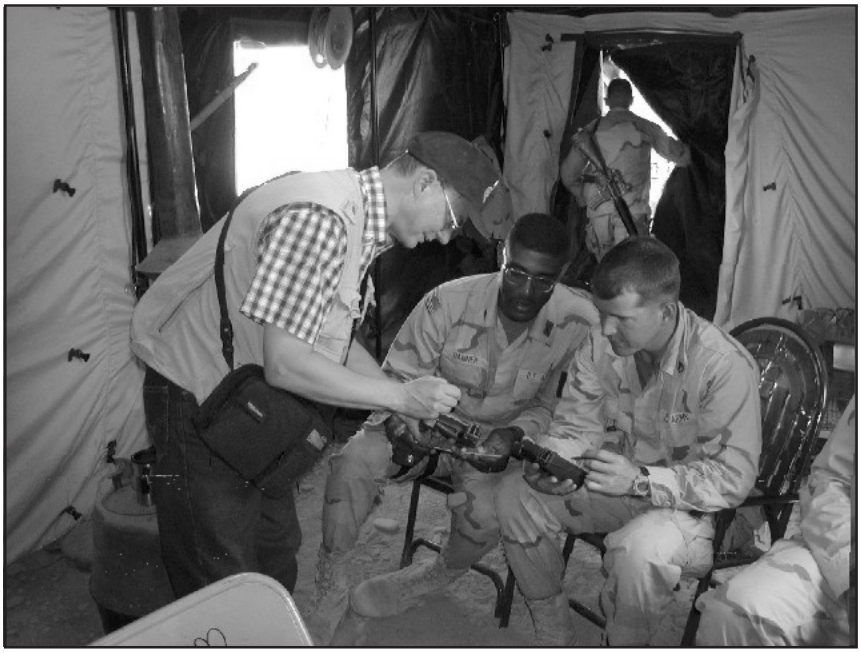
by Lawrence Ricci, assisted by Captain James Smith

A crucial component in supporting the commander's battlefield visualization requirement is communication which, for the purpose of this article, refers to the passing of information between an information source and an information user regardless of means. Conversation, whether face-to-face or by other means, is as effective today as it was in earlier times. Whether determining a threat's location, order of battle, tactics, strategies, or simply asking for directions, conversation has been, and will remain important in future military operations. A stumbling block, however, especially in locations that feature low-density languages, is the inability to translate a complete conversation, or at least the critical elements of that conversation. This article looks at a recently developed system that has already proven its utility and, as it improves, has great potential as a battlefield tool.

Need Realized During DESERT STORM

Soldiers' ability to communicate often limits effective employment of military forces in peacekeeping. During Operation DESERT STORM, mass surrenders of enemy troops overtaxed the coalition's ability to provide medical services. Battlefield doctors improvised a solution using laptop personal computers (PCs) with speech-recognition software, creating a list of frequently asked questions. When the user recognized a phrase, the PC played a WAV [sound] file of the Arabic equivalent. While the laptop had limited vocabulary and portability, the system proved useful. Later, a team headed by a former Navy SEAL (Sea-Air-Land special forces team member) realized that if they could package this function into a hand-held or belt-mounted computer, its utility would increase dramatically. They contacted the Defense Advanced Research Projects Agency (DARPA) about the project.

A number of companies developed the translator with about $1 million in grants from DARPA's Babylon program. The goal is to develop rapid, two-way, natural language, speech-translation interfaces and platforms for use in the field. Here the system will support force protection (FP), refugee processing, and medical triage. Babylon focuses on overcoming many technical and engineering challenges limiting current multilingual translation technology to facilitate future full-domain, unimpeded dialog translation in multiple environments. The Babylon program will focus on low-population, high-terrorist-risk languages that no commercial enterprise will support. The Babylon seedling one-way project, Rapid Multilingual Support (RMS), deployed to Afghanistan in spring 2002. DARPA has selected Mandarin and Arabic based on immediate and intermediate needs.



Photograph courtesy of Ace Sarich, Marine Acoustic, Inc.

LTC Jim Bass, DARPA Program Manager, shows CPT Mark Danner and another soldier from the 519th MP Battalion how to customize the Phraselator for guarding detainees in Khandahar.

Context-Specific Speech-Recognition Software

Context-specific, speaker-independent software is in common use today for 1-800 telephone directory assistance, flight reservations, and other uses. Those applications, however, require server-sized computers. With the goal of bringing speech recognition into mobile embedded devices, the developers contracted to integrate the Phraselator™.

Ruggedized Low Power Consumption

This unit had to be ready for "instant on" phrase translation (e.g., *"Stop or I'll shoot"*) while preserving full-day battery life. The development team started with a 32-bit RISC (reduced instruction set computer) CPU (cen-

Photograph courtesy of Applied Data Systems.

tral processing unit) capable of performing workstation-like speech analysis on little electric power.

After a certified process of uprating for temperature specifications, StrongARM™ provided the core of this system. The team carefully engineered the other components, including a high-fidelity, directional stereo-audio channel with both an inbound and outbound capability to maintain this low-power specification. The operating system offers both multimedia capability and comprehensive communication support for wireless applications. The developers of the system used this operating system to facilitate compatibility with pocket processor applications, and future versions will also be available with the upgraded operating system to encompass more robust network security and accomodate higher performance future CPUs.

Technical Challenges to Meet

A militarized personal digital assistant (PDA) has more requirements than the "traditional" speech recognition, including the ability to run in the toughest environmental conditions over extended temperature ranges in the harshest heat, rain, and snow. The touch-screen display must be readable in full sunlight and full darkness. They had to design a power system that could run for hours from multiple types of batteries (disposable, as well as rechargeable). These batteries would have to be able to accept a charge from various levels of applied current including 12-volts direct current (VDC) and 24-VDC vehicle power and 110- or 220-volts alternating current (VAC).

The developers would have to use special care with the audio system design, allowing full-range frequency response from microphone through a compression/depression module (CODEC) and back out to the speaker. A goal for the speech-recognition capability was set at 98-percent accuracy in near-real time. Finally, the system had to be flexible and built to accept generally available third-party hardware and software.

Due to the urgency of demand following September 11, the contractor engineering expertise was critical in making a fast-turn, fully functioning computer in a few weeks, rather than months or years. That company has specialized in a variety of PDA-type systems for applications ranging from industrial to assistive technology hand-helds. The Phraselator developers selected the RISC CPU and the operating system as both proven and powerful enough for this task.

By basing their device on the advanced operating system, the developmental team was able to complete the Phraselator quickly. They delivered a smart device that supports the speaker-independent speech-recognition functionality that these users required.

Military and Security Applications

Initial sales will be to the U.S. military but the developers anticipate future applications in public safety and health. Police, fire, and emergency medical services can use the Phraselators' ability to translate essential related words into nearly any language. Other potential applications include use in airports, at sports or other events, and in building security where the Phraselator will allow questioning of individuals while maintaining a wireless link to back-office security systems where personnel can analyze profiles and answers.

Phraselator Field Trials in Afghanistan

The Army sent about 500 Phraselator hand-held translator systems to Afghanistan in March 2002 for field-testing. The Afghan RMS unit comes with a "force protection" language module (containing roughly 2,000 to 4,000 phrases) used by soldiers under potentially hostile conditions. This unit keys most of the phrases to specific circumstances such as FP or security. It uses different tones for the preprogrammed Arabic, Urdu, Pashto, and Dari announcements—a stern, authoritarian voice shouts phrases such as "*drop your weapon*" or "*halt*" while a gentler tone would inquire, "*can I help you?*" Phraselator has a kit that allows users to build their own modules. Many users have learned how to customize the system for guarding detainees, prisoner processing and control, medical assistance, and much more.

Mr. Ricci is employed by the Bussiness Development Section, Applied Data Systems. Captain Smith, Concepts Division, USAIC&FH may be contacted at (520) 538-2211.

Attention NCOs

Send us your articles and book reviews. If you have any experience you can share on MI doctrine, professional development, or "how-to" tips, please send them to ***Military Intelligence***. Topics of interest for future issues include: ISR, ENDURING FREEDOM, global conflicts, MI skills training, and tactical operations. E-mail them to michael. ley@hua.army.mil or call (520) 538-0979 or DSN 879-0979.

AIMP Corner

Changing the Fundamentals of Intelligence

by Brad T. Andrew

The duty of the G2 is to give his commander the threat, weather, and terrain information he needs.[1]

—Colonel Richard J. Quirk, III

Most would agree that Colonel Quirk's description (now MG Quirk) is the essence of the G2's job and represents the fundamental requirements for Army Intelligence. Yet, the impact of the cyber domain, geospatial information, and the requirement to address private volunteer organizations (PVOs) and the local population as part of battlespace environment go far beyond providing information on weather and terrain.

We also know that over time new technologies and techniques become available to improve how we accomplish our duties. Developing the concept of anticipatory intelligence operations may "systematize" something that has always been done in a manner similar to the formalization of the IPB process. We need to develop, practice, and refine knowledge management skills and tactics, techniques, and procedures (TTPs). Army intelligence must master the ability to form collaborative teams of expert personnel. We must improve and standardize the conduct of virtual, collaborative, and distributed intelligence operations, as well as address our role in Homeland Security. The challenge is to adequately identify the fundamental changes in how Army Intelligence will operate as part of the transformed force.

Battle Command; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR); command, control, communications, and computers (C4); and intelligence, surveillance, and reconnaissance (ISR) are terms that **MUST** stand for dramatic change. Army Transformation is based on these capabilities which are focused on seeing first, understanding first, acting first, and finishing decisively. Army Intelligence must establish and then inculcate new ways of "doing business" to ensure the grouping of terms is more than a new acronym.

***Doctrinal Note**: FM 2.0 and follow-on manuals will replace the acronym C4ISR with C2 and ISR to more accurately reflect the respective functional areas.*

FM 3-0, **Operations**, states that Battle Command "is the exercise of command in operations against a hostile, thinking enemy." Battle Command is facilitated through knowledge generation and presentation capabilities in these three areas into the decision-making and operations processes. Through this enhanced Battle Command, the Army, from the individual soldier through the Joint Force Commander, will always *act* with precision and speed that cannot be countered nor withstood. The ultimate goal is to leave your opponent bewildered, exhausted, and overwhelmed by an Objective Force that was able to strike at critical junctures and times, appear where least expected, avoid threat strengths, and seemingly anticipate every move. How will Army Intelligence help make this *Vision* a reality?

C4ISR involves the linkage between C4 and ISR. C4 addresses many aspects to include knowing oneself. The soldier and commander know the status of friendly forces through sensing, automatic reporting, and displaying all friendly force locations and status with complete accuracy in real time. This answers the question "where are my buddies?" With the C4 network serving as the foundation for sharing this understanding, blue force decisions and execution status are likewise immediately known throughout the force. This inherently facilitates friendly force synchronization. While not underestimating the associated challenges, the C4 network is primarily a function of employing sensors and soldiers and providing an assured data transport network to process and display the blue information. By definition this activity occurs in a cooperative manner.

While using the same embedded C4 data transport and presentation capability, the ISR challenge is fundamentally different. Knowing the threat force locations, capabilities and intent occur in a noncooperative environment. The threat is purposefully employing camouflage, concealment, and deception (CCD) techniques and attempting to execute operations to retain the initiative and advantage. How Army Intelligence systematically collects in order to discover the threat's attempts to conceal strengths, weaknesses, and intentions is the key to determining new Intelligence fundamentals. It begins with the concept of anticipatory intelligence operations.

At the onset of operations, Army Intelligence must provide the initial knowledge foundation on the battlespace and threat required for friendly force planning. Freed from the mechanics of establishing ad hoc ISR communications links, Army Intelligence must focus on acquiring data, information, and knowledge on the battlespace and opponent. Knowledge "management" focuses

on answering the questions: What do we know? What don't we know? How do we cover the information gaps? What is available? Where is it located? How do we get it? From what we know, what is the threat capable of doing and likely to do? And, most importantly, what is the commander likely to need? How do we provide it in the most understandable and useful manner? To provide relevance to the decision-maker, Army Intelligence analysts must be experts on how to acquire and manipulate existing data and information in order to facilitate knowledge to satisfy those initial requirements.

To accomplish this, Army Intelligence must master the ability to form collaborative teams of expert personnel conducting distributed intelligence operations. Time and effort must be dedicated to developing the organizational construct and the TTPs to perform the associated missions, tasks, and functions on a routine basis. The rapid formation, use, and collapse of these collaborative teams as the norm are fundamental to Objective Force Intelligence operations.

Forward footprint restrictions to achieve rapid deployment and to reduce sustainment and force protection requirements dictate that physical location must not be a factor. The requirement for enroute, real-time intelligence updates to support planning, mission rehearsals, and unit of action operational execution demand that intelligence operations must occur in a virtual environment. These collaborating teams must have access to databases and information and knowledge from throughout the Army, national, joint, theater, multinational, and inter-agency intelligence systems. Seamless, assured connectivity, access, and multi-level security capabilities are fundamental requirements.

In the end, it is Commander's trust that is essential. This trust can only be earned by demonstrating consistent success with our virtual, collaborative, distributed intelligence operations in garrison, on exercises, and in war. The key element in achieving this may be the concept of the Home Station Operations Center (HSOC). As the larger Army attempts to make distributed operations from Home Station a reality, the Army Intelligence role will be fundamental.

We have significantly improved our Brigade and Battalion [reconnaissance and surveillance] R&S planning. Our collectors are becoming more and more effective. However, we have not yet learned how to make full use of the information we collect.[2]

—Major General H. G. Taylor

Endnotes

1. Colonel Richard J. Quirk, III, "Intelligence for the Division – A G2 Perspective" (Carlisle Barracks, PA: U.S. Army War College, 1992), p. 315.

2. Major General H. G. Taylor, "Memo to Newly Assigned S2s" (Fort Stewart, GA: HQ, 24th Infantry Division (Mechanized), 29 September 1989), p. 1.

LTC (Ret) Brad T. Andrew is a Futures analyst at the Army Intelligence Master Plan. His active duty assignments included Commander, 303d MI Bn (Operations), 504th MI Bde, Fort Hood, TX; Deputy Director of Operations, 718th MI Group, Bad Aibling, Germany; J2 JTF-Bravo, Soto Cano, Honduras; and Force Integration Staff Officer, HQDA DCS G3. He has a Masters in Military Arts and Science from Command and General Staff College, Fort Leavenworth, KS, and a BS in Engineering from U.S. Military Academy, West Point, NY. He is also a graduate of the National Security Agency (NSA) Junior Officer Cryptologic Career Program and earned a Space Operations specialty at Peterson Air Force Base, CO. You may contact him at Brad.Andrew@hqda.army.mil or (703) 824-4136 or DSN 761-4785.

Updated FDIC Web Sites on the Way at Fort Huachuca

The Futures Development Integration Center at the U.S. Army Intelligence Center is breathing new life into its elements' web sites by bringing all of the sites under a centralized umbrella to maintain continuity and improve the sites' appearance. Each site has a unique address in the form of http://<**www** or **directorate** or **secure**>.futures.hua.army.mil.

Current Open FDIC Sites

www	Central launching point	**abio**	Army Broadcast Intelligence Office
bcbl	Battle Command Battle Lab-Huachuca	**dcd**	Directorate of Combat Developments
forcedesign	Force Design Division	**jstars**	Joint Surveillance Target Attack Radar System
kaps	Knowledge and Program Services	**nsto**	New Systems Training Office
tencap	Tactical Exploitation of National Capabilities	**tsmuav**	TSM Unmanned Aerial Vehicle
tsmprophet	TRADOC System Manager (TSM), Prophet	**weather**	Army Weather Support Team

Current Secure FDIC Sites (password control software)

secure secure site with doctrine and web enabler sites (uses Army Knowledge On-Line login/password)

Sites Under Development (will be active in a few months)

MIPB	(out of date site available at http://huachuca-usaic.army.mil/mipb/mipbhome/welcome.htm)
car	Concepts, Architectures & Requirements
tsmasas	TSM All-Source Analysis System
weather	(on the https://secure.futures.hua.army.mil site)

Doctrine Corner

by Chester F. Brown, III

As this issue of MIPB is read and passed among the members of your unit, so too will the draft versions of the two newest Military Intelligence (MI) field manuals: FM 2-0, **Intelligence**, and FM 2-01, **Intelligence Synchronization**. These manuals, combined with FM 2-01.3, **Intelligence Preparation of the Battlefield**, form the first iteration of MI manuals being revised to take into account the Operational Environment (OE). FM 2-0 supersedes FM 34-1, Intelligence and Electronic Warfare; FM 2-01 supersedes both FM 34-2, Collection Management and Synchronization Planning and FM 34-2-1, Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance.

These manuals reflect only one facet of the MI Corps' effort to more closely align MI doctrine with Army operational (combined arms) doctrine. Revising MI doctrine is part of a larger Army effort to implement positive changes based upon lessons learned in combat; observations from Combat Training Center (CTC) exercises; CTC intelligence, surveillance, and reconnaissance (ISR) trends reversal issues; and use of operational terms instead of MI specific—stove piped—terms. This article addresses the changes to the manuals identified above.

FM 2.0, Intelligence. The three most fundamental changes in FM 2-0 (FM 34-1) are changing the title, replacing the Intelligence Cycle with the Intelligence Process, and instituting the new intelligence tasks. The new title, *Intelligence*, mirrors that of FM 3-0, Operations. This title is not only simpler but also more accurate. The former title of the MI capstone manual led one to incorrectly surmise that MI does only two things: intelligence and electronic warfare (EW). However, these two functions are distinctly separate. MI and EW are essentially mutually supporting actions in that you cannot perform all-source intelligence without EW and you are unable to perform effective EW without accurate intelligence. EW is more properly placed in its role of supporting operations in general and targeting specifically. By dropping EW from the manual's title, we also underscore that EW is a function—not the reason for the existence of the MI Corps.

A more complex change replaces the Intelligence Cycle with the Intelligence Process. At first reading, one may consider this change to be one of semantics—mirroring the titles of the Operations Process, the Targeting Process, and the Military Decision-Making Process (MDMP). However, the change goes beyond merely substituting words. It more accurately reflects the continuous and inherently flexible nature of a *process* versus the sequential method presented in a *cyclical model*. Let us examine how we present this information in FM 2-0.

The first two steps of the Intelligence Process and the Operations Process remain the same—**Plan**

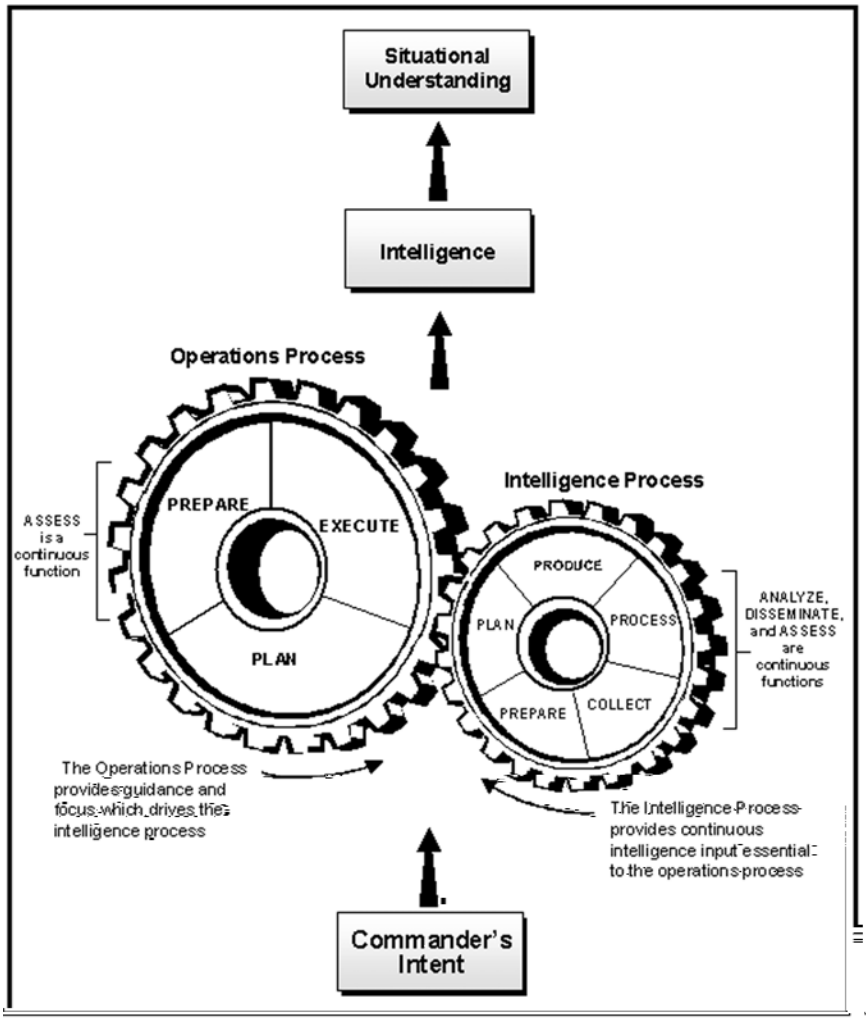


Figure 1. The Relationship between the Operations and Intelligence Processes.

and **Prepare**. We have broken down the third step of the Operations Process—Execute—into the separate steps of **Collect**, **Process**, and **Produce** within the Intelligence Process. Essentially, these are the actions MI systems and soldiers perform during mission execution. The fourth component of the Operations Process—**Assess**—is presented as a continuous function. This is also how it is presented in the Intelligence Process; however, we add two more components that are performed continuously: **Analyze** and **Disseminate**.

We recognize there is an inherent danger in interpreting the Intelligence Process as a sequential methodology, such as the MDMP. We are however, striving to avoid this pitfall by explaining the Intelligence Process in FM 2-0.

Before attempting to understand the Intelligence Process, one must first understand the Operations Process. The Intelligence and Operations Processes are not only complementary but also cannot function effectively without the other. While Figure 1 attempts to show the strong relationship between the Intelligence and Operations Processes, it is important to note that the gear representing the intelligence process is smaller than that representing the Operations Process. This portrays the frequently encountered situation where the Intelligence Process runs through several iterations before the Operations Process completes a single iteration. This is particularly true during the Plan and Execute phases of the Operations Process. It is during these phases that the Intelligence Process may be completed hundreds, sometimes even thousands, of times for each completion of the Operations Process.

The next major doctrinal change presented in FM 2-0 is the subordination of the Intelligence Tasks described in FM 3-0 under the Intelligence Tasks listed in the FM 7-15, **Army Universal Task List (AUTL)**. This subordination is intended to avoid the past confusion that resulted in soldiers referring to the tasks as outlined in several documents (the AUTL, FM 2-0, FM 3-0, or the MI core competencies). Figure 2 shows how we presented the Intelligence Tasks in FM 2-0.

As you can see, we have retained the current Intelligence Tasks identified in FM 3-0 within the AUTL tasks. While some intelligence tasks apply to more than one AUTL task, AUTL procedures limit us to subordinate each task under only one AUTL task.

FM 2-01, Intelligence Synchronization. The doctrinal changes we present in FM 2-01 are also focused on supporting the Operations Process. The most significant changes between FMs 34-2 and 34-2-1 and those presented in FM 2-01

INTELLIGENCE TASKS	COMMANDER'S FOCUS	COMMANDER'S DECISIONS
Support to Situational Understanding **- Perform IPB** **- Perform Situation Development** **- Support to Force Protection**	**Plan a mission** **Secure the force**	**Which COA should I Implement?** **Which enemy actions are expected?**
Support to Strategic Responsiveness **- Perform I&W** **- Intelligence Readiness**	**Orient on contingencies**	**Should I Increase the unit's level of readiness?** **Should I Implement the OPLAN?**
Intelligence, Surveillance, and Reconnaissance **- Perform Intelligence Synchronization** **- Perform ISR Integration** **- Conduct Reconnaissance** **- Conduct Surveillance**	**Plan the mission**	**Which DPs, HPTs, etc., are linked to the enemy's actions?**
Support to Effects **- Support to Targeting** **- Support to IO** **- Perform BDA**	**Destroy/suppress/ neutralize targets** **Relocate intelligence and attack assets**	**Is my fire (lethal or non-lethal) and maneuver effective?** **Should I refire the same targets?**

Key: BDA - Battle damage assessment
COA - Course of action
DP - Decision point
HPT - High-payoff target
IPB - Intelligence processing of the battlespace
IO - Information operations
I&W - Indications and warning
OPLAN - Operations plan

Figure 2. Intelligence Tailored to the Commander's Needs.

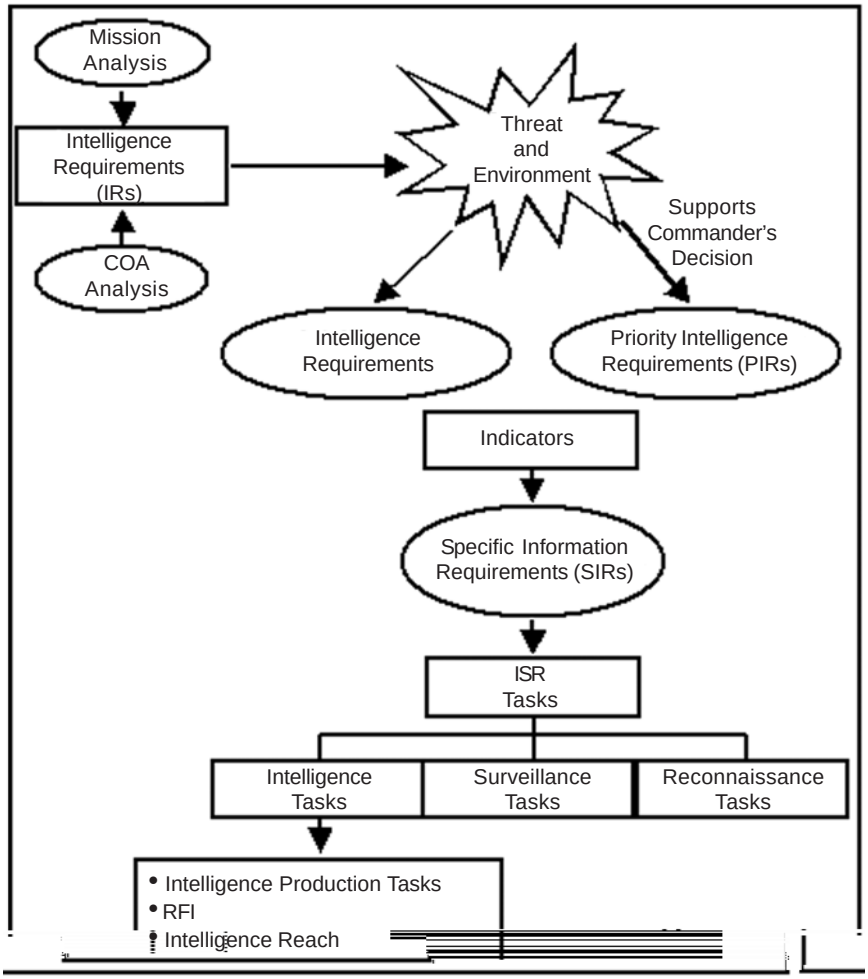


Figure 3. ISR Task Development Process.

relate to the ***requirements management*** process and who exercises control of the effort.

The first noticeable change is replacing the term "collection management (CM)" with the term "Intelligence Synchronization." We avoid using reference to collection manager. These terms specify an intelligence, surveillance, and reconnaissance (ISR) effort under the control, direction, and authority of the G2/S2 and infer a unilateral intelligence effort separate and distinct from the (maneuver) operation or control of the G3/S3. **The sole reason why we conduct tactical ISR operations is to support the commander, whose operations are in turn controlled by the G3/S3.** The ISR effort must be synchronized and integrated into the operation, not serve as a standalone or complementary effort.

This closer integration necessitated a change in the language we previously used to describe the actions of the Intelligence Battlefield Operating System (BOS) when conducting ISR operations. We no longer refer to an ISR collection task or request as a specific order and request (SOR). Instead, we now employ three distinct categories: intelligence tasks, surveillance tasks, or reconnaissance tasks. Furthermore, we have devolved the ISR into three separate components: intelligence production tasks, requests for information (RFI), and intelligence reach tasks. Figure 3 explains this methodology.

We request that you carefully review these new MI manuals when they arrive at your unit. We especially need your input to validate their doctrinal concepts because you have the most recent experience in the operational environment, and each of you has a different perspective of probable future operational environments. Your insight and ideas for improving how MI supports the force are valuable to provide optimal intelligence support to our commanders. Our soldiers and leaders deserve the best intelligence, and you hold the keys to determining how best to accomplish this endeavor. Please forward your recommendations, comments, or questions to Mr. Chet Brown, Operational Environment Doctrine Team Leader, at chester.brown@hua.army.mil, (520) 533-7831, or DSN 821-7831.

Commanders' Safety Course Online—Mandatory for New Commanders

The new Commanders' Safety Course that helps to turn commanders and other unit leaders into their own safety officers is up and running on the Internet. The course, equivalent to 30 classroom hours, gives commanders and first sergeants the tools and knowledge to manage their own safety programs.

The course will be mandatory for all commanders through brigade. Officers selected for brigade and battalion command will complete the course in conjunction with their precommand courses. Captains must take the course as self-development training before company command. Other leaders, soldiers, and employees can also take the course for self-development.

The URL for the website is https://www.aimsrdl.atsc.army.mil/secured/accp_top.htm. You will need a user ID and password but the system will issue those after enrollment. Officers selected for command will be issued a user ID and password when they receive notification from ATRRS (Army Training Requirements and Resources System).

Proponent Notes

by Lieutenant Colonel Eric W. Fatzinger

In this issue we will focus on promotions to include some initial analysis of recent board results. What is clear is that while many things are changing with Transformation, some things remain the same. Selection for promotions is certainly one of those. It is still important that efficiency reports, be they officer or enlisted, paint in clear and unambiguous language the quality and potential of the individual. Having the right job remains a priority but doing each job well remains the key to success on any board.

LTC Eric W. Fatzinger
Director, Office of the Chief, MI
Email: eric.fatzinger@hua.army.mil

Enlisted Actions.

SGM Crossman: Email:
walter.crossman@hua.army.mil

As we begin a new year, I have chosen to provide a few notes on a topic near and dear to all soldiers' hearts: promotions! Specifically, I want to talk about CY02 SFC Promotion Board results, SFC Promotion Board after-action review (AAR) comments, and the re-sequencing of enlisted Centralized Promotion Boards.

SFC Promotion Board Results: Overall, MI did well on the SFC Promotion List released in August 2002. The 33 CMF and 96 CMF came in at 36% and 31% promotion rates, respectively, which put them above the Army Average of 27%. Unfortunately, the 98 CMF was a different story; it came in at only 14%. Military occupational specialties (MOSs) 98H, 98J, and 98K had especially low selection rates for this board. In large measure, the problem is that all of these MOSs are currently above 100% fill at the SFC level and therefore promotion opportunities were hard to come by. Office of Chief, Military Intelligence (OCMI) is researching ways to realign the grade pyramids for these MOSs in the hope of increasing future promotion opportunities.

SFC Promotion Board AAR Comments: The AAR comments from the 2002 SFC Promotion Board were informative and clearly identified ways that soldiers could improve their chances of being selected. The AAR comments can be viewed in their entirety on the OCMI web page at http://138.27.35.32/ocmi/ or by going through the Military Intelligence Center home page at http://usaic.hua.army.mil to OCMI under the Training/MI Professionals department.

I want to highlight one area that continues to be identified as crucial to your chances for promotion. That is the importance of well-written Noncommissioned Officer Evaluation Reports (NCOERs). The AAR comments noted that in NCOERs, the first bullet of each section needs to be the **most** influential and **must** have quantifying data. Promotion Board members have only a limited amount of time to review each file. It is important that the most important and strongest statements are not buried behind excessive verbiage. The AAR also highlighted that in those MOSs that routinely write reports (96 and 98), the rater must be specific as to why a given soldier's report writing is unique (numbers, content, accuracy, and complexity). The board noted that all too often the basis for an excellence rating was simply that the soldier produced "x" number of reports, with no further amplifying data.

Re-Sequencing of Enlisted Centralized Promotion Boards: In the summer of 2002, the Department of the Army (DA) released details on the re-sequencing of Enlisted Centralized Promotion Boards. It was emphasized that the current sequence of conducting boards and the release dates for results often caused problems in filling Advanced NCO Course (ANCOC) and Sergeants Major Course (SMC) class seats. Further, that the sequence resulted in short notice permanent change of station (PCS) notifications that adversely impacted soldiers and their families. Once fully implemented, the release dates for the enlisted boards will be as follows: Command Sergeant Major (CSM), Sergeant Major (SGM), and SMC released in mid-September, MSG released at the beginning of January, and SFC results released in mid-April. These new release dates will allow U.S. Total Army Personal Command (PERSCOM) to more effectively manage assignments as they relate to school seats and PCS moves. In order to make this change, FY03 and FY04 Centralized Boards will be adjusted as needed. The biggest impact of this proposal will be a larger than normal selection zone for the FY03 SFC Board, and no FY04 SFC Board at all. In FY05 the new sequence will be fully in place.

Upcoming NCO Boards. The 2003 MSG Selection Board will be held in February 2003 with May as the expect release date for results.

Warrant Officer Actions.

CW5 Castleton: email:
lon.castleton@hua.army.mil

FY02 Warrant Officer Promotion Board Results: Congratulations to the latest selectees for promotion to CW3, CW4, and CW5. MI did extremely well on Warrant Officer (WO) promotions this year. The average selection rate for technical services WOs, first-time consideration in the primary zone for CW5, was 38.8% and for aviation WOs 46.3%. For MI

WOs the selection rate was 57.1% (4 selected of 7 considered; 1 of 9 selected above the zone). The selection rate for MI WOs to CW4 was 88.9% (16 of 18 PZ, 1 AZ, 1 BZ) and for CW3, 90.9% (110 PZ, 4 AZ, 3 BZ).

FY03 Promotion Preparation: What did it take to get selected for promotion this past year? First, sustained superior performance as reflected in OERs; next, a personnel file that has been maintained and is current. Also, clearly written and understandable OERs, both in the duty descriptions and narratives. Stay away from MI acronyms ("SIGINTers," especially, remember who's on the board!). Other keys to success include being actively involved in your career management right from the start, completing both your military and civilian education, staying technically proficient through developmental assignments and training, and seeking recognized leadership positions at some point. It is not too early to start preparing for next year's promotion board right now. Here are some steps you can take to ensure that the board is presented with the best "picture" of you and your qualifications:

- ❑ Review your microfiche now to ensure it is complete and that all the documents on it are yours. If you review it now, you will have time to get any documents not on the fiche in to PERSCOM. Don't wait until the last minute. Your assignments manager will be very busy getting all eligible records ready for the board, so start your review now.
- ❑ Ensure that you have a current photo and that all awards shown in your photo are reflected in your microfiche. Again, do not wait until the last minute because the photo lab will be flooded with soldiers trying to get their photos updated at the last minute. Remember that photos are only *not* important if *everything* is squared away. If something doesn't look quite right, the photo reportedly can quickly become a discriminator.
- ❑ Review your officer record brief (ORB) to ensure it matches your microfiche.
- ❑ Have a Senior Warrant Officer in your field review your files to ensure that you have done all you can to present yourself in the best light.
- ❑ On OERs put leadership up front. Note the scope of responsibilities, eliminate the words "responsible for," use action verbs, and keep it simple. Senior rater comments must address promotion potential and assignment potential. Senior rater comments are critical due to the limited number of above center of mass ratings allowed.

FY04 MI Warrant Officer Accessions: Accession numbers for the recruiting year for MI are expected to remain constant at around 140 for our 12 MI MOSs. MI accession boards are held in March, July, September, and January. (Note: Not every MOS is accessed at every board.) January 03 will be the last accession board for FY03. The opportunity to become an MI warrant officer has never been better. If you are an NCO interested in applying, please apply as soon as you are eligible. If you are an MI leader who has outstanding NCOs working for you, please point out the great warrant officer promotion statistics and the many benefits in becoming an MI warrant officer. Currently there are 63 approved recommendations going through the implementation process which will improve warrant officer pay, training, education, and remove some of the disincentives to NCOs and units to becoming a warrant officer. Most importantly, reenlistment bonuses will be retained in the future and units will be able to requisition replacements in a more timely manner to replace soldiers selected for warrant officer. Check out the U.S. Army Recruiting Command (USAREC) homepage at http://www.usarec.army.mil/hq/warrant/ for a listing of all MOSs, prerequisites, and application procedures.

Upcoming WO Boards. The next Accessions Board for WO Candidates will be held in January 2003 and the next WO Promotions Board is to be held in May 2003.

Officer Actions.

Ms. Borghardt: email charlotte.borghardt@hua.army.mil

FY02 Army Competitive Category Major Promotion Board Results: The results of the FY02 Major Promotion Board have been released. Overall, MI did better than the Army average with a 93.1% selection rate compared to 89.5%. This latest selection rate shows a marked increase from the previous year (79.8%) and may be partially explained because this is the first of several year groups (92 through 96) which were under-assessed and highly attrited.

FY02 Major's Board AAR Comments: Branch Qualification, as outlined in DA Pamphlet 600-3, is the first thing a board member looks for when assessing a Captain's file. No MI Captain without a command has been selected for promotion in the last three years. After that doing well in all jobs is critical. The competition for, and limiting factors on, above center of mass ratings has required board members to spend more time on, the senior rater's portion of the report, particularly where he has a small number of officers in that grade or has an immature profile, as is the case with many MI senior raters. Bottom line here is that quality officers who have quality performance reports, but where all the reports are not above center of mass, are still competitive for promotion. In many instances, an officer could have several (majority) of his reports center of mass with strong words from the senior rater, and if the command re-

port was above center of mass, he was considered highly competitive. Conversely, officers who had a center of mass command report with mediocre words in the senior rater write-up and with a mature profile were not as highly competitive, even with a majority of above center of mass reports in their files. Again, doing well in all jobs and strong senior rater comments make the difference in the final analysis. The center of mass or above center of mass rating is an indicator, but the comments portion will be the final determination in the mind of the board members as they assess and rank the overall manner of performance of the entire file.

FY02 Career Field Designation Board: There were 11% of MI Officers who were in career field designators this past summer that were selected for career fields outside operations (basic branch). This translates to 19 out of 172 MI officers who switched from the Operations Career Field to one of the Army's new functional areas (FAs). The good news for MI is that 8 of these officers, representing the largest single group, were selected for FA 34, Strategic Intelligence, in the Information Operations Career Field. While these MI officers are no longer part of the Operations Career Field and in the "Command Track," they are the cornerstone of the Army Intelligence Corps at the echelons above corps level and act as the bridge between Corps, Theater, and Strategic echelons. FA 34 Officers are an integral part of our Army Military Intelligence force providing regional and functional intelligence expertise through focused repetitive assignments. All personnel policy issues for FA 34, as are all MI (35) Branch issues, are managed by the same Proponency Office OCMI.

Upcoming Officer Selection/ Promotion Boards: Colonel Command Selection Board is scheduled in 2003 to be held 7-17 January; LTC Promotion Board, 25 February-28 March; Senior Service College, 1-25 April; MAJ Promotion Board, 15 April-16 May; CPT Promotion Board, 6-27 May; Year Group 1993 CFD Board, 17-27 June; and Colonel Promotion Board 29 July-22 August.

FOOTNOTE:

The OCMI website can be reached by going to the Intelligence Center Homepage at http://usaic.hua.army.mil/ and then linking to OCMI with the Training/MI Professionals icon. You will be able to find information on issues ranging from enlisted career field overviews to officer, warrant officer, and civilian updates.

Enduring Freedom

(Continued from page 66)

Lessons Learned.

- Home station training must include all reporting formats and focus on what the unit will do in a war. Units need to ensure their METL is up to date and reflected in their JRTC rotation.
- UAV systems need to have a dedicated focus and mission, coupled with an analysis of mission data to better prepare the unit for what they will be facing.
- Soviet-Afghanistan lessons learned are still valid, especially in mine awareness and how the mountain fighters fight and hide.
- There must be a dedicated MI communications system or O&I net, especially at the brigade level. Too much information goes over the command net and NetMeeting chat to sort through relevancy and capture data.
- Piecemealing information forward does work. This allowed the units to begin the planning process, as they were still collecting and analyzing information. Higher staffs then pushed follow up data to the unit so the fighters had a somewhat common picture.

Contact with the 202d MI needs to occur. They took back AlQaeda tactical training programs (TTPs) and training manuals captured during operations.

From Major Scott Brown: The JRTC Movement to Contact phase needs to be more chaos-oriented to prepare us. We even need to be able to hire locals who in turn try to collect intelligence from us to both work the mess tent at the ISB and during the defense, to fill sand bags to replicate civilians on the battlefield and local hire civilians. This is what is happening in theater. This being said, JRTC, NTC, and CMTC have been directed and are in the process of transitioning from the Soviet form doctrinal fight to what we now call the contemporary operational environment (COE). For further detailed explanation on what COE is, refer to http://call.army.mil/Products/Ctc/COE-handbook/coe-toc.htm for the **COE Handbook**, **How to Fight at the CTCs** on the CALL Gateway.

Sergeant First Class Rob Ehrlich is the Senior Training Management noncommissioned officer (NCO) and Team noncommissioned officer in charge (NCOIC) for the Center for Army Lessons Learned (CALL) Cell at the JRTC. He is responsible for the collection and distribution of information, trends, and data for CALL and the JRTC. He previously served as an observer-controller in the JRTC Operations Group for four and one-half years.

TSM-ASAS Corner

The Little Computer That Could.....

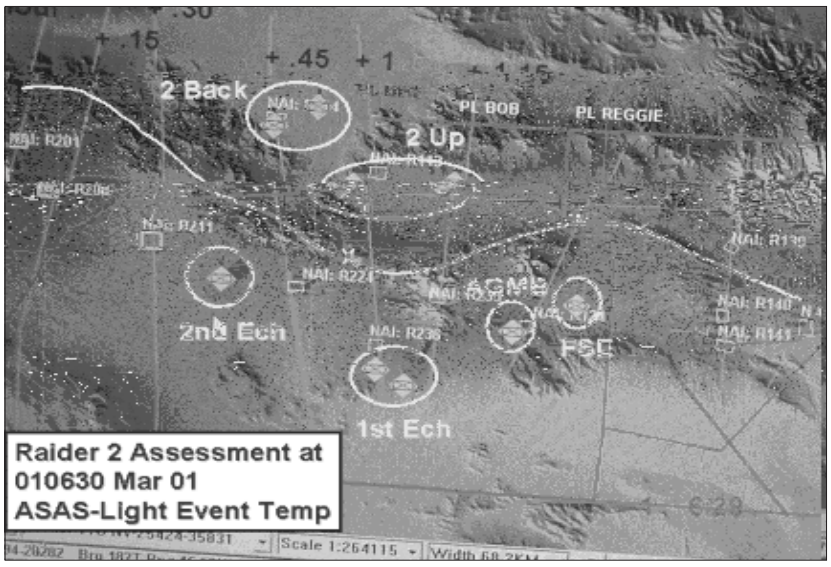
by COL Mike Gearty

Who you gonna call?

When you need something done around your unit, who is it that you turn to? If you are like me, there is no one in the unit that you appreciate more than that young "can do" Sergeant. This is the person that works well as a team member, yet is always striving for the opportunity to be the team leader. When he or she attacks new problems, especially those "impossible" technical ones, they do so with a confidence and dogged perseverance that make you proud to be their leader, peer, or subordinate. When observing this super-Sergeant's intensity and ingenuity, if you find yourself marveling at his or her versatility, you aren't alone. The MI Corps, with our complex and time-sensitive missions, has long placed great value on the versatility of the individual. Now, if only our systems could be more like that Sergeant!

I would be misrepresenting the truth to you if I told you that the All-Source Analysis System (ASAS)-Light could in any way equal the Army's best and brightest. However, because of its unique and emerging versatility, ASAS-Light is quickly becoming the "can do" system in the ASAS family of systems. Aside from the obvious cost benefits associated with this smaller system, the ASAS-Light has, in recent months, provided several multifaceted solutions to assist our best and brightest to overcome some difficult obstacles.

The requirement for a portable, lightweight ASAS was identified during several training events between 1998-2000. It became obvious during these exercises that despite making great strides at the brigade level, S2s at battalion-level, within separate brigades, or within special operations units were not brought into the "digital fold." In order to quickly resolve this deficiency, the materiel developer implemented an innovative design approach that combined Government off-the-shelf (GOTS), commercial off-the-shelf (COTS), and custom software, layered upon a segmented Defense Information Infrastructure Common Operating Environment (DII COE) applications layer. As a result, the program manager TSM-ASAS team was able to go from requirements development to a milestone fielding decision in less than two years. It has also become the first Windows-based, commercial ruggedized laptop Army Battlefield Command System (ABCS) ever approved for fielding. I am proud to say that today the ASAS-Light provides the Military Intelligence Corps with a low-cost laptop intelligence analysis system that meets the peacetime and wartime requirements of the tactical user. Demand for the ASAS-Light has been bubbling up from all corners of the intelligence community. Many units have used their own funds to purchase approximately 600 ASAS-Light over the past 18 months. The word is out!



Courtesy of 4ID AAR on ASAS-Light

Into the breach…

In the best tradition of American military creativity and innovation, local unit commanders often temporarily modify the allocation of their resources in order to best accomplish the mission. During the III Corps' Extended Warfighter Exercise (EWFX) and 02-05 rotation last spring, the 4th ID Commander employed ASAS-Lights with the division and brigade headquarters. Within the D-MAIN, the ASAS-Light was used to build the current enemy situation picture and a predictive analysis model that included 12-, 24-, and 48-hour snapshots of projected enemy dispositions.[1] The system was also used to speed up the scheduled threat updates to the Joint Common Database (JCDB). The ASAS-Light worked as an effective presentation device as well as a division intelligence, surveillance, and reconnaissance (ISR) management tool. This versatility was enhanced by the system's inherent stability, robust and usable map package, and rapid boot-up capability.[2]

Taking on the tough jobs… non-traditional threat and collection management

The Nontraditional Threat Intelligence Toolkit (NTTIAT) (originally designated the Stability Operations and Support Operations (SASO) Toolkit) was developed to respond to the increasing need for an ASAS tool tailored for a Balkans-like operational environment. NTTIAT was the result of a collaborative effort between Program Manager-Intelligence and Effects (PMIE), V Corps, and TSM-ASAS and is currently being validated at the Multinational Brigade (East) in Kosovo. As the software continues to get shaken out and improved, TSM-ASAS is considering how the NTTIAT, installed on the ASAS-Light, can be approved, leveraged, and funded to key locations throughout the force.

The starting point was a simple one: How can we modify the ASAS-Light so that it could perform intelligence preparation of the battlefield (IPB) against an asymmetrical threat (for example, terrorist, criminal, untraditional, unconventional)? In order to do this, we knew that a critical priority must be the enhancement of the current database schema to address individuals, events, and organizations (IE&O). The NTTIAT database accepts IE&O data from Crime Link, Web Quick Forms, Analyst Notebook, custom data from MS Excel and Access, and the EOBSREP (S303) and ENSIT (S309) U.S. Message Text Format (USMTF) messages. And in an effort to simplify training, NTTIAT uses an import wizard to simplify and integrate multiple disparate data sources.

A number of other tools are components of the NTTIAT. A 3D visualization tool allows the operator to apply threat domes for more realistic surface-to-air missile (SAM) and antiaircraft (AA) and antiaircraft artillery (AAA) range fans. Visual lines-of-sight (LOSs) can also be displayed with transparent colors to delineate viewable and obstructed areas. Using the Open-Source Automated Link-Analysis Tools (OSALAT) the operator can search databases via the Nonclassified Internet Protocol Router Network (NIPRNET), organize the results, build cases, and export the results to the IE&O database. Examples of the relationship between OSALAT searches and the IE & O database are shown below in Figure 1.

Another important feature is the Intelligence, Surveillance, and Reconnaissance Automated Toolset (ISR-AT), which was added to provide user-friendly generation and maintenance of priority intelligence requirements (PIRs), information requirements (IRs), specific information requirements (SIRs), specific orders and requests (SORs), and collection assets. As the analyst adds data to electronic "index" cards, an intelligence synchronization matrix (ISM) is automatically generated. This can be posted to the ASAS Web and simultaneously to the Unit Web or alternate web site with one click.[3] Altogether, the NTTIAT, when fielded, will provide a powerful analytical capability to both new and advanced users.

Digital Liaison

During validation testing with the Marine Corps, the ASAS-Light was called upon to not only facilitate the transfer of data but also to visualize the data through the use of overlays. In this case, the versatile ASAS-

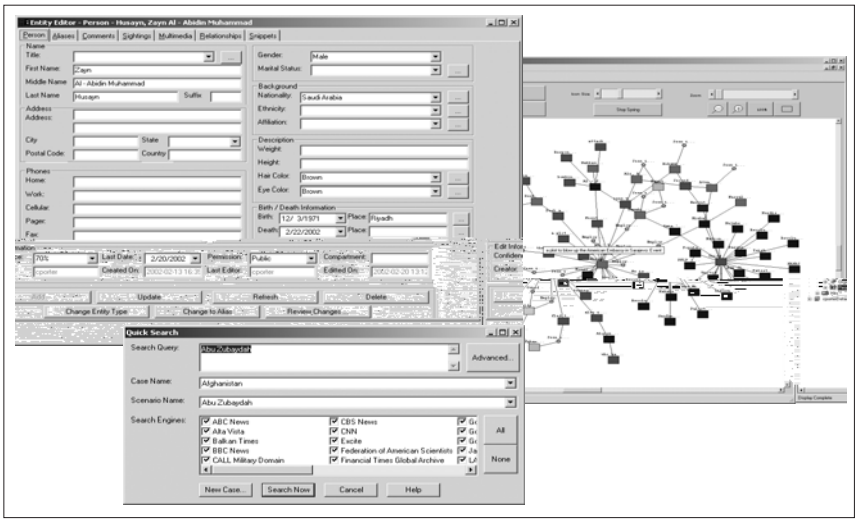


Figure 1. OSALAT and Link-Analysis Screen Shot.

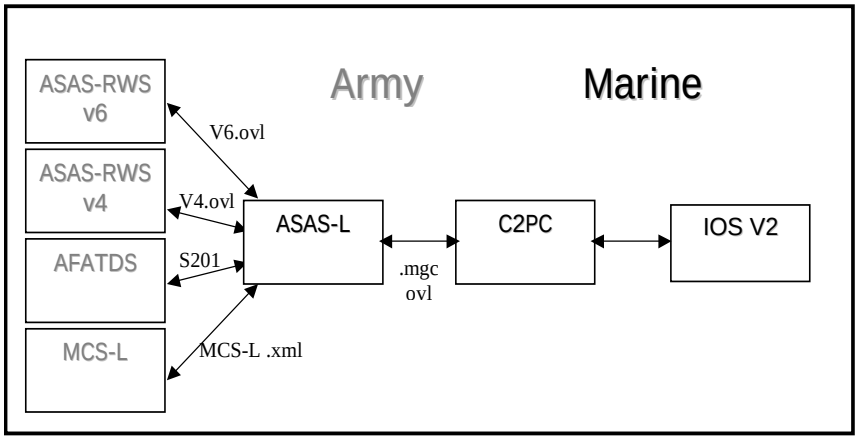


Figure 2. ASAS-Light Format conversions.

Light stepped into the gap, at least on an interim basis, to serve as a "digital liaison."

In an effort spearheaded by the 513th MI Brigade, a few ASAS-Lights have been modified to exchange overlays with the Marine Corps-based Command and Control Personal Computer (C^2PC) software. C2PC is a client application that displays tactical track data from a UNIX-based Tactical Database Manager (TDBM) data server. It is also used extensively within the Army. ASAS-Light converts Army formatted Overlay messages to a ".mgc" format that is the standard for C^2PC; or, in turn, takes the USMC C^2PC formatted Overlays and converts them to the Army ".ovl" format, as shown in Figure 2.

Even with this interim fix, interoperability challenges continue to careen around every new corner at us. However, if the past is an indicator of the present, the ASAS-Light software baseline has shown a propensity to offer quick solutions.

On the horizon!

With much of the planned fielding completed for the ASAS-Light, TSM-ASAS is rapidly assessing the way ahead for this useful tool. The outstanding characteristics of the ASAS-Light—versatility, portability, responsiveness—represent the heart of the Army and Department of Defense Transformation effort. This proven software will likely serve as an important fusion platform as we move toward the future; acting as a critical bridge to the Objective Force.

For the time being, however, the ASAS-Light's slate is full. Much work is still needed in order to completely leverage the capabilities of the ASAS-Light within the rapidly maturing Stryker Brigade Combat Team (SBCT) units. Headquarters, INSCOM, has begun some initial experimentation with the ASAS-Light in order to eventually modify it for a unique echelon above corps (EAC) mission. Finally, TSM-ASAS is regularly reviewing unit architectures and basis of issue plans in order to ensure the right mix of remote workstations (RWS) and ASAS-Lights exist within the Army.

With all of these challenges, the ASAS-Light remains a proven performer. Like that versatile "go to" sergeant in your unit, the ASAS-Light stands ready for your next mission.

(Special thanks to John Loth of Austin Information Systems, MAJ Nicole Brooks and CW3 Dennis Karambelas of the 4ID; and CW3 David Kuroda of the PMIE ASAS-Light Product Team.)

Endnotes

1. 16 Apr 02, MAJ Nicole Brooks and CW3 Dennis Karambelas.

2. Ibid.

3. **ASAS-Light Student Handout**, Austin Information Systems, 7 Aug 02.

Website for Future Leaders

CompanyCommand.com is a website (http://www.CompanyCommand.com) dedicated to company-level leaders wanting to learn and share ideas on topics such as command philosophies, Army policies, leadership counseling, officer professional development (OPD), and professional reading programs. Staff and faculty officers at the United States Military Academy at West Point, New York, operate the website during off-duty hours without remuneration.

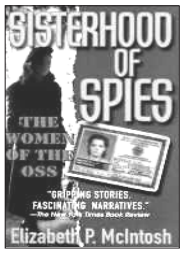
The website meets its goal to improve institutional knowledge at the company-level by facilitating lateral information flow and serving as a user-driven forum whereby former and current company commanders share ideas, products, and lessons learned with others. Majors Nate Allen and Tony Burgess, the site's founders, commented that their sole purpose is helping leaders grow great units and soldiers.

CompanyCommand.com has a section organized by branch that links the experiences and competencies of former and current commanders. For example, it lists for the intelligence community some Military Intelligence contacts including former MI company commanders who are volunteer mentors. The operators of the site plan to expand it with platoon leader tools for junior leaders.

Among the website's other offerings are a "command tools" section with professional presentations, lessons learned, and stories. It also contains quizzes, after-action reviews, tactical scenarios, monthly updates, links to other military websites, and much more. Popularity of the site has increased since its debut in February 2000.

Professional Reader

Sisterhood of Spies: The Women of the OSS, by Elizabeth P. McIntosh (Dell Publishing Company, reprint March 9, 1999, originally published in hardcover by US Naval Institute Press in May 1998), 368 pages, $6.50.



By documenting many tales of the courage and exploits of dozens of women of the Office of Strategic Services (OSS), author Elizabeth P. McIntosh adeptly educates the reader on the history of the OSS while simultaneously telling of the women who pioneered the modern intelligence era. Herself a veteran of the OSS during World War II and then its protégé, the Central Intelligence Agency (CIA), McIntosh more than aptly handles this subject. Her intimate knowledge of many of the OSS officers and operations lends credibility to her expertise in the field, yet she carefully restrains from any obvious bias throughout her discourse in *Sisterhood of Spies, the Women of the OSS.*

In *Sisterhood of Spies,* McIntosh recounts the tales and exploits of women in the OSS, followed by a brief synopsis of their continuance into the modern intelligence community. With this effort she successfully provides the reader with the sense of purpose and excitement felt by these women. Entering the OSS during a time in which the U.S. was entrenched in a world war, these women served in all of the war's many theaters of operation. Casting aside political differences, societal class standing, and education status, these women played key roles in ensuring the success of OSS operations worldwide. Ms. McIntosh begins the book by introducing General William "Wild Bill" Donovan's OSS ends it by addressing women's roles in the modern intelligence community, McIntosh also suggests the importance of the women of the OSS as pioneers. Additionally, she provides many details of the prejudices and adversity the women of the OSS encountered during their tours of duty.

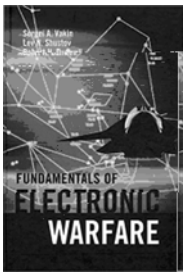
Throughout the twenty accounts of the women of OSS, McIntosh provides evidence of the significant role they played. She relies heavily on interviews, diaries, and existing literature to develop chronicles of each of these women. She further describes how each of them entered the OSS, their role in OSS operations, and their subsequent lives following the termination of the OSS after the war. McIntosh's writing style is narrative in nature and reads like a good spy story; it would be easy to believe that many of the tales were fiction if they were not documented as otherwise. Where appropriate, McIntosh provides personal accounts of her interface with these OSS women, imparting personal details that might otherwise have been overlooked. She is careful not to inundate the reader with personal accounts though most add a great deal to the publication. As evidenced by her vast collection of notes and extensive bibliography, McIntosh went to great effort to ensure her documentation was both accurate and well supported.

Ms. McIntosh's in-depth research and personal experiences allow her success in telling the story of the women of the OSS. Never, during the course of reading the book, will readers find themselves wondering what the rest of the story is about; each tale is that fully presented. This same strength also presents itself as a potential weakness, however. So intent is McIntosh on conveying the atmosphere of the time, that readers may find themselves bored with the details of the societal aspects of these women. It seems, after awhile, as if there is a focus beyond what the women accomplished – more on whom they married and what role in society they played after the war. Readers must try to remember that the vast majority of the women in the OSS came from the upper crust of society and that such details mattered to them, as they apparently did to McIntosh. Needless to say, the book would not have lost anything if such details were omitted.

Like so many books regarding the period, *Sisterhood of Spies* belies a pride in what the U.S. and the OSS accomplished during the time. While rightly deserved, at times the book appears unbalanced as it shows little criticism of the OSS women's efforts. Nonetheless, on the whole the book stands as an authoritative and substantive chronicle of the early contributions of women to the U.S. intelligence community. It is well worth the reading.

Katherine R. Coviello is employed by the U.S. Army Intelligence and Information Warfare Directorate, Fort Monmouth, NJ. She can be reached at Katherine.Coviello@us.army.mil.

Professional Reader



Fundamentals of Electronic Warfare,

S. A. Vakin, L. N. Shustov, and R. H. Dunwell (Norwood, MA: Artech House, 2001)

Fundamentals of Electronic Warfare (EW) introduces the reader to the basic concepts involved in aircraft survivability equipment (ASE), with particular emphasis on defeating antiaircraft (AA) radars. The authors define EW as:

> *A set of measures and actions performed by the conflicting sides to detect and electronically attack enemy electronic systems for the control of forces and weapons, including high-precision weapons, as well as to electronically defend one's own electronic systems and other targets from technical intelligence (electronic intelligence, ELINT), jamming and nondeliberate interference.*

The authors consider all methods of protecting aircraft part of the taxonomy of EW, to include regular jamming of air defense radars (called masking jamming), deception, jamming the radars on high-speed antiradiation missiles (HARMs), and directed energy destruction of radars. All of these are referred to as types of jamming. Jamming is presented as a method of reducing the target's *information stability*. Information stability is the opposite of *information damage*, which is what a jammer attempts to do to a targeted system.

With few exceptions, the material in this book (in particular Chapters 1 through 3) can be applied to all electronic attack (EA) analyses. These chapters present mathematical models of radar and jamming signals as well as models of systems as targets and jamming systems. These models are used in later chapters to analyze the effectiveness of various EW techniques.

Chapter 1 sets the stage for the material to follow. Basic terms are introduced and the problems associated with jamming AA thrusts are presented. This chapter develops mathematical models of the radar and HARM targets.

Chapter 2 presents mathematical models of jamming signals and systems. Application of zero-sum game theory is discussed at the end of Chapter 2 as an interesting way to view the radar and radar jamming situation.

Chapter 3 introduces four jamming effectiveness criteria. The first is based on the amount of information damage a jammer can achieve, and is developed using the tenants of information theory introduced by Shannon in 1948. The second criterion is based on "energy" which refers to the required jam-to-signal-power-ratio (JSR) needed at the radar to be effective. The last two effectiveness indicators of jamming are of particular interest to practitioners of the jamming art. One indicator is based on how usable it is in an operational and tactical environment; the other is based on the military utility considering economic constraints. All but the last one of these indicators have quantitative criteria developed in this chapter.

Chapter 4 introduces the jamming equation and its characteristics. This equation governs the entire jamming process and is used to ascertain the effectiveness of jammers against radars. Discussed are the various aspects of the parameters involved with this equation to include the effects of signal polarization and possible mismatches thereof, the attenuation of signals as they traverse space, and the aircraft radar cross section (RCS). Included are presentations on jamming coherent and noncoherent radars, synthetic aperture radars (SAR), and bistatic radars, as well as using jammers for screening.

Chapter 5 introduces the notions of passive and active-passive jamming. Passive jamming is another appellation for chaff while active-passive refers to combining aircraft survivability equipment (ASE) jamming with chaff by, for example, reflecting the ASE jamming signal off chaff, thereby misdirecting a jamming antiradiation missile (ARM).

The effectiveness of decoys and other forms of false targets is analyzed in Chapter 6. Techniques are presented that increase the RCS of decoys, such as corner reflector for radar signals. Characteristics of expendable thermal decoys, and their effectiveness, are presented for addressing the threat posed by heat-seeking ARMs.

The main point of the last chapter is that radar detection range decreases

(Continue on page 83)

MI Heritage

"Buffalo Bill" Remembered: LTG William W. Quinn

by Katherine Schmidli

The Army transforms and technology evolves. Good leadership, however, transcends change that is recognized by generations of soldiers. Every soldier knows exactly what it means when someone is called a "soldier's soldier": clear and decisive leadership ability; a team builder; one who fosters unit cohesion and strong morale; a leader who inspires loyalty and trust by giving back the same.

Lieutenant General William W. Quinn was a "soldier's soldier." Raised in a middle-class family in Maryland, Bill Quinn knew before he graduated from high school that he wanted to be a soldier. Thwarting his father's plans that he become a lawyer, he entered West Point in 1929, doing it the hard way– by working odd jobs, studying extra for exams, and persevering the old fashioned way. He graduated in 1933.

Due to extreme officer shortages, 2LT Quinn was immediately given command of Company L, 5th Infantry Regiment, Fort McKinley, Maine. Already a common-sense leader, 2LT Quinn called in his First Sergeant and told him:

The first fact I think should be discussed here is that I don't know my ass from third base about running a company. An additional fact is that you and I know it.… I'm going to take your advice and your recommendations as to discipline, of rewards and punishments, of planning, of training, things to do, when to do it, how to do it, the mess, the food, the morale, etc. Now the final fact is that I don't know what I am doing today, but Sergeant Warwick, I will know someday, and it won't be too far off. So I will just let that rest with you.[1]

From 1937-38, 1LT Quinn served as the provost marshal of Manila, in the Philippines. He attended the infantry school at Fort Benning, Georgia, during 1938-39 and Command and General Staff School at Fort Leavenworth, Kansas, in 1941.

It was in the North Africa Theater and subsequently in Italy that Bill Quinn made his mark. In 1943-44, Quinn served as the Division and later as the IV Corps G2 in North Africa and Italy, under the command of LTG Alexander M. "Sandy" Patch. In 1944-45 LTC Quinn was appointed the G2 of the Seventh Army. Although he held the relatively junior rank of lieutenant colonel, he was responsible for coordinating and planning all intelligence supporting the invasion of southern France (15 August 1944).

Four months later, LTC Quinn correctly predicted that a German offensive was planned for New Year's Eve 1944, near Colmar in northeastern France. For this timely intelligence work, he was awarded the Distinguished Service Medal.

Throughout World War II, LTC Quinn worked closely with the Office of Strategic Services (OSS) to receive the latest intelligence on the situation in Germany and France. Although his sources were disputed at the time by more conventional Army leaders, this association with General "Wild Bill" Donovan and the OSS prepared LTC Bill Quinn for his next assignment.

In late 1945 he was named director of the Strategic Services Unit (SSU). His job was to preserve OSS intelligence assets through the post-war drawdown until a national intelligence agency could be formed. In July 1946, LTC Quinn was named chief of operations of the Central Intelligence Group (CIG), remaining in that position until

1947, when the organization became the Central Intelligence Agency (CIA). Had the agents and assets of the OSS (SSU/CIG/CIA) not been saved, Quinn wrote, "the talents of Richard Helms, Harry Rositzke, William Harvey, Alfred Ulmer, Jr., Frank Wisner and William Colby, and some of the other great leaders and minds in the intelligence field, would have been thrown to the winds. Their talents would have been lost, as well as the background and mass of experience and bulk of intelligence that had been collected." [2]

When the Korean conflict began in 1950, LTC Quinn was a member of General Douglas MacArthur's staff. He was put in charge of intelligence planning for the amphibious assault at Inchon. His intelligence preparation for the invasion was thorough and accurate and significantly contributed to one of the most daring and successful amphibious landings in history. T.R. Ferenbach, in ***This Kind of War***, wrote: "the X U.S. Army Corps, 70,000 men, was at sea. It had been formed from scratch, operating against time, manpower, and every known logistic difficulty, and its very conception embodied the best of American military capability.… Whatever the early American participation in the Korean conflict had been, the amphibious assault by X Corps was no small operation. It involved more ships and men than most of the island operations of the Pacific War…."[3]

Promoted to Colonel, he would later serve as the G2 for the Army's X Corps, but in January 1951 he was given command of the 17th Infantry Regiment. It was his first command of combat troops. The 17th Infantry had just received a new call sign– "Buffalo," and COL Quinn decided to call his troops the Buffaloes. The regiment mailed home press releases about the Buffaloes and a short time later war correspondents began to call him "Buffalo Bill." The name stuck. Clay Blair in ***The Forgotten War*** wrote: "Almost overnight the Buffaloes became famous. Hundreds of GIs requested a transfer to the outfit; some even went AWOL to join."[4]

Over the next eight months, COL Quinn was awarded the Silver Star, for personally reorganizing a stalled attack, and the Bronze Star with "V" device, for leading a patrol eight miles behind enemy lines.

Between 1953 and 1955 COL Quinn served as the Chief of the Army section of the Joint U.S. Military Advisory Group (MAG) in Greece. This was followed by infantry command assignments during 1955-57. He was later promoted to Brigadier General and from 1960-61 served in the Pentagon as the chief of the Army's Public Information Division.

In 1961, LTG Quinn was named Deputy Director of the newly established Defense Intelligence Agency (DIA). In 1964 he left DIA to take command of the U.S. Seventh Army in Germany.

LTG Quinn retired in 1966 but continued to serve soldiers and the nation. He was a consultant to the Senate Select Committee on Intelligence and a trustee of the National Historical Intelligence Museum. He was appointed Honorary Colonel for Life of the 17th Infantry Regiment in 1985, and in 1992 he established the 17th Infantry Association to honor all the Regiment's veterans and serving soldiers.

In 1997, LTG Quinn was awarded the Central Intelligence Agency Seal Medallion for his important role in maintaining the nation's intelligence capability between World War II and the onset of the Cold War.

We lost "Buffalo Bill" on September 11, 2000, when he passed away at the age of 92. He was buried at Arlington Cemetery. LTG "Buffalo Bill" Quinn was a groundbreaking intelligence professional and legendary infantry commander and established the high standards expected of a "soldier's soldier."

Note: *Military Intelligence was not officially recognized as a separate branch of the Army until July 1962. Except in organizations like the Counter Intelligence Corps (CIC), OSS, officers who possessed the skills for Army Intelligence were called to serve, but were expected to return to their branch for leadership positions and command time.*

Endnotes

1. William W. Quinn, Buffalo Bill Remembers: *Truth and Courage* (Fowlerville, Michigan: Wilderness Adventure Books, 1991), 33-35.

2. Quinn, 254.

3. T. R. Ferenbach, *This Kind of War Korea: A Study in Unpreparedness* (New York: Macmillan Company, 1963), 257-258.

4. Clay Blair, *The Forgotten War America in Korea 1950-1953* (New York: Random House, Inc., 1987), 616.

Professional Reader

(Continued from page 81)

slowly with reduction in the RCS by physical means. Due to aerodynamic considerations, it is not possible to reduce the physical RCS past a certain point where modern AA radars can still be effective. However, if the reflection characteristics of the aircraft or the atmospheric parameters between the radar and the aircraft can be changed, detection range decreases faster. This is important, for example, for reduction in the power and size of an ASE jammer as well as expenditure rates for passive and active-passive devices. The technologies discussed for accomplishing this include radio frequency absorptive coatings for the aircraft surface and surface design so that reflected radar signals interfere with one another to cancel and reduce the RCS of antennas on the aircraft. Also discussed are the effects of changing the atmosphere between the radar and aircraft by artificial ionization and nuclear means.

Although the book is quite technical, in general, there is enough operational information included to make an interesting read for a non-technical audience. It contains a great deal of mathematics to include some elementary calculus and development and solution of differential equations, but, for the most part, it is not difficult to follow. The math can be skipped with little loss of the information flow. For anyone who wants a relatively thorough introduction to aircraft ASE techniques and their effectiveness, *Fundamentals of Electronic Warfare* is a good place to start.

by Richard A. Poisel

Fort Huachuca, Arizona

Contact Information and Submissions

This is your magazine and we need your support in writing articles for publication. When writing an article, select a topic relevant to the Military Intelligence community; it could be historical or about current operations and exercises, equipment, TTP, or training. Explain lessons learned or write an essay-type thought-provoking article. Short "quick tips" on better use of equipment, personnel, or methods of problem-solving and articles from "hot spots" are always welcome. Seek to add to the professional knowledge of the MI Corps. Propose changes, describe a new theory or dispute an existing one, explain how your unit has broken new ground, give helpful advice on a specific topic, or explain how a new piece of technology will change the way we operate.

Maintain the active voice as much as possible. Make your point. Avoid writing about internal organizational administration. If your topic is a new piece of technology, tell the readers why it is important, how it works better, and how it will affect them. Avoid lengthy descriptions of who approved the new system, quotations from senior leaders describing how good the system is, reports your organization filed regarding the system, etc.

The ***MIPB*** staff will edit the articles and put them in a style and format appropriate for the magazine. You can send articles, graphics and photographs via E-mail to **mipb@hua. army.mil** or mail (with a soft copy on disk) to Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-FDR-CB, Bldg 61730, Room 105, Fort Huachuca, AZ 85613-6000. (Please do not use special document templates and please attach the graphics separately.) We can accept articles in Microsoft Office 2000, Word 7.0, Word Perfect 6.0a, and ASCII; we need the graphics in Adobe, Corel, or PowerPoint (in order of preference). Please include with your article:

- ❑ A cover letter with your work and home E-mail addresses, work telephone number, and a comment stating your desire to have the article published.
- ❑ A release signed by your local security officer or SSO stating that your article is unclassified, nonsensitive, and releasable in the public domain. (***MIPB*** is available for sale by the Government Printing Office.)
- ❑ Pictures, graphics, and crests/logos with adequate descriptions. Submit clear "action" photos that illustrate your article with captions for the photos (the who, what, where, when, why, and how); the photographer credits; and include the author's name on photos. Please do not embed graphics.
- ❑ The full name of each author in the byline and a short biography for each. The biography should include the author's current duty position, related assignments, relevant civilian degrees (degree, school, major), and any special qualifications. (Indicate whether we can print your telephone number and your E-mail address with the biography.)

We cannot guarantee we will publish all submitted articles but will send you a message acknowledging its receipt. We may notify you again when we get ready to publish it. Please inform us of any changes in contact information as it can take a year or more before some articles are published.

If you have any questions, please call (520) 538-0564/1005 or DSN 879-0564/1005.

Military Intelligence Professional Bulletin
2003 Issues
Upcoming Themes and Deadlines for Article Submission

Issue	Theme	Deadline
Apr-Jun	Force Protection	5 Jan 03
Jul-Sep	Information Operations	5 Apr 03
All Issues	War on Terrorism Operation ENDURING FREEDOM	

323d Military Intelligence Battalion (CE)

Oriental blue and silver grey are the colors traditionally used by the Military Intelligence Corps. Red denotes valor and zeal. The two colors of blue represent day and night vigilance and the unit's covert and overt operations. The lightning bolt highlights the unit's speed and the dominant role of combat electronic warfare on the battlefield.

The 323d Military Intelligence Battalion (CE) traces its lineage to the 19th MI Battalion, which activated in Germany in 1968. In February 1996, the 19th redesignated as the 323d MI Battalion and activated at Fort George G. Meade, Maryland, its current home station. The battalion is composed of four organic companies: Headquarters and Headquarters Company, A Company (Electronic Warfare [EW] and Measurement and Signatures Intelligence [MASINT]), B Company (Counterintelligence [CI]), and C Company (Interrogation and Exploitation). The 323d continues to deploy soldiers in support of missions in the Balkans and has deployed multiple intelligence teams in support of the NOBLE EAGLE and ENDURING FREEDOM antiterrorism campaign.

The capabilities of the 323d MI Battalion include electronic attack (EA) and electronic warfare support (ES), CI and human intelligence (HUMINT), and exploitation and interrogation. The AN/TLQ-17A (V) 4 SANDCRAB is a tactical communications, high-frequency sky-wave jammer with a 1500-watt transmitter having both EA and ES capabilities. Another system they use is the Counterintelligence/Human Intelligence Automated Tool Set (CHATS), an Army hardware/software suite designed to meet the unique requirements of HUMINT teams operating in diverse operational environments. The Interrogation/Exploitation Teams use sophisticated procedures to gain, analyze, and exploit HUMINT from enemy prisoners of war (EPWs) and other sources.

The Battalion's WARTRACE assignment involves support to the 513th MI Brigade. The 323d MI Battalion formally aligns for training and deployments with the 513th MI Brigade at Fort Gordon, Georgia, and its subordinate 201st, 202d, 204th, and 297th Military Intelligence Battalions.

COLLECT AND EXPLOIT!

Commander
U.S. Army Intelligence Center and Fort Huachuca
ATZS-FDR-CB (12)
Fort Huachuca, AZ 85613-6000

PRESORTED STANDARD
U.S. POSTAGE & FEES PAID
NIAGARA FALLS, N.Y. 14304
PERMIT NO. 28

Headquarters, Department of the Army.
This publication is approved for public release.
Distribution unlimited.

PIN: 080530-000