MIPB

MILITARY INTELLIGENCE PROFESSIONAL BULLETIN

APRIL-JUNE
2003
PB 34-03-2

INTELLIGENCE SUPPORT TO FORCE PROTECTION

From the Editor

This edition of the ***Military Intelligence Professional Bulletin*** focuses on Intelligence Support to Force Protection. In holding with our charter, I am writing this section to spur input from you, the reader.

September 11, 2001, altered the way most U.S. citizens view the world; however, the reality of the world we live in did not change. Global terrorism is and has been a significant world dilemma for many years. The requirement for U.S. forces to remain vigilant remains unchanged. The challenges associated with intelligence support to force protection are daunting. When intelligence personnel perform this task well, it supports the commander's use of a myriad of potential friendly actions and counteractions. Otherwise, if intelligence personnel do not perform this task adequately, the results can be catastrophic.

Antiterrorism (AT) and force protection (FP) are inextricably linked missions and operations. However tied these missions are, AT alone does not just equate to providing sufficient FP. The Army must train, staff, and support these programs and missions throughout the whole force. There is no easy "cookie-cutter" approach to FP.

There is a lot of misunderstanding associated with FP. It is not solely—

□ Counterintelligence teams performing CI operations.
□ Human intelligence teams conducting HUMINT operations.
□ Soldiers pulling a security detail at a forward-deployed basecamp.
□ The staff producing a threat and vulnerability assessment (TVA).

The CI and HUMINT teams and security detail may contribute to FP, but alone they do not equal force protection, and the TVA is just a tool. FP consists of all of the actions taken to prevent or mitigate hostile actions against personnel, resources, facilities, and critical information. Adequate FP requires the—

□ Synchronized and integrated planning, preparation, execution, and assessment of intelligence, surveillance, and reconnaissance (ISR) operations and focused intelligence production in support of the commander's requirements. Accomplishing this goal will facilitate the commander's visualization and situational understanding.
□ Entire staff participates as critical contributors throughout the planning process and orders production to include during the intelligence preparation of the battlespace.
□ Coordination and deconfliction with the different staffs (especially involving intelligence) from the lowest to highest echelons within the theater or operation. Often this requirement will extend to multinational and interagency partners.
□ Unit or task force to develop appropriate security taskings and plans to counter the threat outlined in the TVA and those threats predicted in other intelligence products.
□ Strict adherence to and implementation of all security policies outlined by our Army regulations. The physical security, operations security, subversion and espionage directed against the Army (SAEDA), and other regulations and policies directly contribute to the overall FP of a deployed unit or task force.

Finally, FP requires realistic training that incorporates all FP policies and programs along with the supporting programs and measures. This training ensures that soldiers actually perform to standard. The Army must conduct FP 24 hours a day, 365 days a year, whether deployed overseas or at your home station. As intelligence professionals, we must be ready to answer the call and provide the best intelligence possible to answer the commander's requirements.

Please send your comments on any aspect of this topic to mipb@hua.army.mil.

Stephen B Leeder

Stephen B. Leeder

MILITARY INTELLIGENCE

PB 34-03-2
Volume 29 Number 2
April-June 2003

Check us out on the Internet
http://mipb.futures.hua.army.mil

STAFF:

Commanding General
Brigadier General John M. Custer

Deputy Commandant for Futures
Jerry V. Proctor

Director of Training Development and Support
Colonel Jack W. Russell

Deputy Director, DTDS
Russell W. Watson, Ph.D.

Chief, Doctrine Division
Stephen B. Leeder

Acting Managing Editor
JoNell M. Elkins

Editor
Elizabeth A. McGovern

Operations Supervisor
Second Lieutenant F. Mia Clements

Design Director
Specialist Ernesto A. Bolaños

Associate Design Director and Administration
Specialist Misty L. Simpkin

Word Processing Support
William J. Gleason
Ruth Valenzuela

Cover Design:
Specialist Misty L. Simpkin

Purpose: The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) publishes the ***Military Intelligence Professional Bulletin*** quarterly under provisions of **AR 25-30**. ***MIPB*** disseminates material designed to enhance individuals' knowledge of past, current, and emerging concepts, doctrine, material, training, and professional developments in the MI Corps.

Subscription: Subscription rates are $21.00 (Domestic, APO, and FPO) and $29.40 (Foreign). For information on changes of address and subscriptions, see page 4.

Disclaimer: This publication presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other U.S. Army publications. We reserve the right to edit any submitted material.

Contact Information for ***MIPB*** is on page 72.

FEATURES

DEPARTMENTS

By order of the Secretary of the Army:
Official:

JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army
0302322

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

Intelligence Support to Force Protection

As intelligence professionals, we must become proficient in supporting force protection (FP) during daily operations. On or off duty, protecting our military forces near and far is a critical mission we cannot and will not neglect. Here are a few fundamental keys that will lead us to success in providing the intelligence necessary to safeguard the force.

The first key is to increase your knowledge and personal awareness about FP. Train on antiterrorism (even if it is just online), follow the latest news and other open sources of information, pay attention to your surroundings, and stay vigilant.

As U.S. citizens, we changed our minds about the importance of security when terrorist attacks dramatically altered our perceptions about the world on September 11. We became vividly aware of evil possibilities—the unthinkable was no longer impossible within our borders. What is disturbing is that terrorists may live among us in our own towns. We must be vigilant, without succumbing to fear or paranoia, so that we can witness any subtle indicators of terrorist activity. Quickly report such information to appropriate authorities, since the minor clue you provide may lead to uncovering a terrorist operation.

The second key is to make sure that you make a significant contribution to improving intelligence operations within your unit or organization. Recently, our problems with processing timely intelligence resulted in serious consequences during the Khobar Towers attack in Saudi Arabia and the bombing of the U.S.S. Cole off Yemen. Terrorists will attack the U.S. forces again. However, if we improve our intelligence procedures, take quick action to report possible terrorist activities, and then use the intelligence while it is still timely and accurate, we can avoid or mitigate our losses.

We should continually strive to improve intelligence procedures. Military Intelligence professionals worldwide are working around the clock to build the new infrastructure that now includes the U.S. Northern Command. NORTHCOM is responsible for the land, aerospace, and sea defenses of the United States.

Understandably, all echelons face great challenges in supporting Homeland Security and our own FP. These challenges include a finite budget, and limited personnel and resources. We must utilize our vast technology and communication tools to enable the free flow of information. However, we must also continue to work hard, improve our fundamental skills, and build on our growing institutional knowledge.

The final key is to make sure intelligence is an integrated and integral part of staff operations and effectively supports the commander. It is not enough to simply manage and produce intelligence. The intelligence products and staff operations must incorporate the work and experience of all the staff and be tailored to provide sufficient support to everyone as well. The intelligence officer must know his commander intimately so he can tailor the intelligence reports and products to best facilitate the commander's understanding and visualization of the battlefield. Every commander visualizes differently; therefore, an intelligence officer must change, update, or modify the products based on the commander's needs. Additionally, the intelligence officer must train his subordinates to produce reports and products that answer all staff requirements and facilitate the commander's visualization.

As our military forces continue to deploy and expand their missions worldwide, it is crucial that we maintain time-tested fundamentals while blending in new systems, organizations, and procedures. We must assess the actual risks so we can develop adequate plans and deploy with adequate countermeasures, even with our limited resources. You play a critical part in protecting the force.

ALWAYS OUT FRONT!

CSM Forum

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

I would first like to say *"congratulations"* to the newly selected Sergeants Major (SGMs), Command Sergeants Major (Designee), and those Master Sergeants selected for attendance at the U.S. Army Sergeant Major Academy (USASMA). Our Military Intelligence (MI) Corps did very well on this past year's Sergeants Major Board. Our Corps has been very successful at the board two consecutive years. Again, congratulations to those newly selected SGMs: "*The sergeants major are the leaders of our NCO Corps! We wear the Star, we wear the Star and Wreath, and we are one, we are the NCO Corps."* As I have said before, *"take care of our soldiers for they are our sons and daughters, on the point of the bayonet, an investment in our Army and defense of this great nation of ours."* I thank you, the sergeants major, for being the leaders of our Noncommissioned Officer (NCO) Corps and for taking care of our soldiers, our MI Corps, and our Army.

This past January, I attended the third annual Sergeant Major of the Army's (SMA) nominative SGMs conference held at Fort Bliss, Texas. One of the conference goals was to help the Army, U.S. Army Reserve (USAR), and the U.S. Army National Guard (ARNG) ("The Army") to gain the benefit of the knowledge and experience of our 225 SGMs as the Army seeks to move 15 issues toward resolution. A few of the issues addressed during the breakout panels were—

- □ Duty MOS qualification.
- □ Timely notification of USAR and ARNG forces for routine missions.
- □ NCOES (NCO Education System) infrastructure.
- □ U.S. Army Forces Command (FORSCOM) NCOES university concept.
- □ Army weight control pilot study.
- □ Travel charge card program.
- □ Safety awareness improvements, including reducing privately owned vehicle (POV) accidents.

Several individuals from the Army leadership spoke to us. They were the Chief of Staff of the Army (CSA), Secretary of the Army, Commanding General (CG) of the National Guard, CG of the Army Reserve, Army G1, Army G3, and the SMA; all the speakers had two common themes: the Global War on Terrorism and safety awareness.

The war against terrorism in Afghanistan has taken the lives of 100 and injured 87 great Americans in Afghanistan. The SMA stressed that it is about fundamentals in our Army, "*have your war face on!*" If not, you are wrong! Our great soldiers continue to tell our senior leadership that the key to success in Afghanistan is to be able to perform the basic tasks to standard. The four keys to our soldier's success are—

- □ Physical and mental toughness developed through combat focus.
- □ Marksmanship—shoot well in hot and cold weather.
- □ Combat life-saver skills.
- □ Small-unit drills performed in all environments.

This is clearly NCO business! Training to standard should be our focus and mission. Our soldiers know when they are receiving training to standard, they know when the leadership is there taking care of them, and our soldiers will follow leaders anywhere. We as soldiers have a special trust and honor which bonds us even closer in a unique brotherhood of war. I ask you all to share our special comaraderie and the emotional relationship we have with others. We have the finest young men and women in the world in our Army and all of our Services today; it is an honor to lead, coach, teach, and mentor them. The basic skills and survivability of our soldiers are about attitude and motivation, which are NCO business. I thank the Sergeants.

With reference to safety and POV accidents, this is a leadership challenge and demands our attention and

(Continued on page 4)

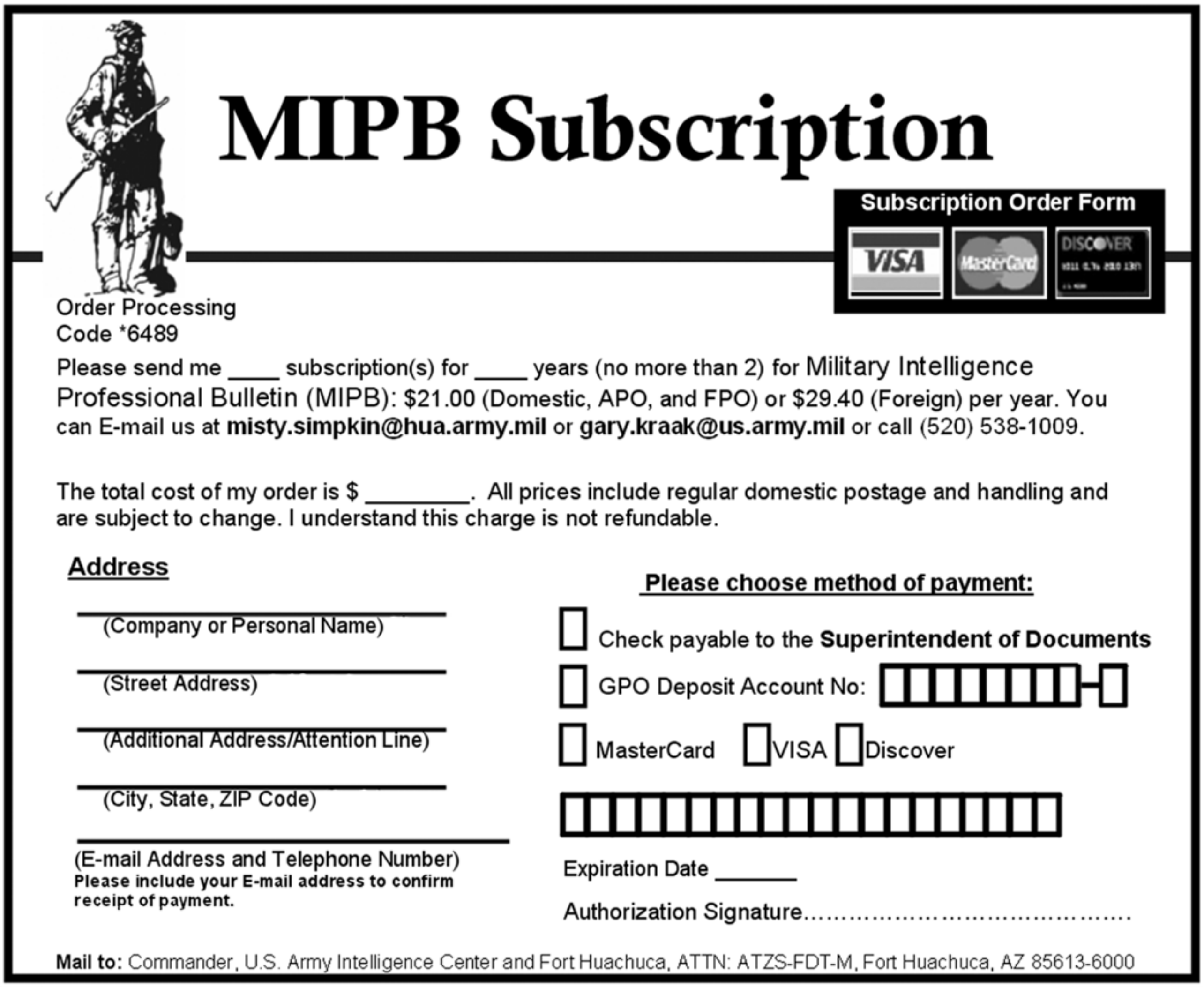
(Continued from page 3)

that of all of the command leadership teams. This past year we lost 206 of our soldiers in safety-related accidents—113 were POV accidents, and the majority of those soldiers were not wearing their seat belts. Any death is a great loss, especially when there is a chance leaders could have prevented a fatality through their vehicle safety programs. The biggest contributors to death and vehicle injuries are not driving under the influence, but speed, fatigue, and soldiers not wearing their seatbelts. We have excellent young soldiers; however, what kills our great soldiers is their trying to get from one place to another too quickly or soldiers not performing a crucial task when preparing for a trip. They do not do what the military does before all training missions—a risk assessment. I recommend that we as leaders incorporate the risk assessments into our safety briefings so they become ingrained. As leaders, we must focus on safety and endeavor to reduce POV accidents for all of our soldiers.

Although leaders have the major responsibility to educate our soldiers on safety and to prevent accidents, I must stress that we soldiers still have to take care of each other. Safety starts at the top with the leadership, but it is everybody's responsibility. We have to look out for the welfare of the United States. We are in a war right now, and our soldiers are an investment in the defense of our great nation. To lose a soldier in a tragic accident is too much. Finally, remember you are only as safe as the other U.S. soldier out there. Maintain situational awareness of your surroundings wherever you are. *"Safety does not happen by luck: safety happens because everyone is involved!"*

I 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!



MIPB Subscription

Subscription Order Form

VISA
MasterCard
DISCOVER

Order Processing
Code *6489

Please send me ____ subscription(s) for ____ years (no more than 2) for Military Intelligence Professional Bulletin (MIPB): $21.00 (Domestic, APO, and FPO) or $29.40 (Foreign) per year. You can E-mail us at **misty.simpkin@hua.army.mil** or **gary.kraak@us.army.mil** or call (520) 538-1009.

The total cost of my order is $ ________. All prices include regular domestic postage and handling and are subject to change. I understand this charge is not refundable.

Address

____
(Company or Personal Name)

____
(Street Address)

____
(Additional Address/Attention Line)

____
(City, State, ZIP Code)

____
(E-mail Address and Telephone Number)
Please include your E-mail address to confirm receipt of payment.

Please choose method of payment:

□ Check payable to the **Superintendent of Documents**

□ GPO Deposit Account No: □□□□□□□□-□

□ MasterCard □VISA □Discover

□□□□□□□□□□□□□□□□□□□□

Expiration Date _______

Authorization Signature...

Mail to: Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-FDT-M, Fort Huachuca, AZ 85613-6000

ISR Support to Force Protection[1]

by Jerry W. Jones

The highest priority of the United States is Homeland Security. The military mission sets are Homeland Defense (HLD), civil support, and emergency preparedness. The military components play a vital role in HLD of the security of the U.S. homeland. Military forces will execute their assigned missions in circumstances of emergency, routine, or extraordinary nature.

This article discusses organizational and operational (O&O) concepts for intelligence, surveillance, and reconnaissance (ISR) support to installation force protection (FP) initiatives as a subset to HLD. It draws heavily on the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) submission to Headquarters, U.S. Army Training and Doctrine Command's (TRADOC), Force Protection O&O Plan, which focused on FP operations for a region, major Army command (MACOM), and Army installation operations center (IOC).[2, 3] It encompasses all ISR activities with emphasis on intelligence "reach" and analysis. The principles that guide ISR in other operations along the spectrum of conflict are applicable to activities that protect the force in a garrison environment.

ISR is a critical component of information superiority. Defeating imaginative, nontraditional adversaries requires ISR operations to maintain the capability to gain information superiority and to respond quickly and effectively to new threat capabilities, new tactics, unpredictable patterns of operations, and changing battlefield conditions. It requires the fusion of data, information, and intelligence from multiple organizations, which enables the installation and region to identify proactively and counter threat organizations before they strike. It embraces the "quality of firsts" emphasized in our Objective Force concepts.

Operational Concept

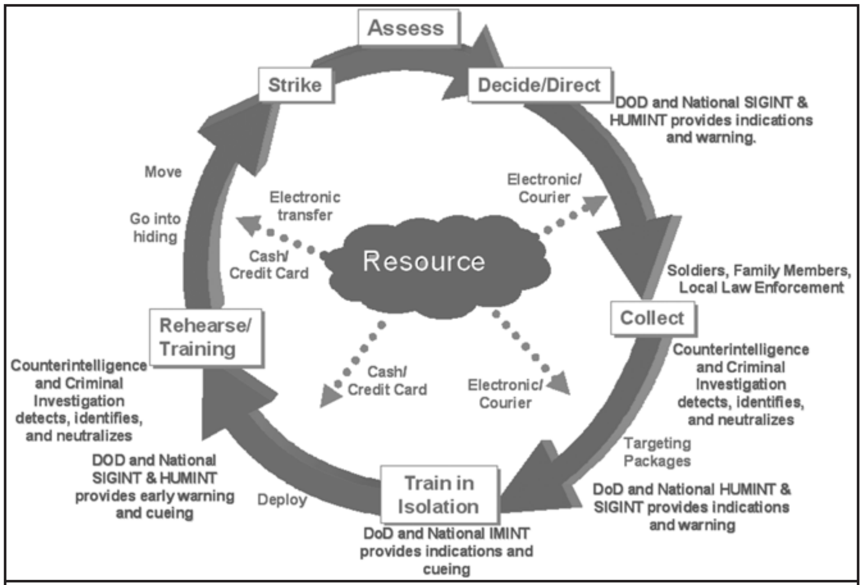
The mission of the ISR system is to provide timely, relevant, and accurate early warning and predictive intelligence products to enable proactive FP condition (FPCON) (formerly known as threat condition [THREATCON]) decisions by the regional directors and garrison commanders that result in actions by installation entities.

ISR is the complex endeavor to combine and integrate the capabilities and tasks of the Intelligence battlefield operating system (BOS)—which includes the plan and direct, process, analyze and produce, and disseminate portions of the intelligence cycle—with the command and control (C2) and information collection capabilities, tasks, and operations of reconnaissance and surveillance (R&S) capable units and organizations throughout the entire operations process (plan, prepare, execute, and assess). Crucial to providing this support is developing a common understanding or operating picture of the threat and the environment through the coordinated actions of all the organic and supporting analytic and ISR collection assets. ISR is the sum of the battlefield function of intelligence with two full-spectrum missions, reconnaissance and surveillance, required to support intelligence. Individually and collectively, this ISR force supplies the installation and region with the capability to plan and direct ISR operations, collect and process information, produce predictive intelligence assessments, and disseminate combat information and intelligence to those who need it, where they need it, and when they need it. In homeland operations, R&S-capable units include the U.S. Army Criminal Investigation Division Command, U.S. Army Intelligence and Security Command (INSCOM), and various installation entities (military police, medical, public affairs, etc.). ISR is fundamental to gaining and maintaining information superiority—the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority is the critical component to ensuring the commander can act inside the decision cycle of the adversary (see Figure 1). Commanders must "see first, understand first, act first, and finish decisively" to mitigate threat activities directed at our installations.

The ISR system consists of organizations, sensors, and analysts that enable the commander to understand the threat and environment. The challenge is to contend with a complex and dynamic threat environment. The threat operational paradigm includes certain attributes:

- ❑ Deliberate planning with good intelligence about the installation including target importance and vulnerability.
- ❑ Conduct of live, virtual, and remote reconnaissance of the installation.
- ❑ Trained and rehearsed team in isolated areas.
- ❑ Exploitation of our freedoms by the threat.
- ❑ Operational security (OPSEC) is a way of life, not a function.

ISR operations in this environment require a flexible, integrated military and civilian ISR capability. This threat demands a wide range of capabilities across law enforcement, governmental entities, and intelligence elements with greater reliance on their ability to synchronize efforts and conduct continuous operational assessments to understand the environment and situation. As a result, each region and Army installation requires a capability to integrate collection across multiple agencies (or-



Assess
Strike
Decide/Direct
DOD and National SIGINT & HUMINT provides indications and warning.
Move
Go into hiding
Electronic transfer
Electronic/ Courier
Cash/ Credit Card
Resource
Soldiers, Family Members, Local Law Enforcement
Collect
Rehearse/ Training
Counterintelligence and Criminal Investigation detects, identifies, and neutralizes
Cash/ Credit Card
Electronic/ Courier
Counterintelligence and Criminal Investigation detects, identifies, and neutralizes
Targeting Packages
DOD and National SIGINT & HUMINT provides early warning and cueing
Deploy
Train in Isolation
DoD and National HUMINT & SIGINT provides indications and warning
DoD and National IMINT provides indications and cueing

Key: DOD — Department of Defense
HUMINT — Human intelligence
SIGINT — Signal intelligence
IMINT — Imagery intelligence

Figure 1. Threat Attack Cycle Versus Blue Collection Cycle.

ganic and non-organic; technical and nontechnical), and an analytical capability that facilitates situational understanding to each installation commander. This analytical capability will merge criminal intelligence efforts of criminal investigation detachments (CIDs) with traditional all-source intelligence analysts of the Military Intelligence (MI) Corps. Together with theater, departmental and national entities, they create a synergy to deliver indications and warning (I&W) that will lead to neutralization of threat activities before an attack.

The ISR capability must be proactive in interacting with non-organic resources to obtain information required by the regional director and installation commander. It is the process of identifying and tracking the threat before it arrives at the installation. The military ISR organizations exist in a complex and intertwined operational environment consisting of city, county, state, and federal entities (governmental, law enforcement, intelligence, and infrastructure). The identification of threat entities outside the installation's area of influence (AI) provides the most protection and allows for close coordination with non-organic entities. ISR elements must engage the plethora of entities in this environment and establish interdependent relationships to assure timely transmission of relevant information to a centralized, focused intelligence center that will respond to the regional director and installation commander. Through engagement and collaboration, the installation and regional fusion cells will maintain an accurate understanding of the threat enabling commanders to execute proactive FP activities.

The ISR capability will support current installation activities and, as appropriate, the projection of forces to a contingency mission. Each installation with a force that may deploy to a contingency must be able to coordinate FP during deployment and at the embarkation point. The ISR capability must respond to requirements at the installation and at the port. In some cases, the installation will deploy appropriate ISR assets to the port to enhance FP support.

ISR analysts will work with the commander and others to develop a list of priority intelligence requirements (PIRs) that will drive the collection and analysis effort. They tie PIRs to decision points. As data and information are collected and analyzed, the analyst collaborates with counterparts horizontally and vertically to identify indicators that satisfy the PIRs. As a series of indicators answer a PIR, the analyst will advise the commander. As they present the analyzed information, the commander will determine the level and adopt additional protective security measures.

Required Capabilities

An ISR fusion cell at a region or installation will furnish timely, relevant, and accurate early warning and predictive intelligence products to answer the regional directors' and installation commanders' critical FP information requirements (IRs). The regional and installation ISR system will supply I&W of threat activity and enable each commander to institute FP measures proactively. A critical facet of providing this support is developing an understanding of the threat and environment through the synchronized actions of all organic and supporting collection assets and the integration of the information in a dedicated analytic cell.

General Capabilities. The general requirement is for centralized planning and decentralized execution of collection activities characterized by focused tasking of available assets and requests to multiple agencies to ensure rapid satisfaction of requirements in the battlespace. The required capabilities are—

- ❑ Situational awareness regarding threat actions to enable each installation commander to make correct FP-related decisions.
- ❑ Capabilities to see and understand the situation nationally, regionally, and at other installations in order to assess impacts locally and contribute assistance as required.
- ❑ "Smart push" and "smart pull" technologies with automatic processing of requests for information (RFIs) to answer each installation commander's IRs.

- ❑ Organic and remotely accessible databases to give FP personnel the ability to screen potential threat individuals rapidly.
- ❑ Actionable intelligence to enable information operations (IO) implemented by installation commanders under applicable policies and directives.
- ❑ Proactive intelligence assessments to support an installation's quick reaction force (QRF) with real-time, on the move, threat-oriented, and protection-oriented intelligence.
- ❑ Specialized technical intelligence (e.g., medical, chemical, radiological, biological to facilitate I&W) collected, analyzed, and disseminated to the commander. For instance, the installation director of health services gathers and analyzes information from local area hospitals to enhance situational awareness and understanding.

To mitigate threat activities, ISR support to installation and MACOM operations includes planning, directing, and executing activities. It also comprises analyzing and presenting intelligence to support FP and the commander's decisions as well as providing technical and nontechnical support to IO.

Plan and Direct. ISR support to FP operations requires a dedicated, trained, ISR planning and integration capability. It is conceivable that the region and installation will perform a variety of simultaneous tasks. The ISR system must rapidly identify the commander's IRs and adjust collection and analytical activities to fill information gaps. The region and installation will receive information and intelligence from a variety of organizations from local entities to national intelligence agencies. Installations will forward reporting from local (city, county, state, and federal) agencies, while the region will pull information and intelligence from national agencies. Once received, the ISR element analyzes and submits the information to the installation commander continuously to ensure he bases his decisions on timely and accurate situational awareness. Specifically the ISR element—

- ❑ Ensures the installation and tenant commanders have situational understanding on a regional and national basis.
- ❑ Conducts support to FP operations while continuing support to installation FP activities.
- ❑ Tailors and maintains an integrated communications and processing architecture that enables collaboration with local agencies, other installations, the region, MACOMs, and national entities.
- ❑ Furnishes timely I&W to support FP across the installation's area of interest (AOI).
- ❑ Maintains threat situational awareness within the AOI of the installation to support the commander's decisions.
- ❑ Manages PIRs and RFIs to satisfy the commander's knowledge requirements.
- ❑ Coordinates local training to ensure full threat awareness at the local level and collaborates with other installations to ensure a common operational picture (COP).

Collect. Many organizations will rely on collection capabilities at the installation level as well as information disseminated by national agencies. The challenge lies in the management of requirements so that collection resources positioned at each installation can also respond to those that need local information. The primary collectors are the local resident agents of the U.S. Army Criminal Investigation Division Command (USACIDC) and INSCOM. Analysts must be able to access relevant information from the USACIDC, INSCOM, and external sources (local law-enforcement agencies [LEAs]). The challenge lies in the coherent and coordinated management and integration of resources positioned throughout the installation and surrounding areas. The design of the ISR capability must integrate collection results to provide situational context, intent of the adversary, and actionable intelligence focus on decisionmaking and influencing operations. Effective collection management should—

- ❑ Leverage time-sensitive information and reporting from national, region, and local (city, country, state, and federal) government and LEAs.
- ❑ Contribute awareness and sensitize installation personnel on reportable information.
- ❑ Leverage information and reporting from joint, interagency, multinational, and commercial collection resources.
- ❑ Conduct liaison with the city, county, state, and federal governmental entities.
- ❑ Guide and coordinate activities by various installation entities as they interact with local civilian government and LEAs, military resources at the installation, and local federal representatives.

Process. The ISR fusion cell in the operations center will be the focal point for collection, ISR, and information processing and dissemination. It will exploit reporting from each installation while leveraging information and intelligence available from national, MACOM, and regional entities. The ISR fusion cell will—

- ❑ Receive processed real-time intelligence products from national and theater intelligence centers.
- ❑ Receive the processed, single-discipline reported information for fusion and analysis to satisfy the installation commander's requirements.
- ❑ Access, focus, and tailor the technical and analytic products from the national and theater analytic centers to meet the installation's needs.
- ❑ Receive and process broadcast downlinks.

❑ Maintain multilevel security databases that safeguard sources and permit authorized access to unprocessed data.

❑ Furnish the capability to develop, transmit, and store the graphic products with supporting data.

❑ Access existing databases, products, and analytic expertise resident in Service, joint, and national reconnaissance and surveillance resources. This reach capability will facilitate collaboration, task-sharing, access to higher echelon databases (virtual databases in the future), as well as intelligence preparation of the battlefield (IPB) products and focused analysis.

❑ Access data from each installation's operations center.

❑ Access data from local LEAs.

Analyze. Analysis will occur in the operations center performed by the dedicated ISR fusion cell that includes counterintelligence (CI) and criminal investigation expertise. Within the distributed and collaborative framework, each installation will analyze information relevant to its AOI. Automation allows intelligence analysts to share their assessment of the situation with other installations, the region, and the appropriate MACOMs. This process shares the results of analysis, not just data. Subordinate and tenant units, higher headquarters, and external organizations all share a common understanding of the threat. This process demands collaboration. As the fusion cell at the region compares, merges, and evaluates each installation's representation of the situation, the cell members continuously discuss discrepancies to preclude both duplicate reporting and re-analyzing information. The region has the organic processing and communications systems to collaborate with external analytic elements in order to update and refine situational awareness continuously. The regional fusion cell will—

❑ Exchange situational awareness and discuss issues with experts using collaborative tools.

❑ Conduct analysis of local information to determine threat patterns of operation in the neighboring area and deliver information and analysis to the region, other installations, and the appropriate MACOMs.

❑ Perform all-source analysis to develop an understanding in each installation's area of operations and AOI through the analysis and fusion of information with multidiscipline intelligence using collaborative analytic, development, and visualization tools.

❑ Fuse vertical and horizontal information from organic and non-organic entities, the region, appropriate MACOMs, and joint, multinational, and interagency organizations.

❑ Perform trend and predictive analysis to facilitate situational understanding (evaluate, integrate, analyze, and interpret).

❑ Detect, identify, and report all threat IO activities with emphasis on threat use of deception and psychological operations (PSYOPs).

❑ Offer a near-real-time (NRT) assessment of the capabilities and vulnerabilities of the adversary.

Disseminate and Present. Underpinning all ISR operations to achieve situational understanding is the development and maintenance of a robust intelligence and communications architecture that links the region with each installation and ISR organization including links into the I&W network. The region establishes the intelligence operational architecture that seamlessly links the region internally and externally. This architecture must be a highly mobile, self-organizing, self-healing, routed, wireless, multiple security-level environment that facilitates the exchange of information between installation commanders at the lowest level and intelligence activities at joint and national levels. At the installation level, the architecture facilitates the exchange of information between installation commanders and local government entities including LEAs. The region's ISR architecture and support relationships must be sufficiently resilient to expand and contract as the situation dictates; they must also remain responsive to the rapid flow of information and intelligence at all FPCON levels. Additionally, the network must supply multimedia capabilities (data, voice, and video); interface with FP units as they deploy from installation to port (or port to installation); and ensure compatibility with city, county, state, and federal agencies to enable collaborative analysis of information. The network should—

❑ Possess secure, redundant, and broad-bandwidth communications with a multiple security-level capability that enables the exchange of analytic findings.

❑ Disseminate and collaborate between elements internal and external to the region in real time over an expanded AOI.

❑ Receive broadcast intelligence that furnishes I&W, and location information of threat entities.

❑ Dynamically update the situation from organic and non-organic collectors and processors.

❑ Present the current threat situation and threat intent to facilitate situational understanding.

❑ Provide an NRT visualization of each installation commander's area of responsibility (AOR) and AOI.

The concept for ISR support centers on a flexible and tailorable force of personnel, organizations, and systems designed to execute ISR operations. Individually and collectively, this ISR force gives the installation and region the capability to plan and direct operations, collect and process information, produce relevant intelligence, and disseminate information and intelligence to the subordinate elements. Although the installation has some organic capability, it does not possess all the ISR collection, processing, integration, and analytic assets that enable the above actions. It still must rely on receiving real-time processed intelligence data from local, state, and federal LEAs; regional and national intelligence agencies; and other installations.

Based on the FPCON, each installation commander establishes information and intelligence requirements to enable decisionmaking. The regional operations center integrates available assets and collaborates with external entities to satisfy the commander's requirements. The region's intelligence and information processing, planning, and analytic capability resides in the operations center, while the collection capability is resident within multiple military, national, and civilian organizations.

Depending on the current FPCON, the installation commander establishes information and intelligence requirements to enable decisionmaking. The ISR fusion cell integrates available resources and collaborates with external entities to satisfy the commander's requirements. The installation's intelligence and information processing, planning, and analytic capability resides in the installation operations center (IOC), while the installation's collection capability is resident within the installation's population.

At *Minor* and *Other* installations, the ISR capabilities to integrate, plan and direct, collect, and analyze are limited. The installation commander's AOR is the military installation, but he must have situational understanding beyond the local military community just as *Major* installations do. The analyst will depend on reach and collaboration with *Major* installations and the region to obtain tailored analytical products that meet the installation commander's requirements. The IOC's liaison with local LEAs is critical for the installation to maintain situational awareness. If the commander has CIDC or INSCOM support on the installation, those representatives will be an essential element to liaison with local LEAs.

Force Design Parameters

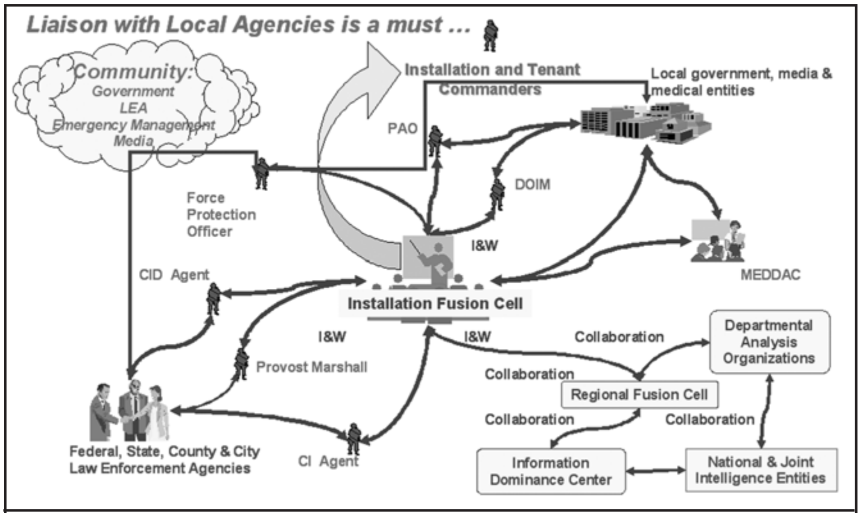
Each installation and region requires a dedicated ISR fusion cell. This cell will ensure the satisfaction of installation commanders' and tenant organization commanders' critical information requirements (CCIRs). Among other things, each fusion cell will perform the following tasks to accomplish the stated purpose:

- ❑ Furnish timely I&W and predictive and tailored products to support FP and enable a continuous operational assessment.
- ❑ Maintain an integrated picture throughout the AOI to support the commander's decisions, operational actions, FP measures and further analysis.
- ❑ Establish PIRs and RFIs to satisfy operational requirements, tailored to installation needs.
- ❑ Prepare and execute an ISR collection plan to focus available resources on information requirements.
- ❑ Conduct all-source analysis to support timely predictive assessments that lead to correct decisions.
- ❑ Supply timely information to department, joint, and agency levels to ensure a common operational picture (COP) and appropriate distribution of resources.
- ❑ Maintain connectivity with joint, national, combined, and Service intelligence and LEAs to ensure common situational understanding that leads to information superiority.
- ❑ Disseminate intelligence to subordinate installations and organizations to support current and future operations and plans.
- ❑ Fuse criminal information to present a seamless threat picture to enhance FPCON decisions.
- ❑ Conduct analysis of local information to determine threat patterns of operation in the local area and deliver information and analysis to the region, MACOM, and other installations.
- ❑ Collaborate with other installations, the region, and the appropriate MACOMs to ensure coverage of the AI and AOI and enable operational awareness and situational understanding of the threat at the installation level.
- ❑ Establish a robust and routine relationship with the local liaison to gather information and to ensure connectivity with important sources of information to satisfy the commander's requirements.

If the ISR fusion cell is successful in executing missions as described above, critical decisionmakers will mitigate the ability of the threat to—

- ❑ Determine vulnerable targets, which will deter attacks against installations.
- ❑ Collect the information required to make decisions with regard to targeting.
- ❑ Train teams to plan and execute an attack.
- ❑ Infiltrate a team to conduct rehearsals and final training.
- ❑ "Blend into the community" while waiting for final instructions to execute an attack.
- ❑ Gain access to an installation to conduct an attack.

At the installation level, there are numerous sources of information imperative to maintaining situational awareness and understanding in the AOR and AI (see Figure 2). These entities include the local LEAs (city, county, state, and federal), governmental organizations (e.g., city manager, public works, emergency management activity, board of supervisors, and health and social services), emergency organizations (e.g., fire department), medical facilities (e.g., clinics and hospitals),


Liaison with Local Agencies is a must …
Community:
Government
LEA
Emergency Management
Media
Installation and Tenant Commanders
Local government, media & medical entities
PAO
DOIM
Force Protection Officer
I&W
MEDDAC
CID Agent
Installation Fusion Cell
I&W
I&W
Collaboration
Departmental Analysis Organizations
Provost Marshall
Collaboration
Regional Fusion Cell
Collaboration
Collaboration
Federal, State, County & City Law Enforcement Agencies
CI Agent
Information Dominance Center
National & Joint Intelligence Entities

Key: DOIM — Directorate of Installation Management
I&W — Indications and warnings
LEA — Law-enforcement agency
MEDDAC — U.S. Army Medical Department Activity
PAO — Public affairs office

Figure 2. Installation Information Linkages.

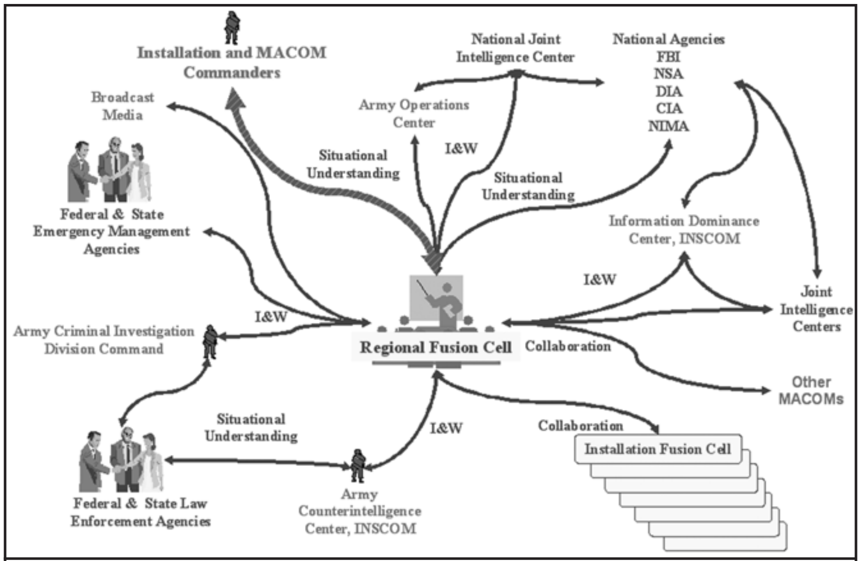
private organizations (e.g., media, American Red Cross) and civic entities (e.g., chambers of commerce). Additionally, the installation's ISR fusion cell must collaborate with external organizations to maintain situational awareness in the AOI. These organizations include national intelligence organization's websites (e.g., the Central Intelligence Agency's Counterterrorism Center), Army Departmental level intelligence entities (e.g., Army Counterintelligence Center, USACIDC Analysis Center, INSCOM's Information Dominance Center), the MACOM's ISR cell, and other installations.

The Mission/Task/Purpose analysis concluded that at *Major* installations (see Figure 3) the minimum number of intelligence individuals required are eleven at FPCON "Bravo." These individuals should be civilian personnel in order to maintain continuity with local agencies and understanding of the threat environment.

The ISR fusion cell will provide the installation commander with a capability to maintain situational awareness and to enable situational understanding in the AOR and AI. It will maintain situational awareness in the AOI. The supervisor should be a GG-0132-13 and the analysts GG-0132-11 and -12. At FPCON "Charlie" or "Delta," the ISR cell measures augmentation with individuals from a mobilization table of distribution and allowances (TDA). To be effective, this should be a drilling individual mobilization augmentee (DIMA) TDA consisting of one 0-4 35D (All-Source Intelligence Officer), one Chief Warrant Officer (CWO) 350B (All-Source Intelligence Technician), one E-7 96B (Intelligence Analyst) and one E-7 97B (Counterintelligence Agent). Additionally, a *Major* installation requires five USACIDC analysts to supply the needed criminal intelligence analysis and law-enforcement planning capability to the IOC.

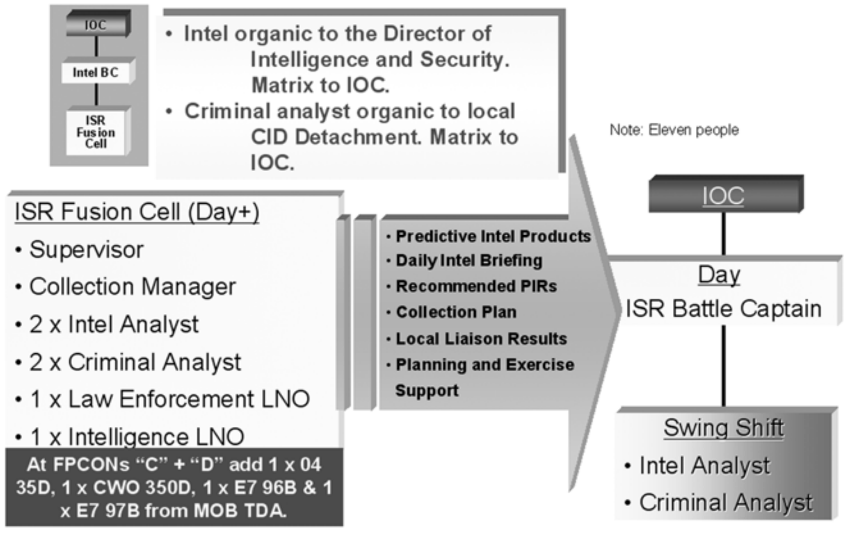
Generally, *Minor* and *Other* installations (see Figure 4) require a small, dedicated capability to give the installation commander with situational awareness.[4] This would be two advisor/analysts. (Some *Minor* and *Other* installations will have a dedicated 902d MI Group CI covering agent. Otherwise, coverage will be from the *Major* installation.) At FPCONs "Charlie" and "Delta", *Minor* and *Other* installations would require three analyst/advisors.

The designation of the current Director of Security at each installation should change to Director of Intelligence and Security, coded as a GG-0132. Depending on the size and mission of the installation, the grade should be either 13, 14, or 15. The ISR fusion cell discussed above is subordinate to the Director of Intelligence and Security, but their place of duty is in the IOC. The five USACIDC analysts are assigned to the local CID detachment with duty in the IOC.


Installation and MACOM Commanders
National Joint Intelligence Center
National Agencies
FBI
NSA
DIA
CIA
NIMA
Broadcast Media
Army Operations Center
Situational Understanding
I&W
Situational Understanding
Federal & State Emergency Management Agencies
Information Dominance Center, INSCOM
I&W
I&W
Joint Intelligence Centers
Army Criminal Investigation Division Command
Regional Fusion Cell
Collaboration
Other MACOMs
Situational Understanding
I&W
Collaboration
Installation Fusion Cell
Federal & State Law Enforcement Agencies
Army Counterintelligence Center, INSCOM

Key:
CIA — Central Intelligence Agency
DIA — Defense Intelligence Agency
FBI — Federal Bureau of Investigation
NIMA — National Imagery and Mapping Agency
NSA — National Security Agency

Figure 3. *Major* Installation Fusion Cell.


IOC
Intel BC
ISR Fusion Cell
• Intel organic to the Director of Intelligence and Security. Matrix to IOC.
• Criminal analyst organic to local CID Detachment. Matrix to IOC.
Note: Eleven people
ISR Fusion Cell (Day+)
• Supervisor
• Collection Manager
• 2 x Intel Analyst
• 2 x Criminal Analyst
• 1 x Law Enforcement LNO
• 1 x Intelligence LNO
At FPCONs "C" + "D" add 1 x 04 35D, 1 x CWO 350D, 1 x E7 96B & 1 x E7 97B from MOB TDA.
• Predictive Intel Products
• Daily Intel Briefing
• Recommended PIRs
• Collection Plan
• Local Liaison Results
• Planning and Exercise Support
IOC
Day
ISR Battle Captain
Swing Shift
• Intel Analyst
• Criminal Analyst

Key:

BC — Battle captain	LNO — Liaison officer
CWO — Chief warrant officer	MOB — Mobilization
Intel — Intelligence	TDA — Table of distribution and allowances
IOC — Installation operations center	

Figure 4. *Minor* and *Other* Installation Fusion Cells.

At the regional level, gaps and seams will exist between installation AORs and AIs (see Figure 5). The region must have a dedicated ISR fusion cell to maintain situational awareness within these gaps and seams while supporting the efforts of installation fusion cells.

To maintain situational understanding, the region is dependent upon the installation ISR fusion cell for local information and analysis. Additionally, the region will maintain information linkages (see Figure 6) with LEAs (e.g., Federal Bureau of Investigation (FBI), state police), federal and state emergency management agencies, national intelligence agencies, the five geographic Unified Command Joint Intelligence Centers, and the appropriate MACOMs.

The structure of the ISR fusion cell at the regional level must account for providing intelligence to all installations in the region and to the appropriate MACOMs. Each region's ISR fusion cell (see Figure 7) must be capable of conducting continuous operations. The ISR fusion cell at the regional level should be subordinate to the Director of Intelligence and Security's office, which will furnish matrix support to the region's operations center.

The force structure required at FPCONs "Charlie" and "Delta" increases to allow the Director of Intelligence and Security to surge increased analytical resources. A mobilization TDA will document the increase in personnel. Optimally, these will be DIMA individuals.

At the theater and national levels, intelligence organizations need to increase their capability to support FP on installations. Additional INSCOM CI and CIDC special agents are necessary at the installation level. CI and Criminal Investigators will collect information pertaining to the full-spectrum, FP threat. In addition, INSCOM and CIDC need to increase their analysis capability by adding analysts and requirements managers.

Conclusion

The United States' commitment to democratic principles, individual freedom, and support for human rights is essential to our leading role in the world community, but increases our vulnerability to asymmetric, unconventional, or indirect actions. Our involvement in world affairs and the secular nature of our government are perceived as threatening to some ideologies, cultures, and religions. Our relative wealth generates resentment in populations and regions that lack the resources to meet the basic needs of their people. The result—against a background of ethnic friction, civil war, and large refugee populations—is often an environment hostile to the United States.

Transnational organizations have and will continue to wage overt and covert war against the United States. Campaigns conducted against our nation will leverage proliferation in technology; nuclear, biological, and chemical (NBC); and unconventional international actions. Examples of these include the 1993 bombing at the World Trade Center, 1996 attack on Khobar Towers, 1998 destruc-

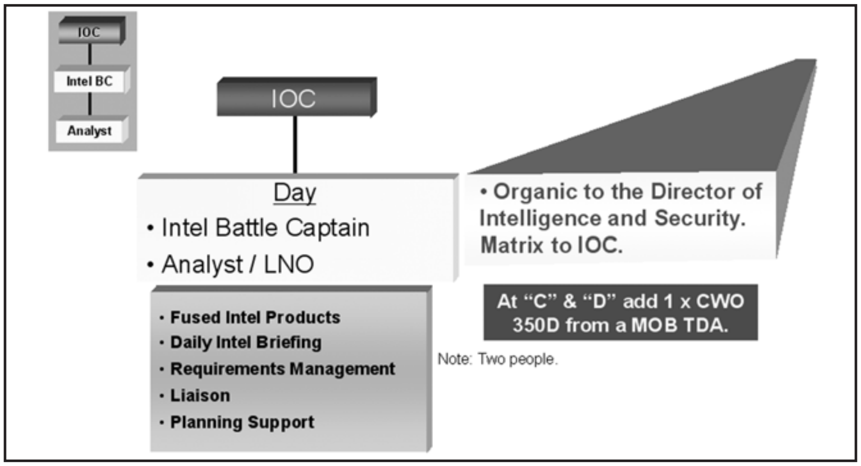


Figure 5. Regional Battlespace.

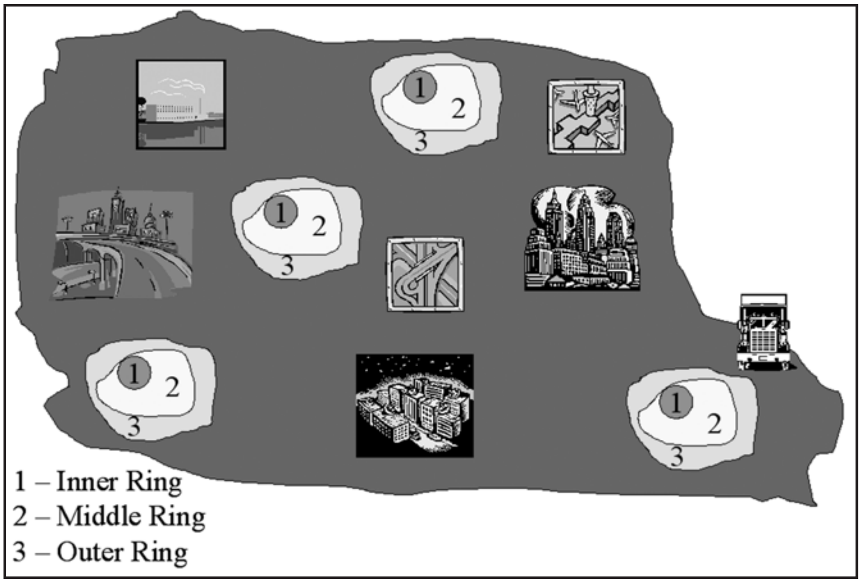


Figure 6. Regional Information Linkages.

tion at two U.S. embassies in Africa, the 1999 Millennial Bomber, the 2000 attack on the U.S.S. Cole off Yemen, and the 2001 World Trade Center and Pentagon attacks.

The transformation of the Army and the shift in operational environment coupled with increased terrorist attacks against the United States dictate that the Army review its capabilities and adjust its organizational structure to prevent, deter, defend, and respond to any type of terrorist attack against its installations. As outlined in the Quadrennial Defense Review, dated 30 September 2002:

> *The highest priority of the U.S. military is to defend the Nation from all enemies. The United States will maintain sufficient military forces to protect the U.S. domestic population, its territory, and its critical defense related infrastructure against attacks emanating from outside U.S. borders, as appropriate under U.S. law.*

Endnotes

1. The basis of this article is the USAIC&FH submission to Headquarters TRADOC for the *Force Protection Organizational and Operational Plan* dated 30 July 2002.

2. According to the Assistant Chief of Staff for Installation Management (ACSIM) Plans and Operations Division, *Major* installations have an ***Army Stationing and Installation Plan*** *(**ASIP**) (**AR 5-18**)* total population of 5,000 or more. *Minor* installations have an ASIP total population of 1,000 to 4,999 or a U.S. civilian population of 300 or more. *Other* installations have an ASIP total population of 1 to 999 and U.S. civilian population of less than 300.

3. While this section discusses ISR in a MACOM, the concept, required capabilities, and force design could apply to a regional organization rather than MACOM structure.

4. Due to their mission and location, some *Minor* and *Other* (see note 2) installations will require a larger dedicated capability. Each *Minor* and *Other* installation must conduct a task and purpose analysis including a troop-to-task analysis to determine the exact requirement.

Jerry Jones (Colonel, U.S. Army, Retired) is currently the Chief of Concepts, Architectures, and Requirements (CAR) in the Directorate of Combat Developments, U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH), where he serves as the concepts development and future requirements subject matter expert. He was a contractor with USAIC&FH responsible for planning and executing training for the Initial Brigade Combat Team following his 30-year retirement from the Army on 1 June 2000. He finished his Army career at Fort Huachuca, Arizona, as the Commander, INSCOM Training and Doctrine Support (ITRADS) Detachment. He served at all echelons from tactical to national and was a 35F (Human Intelligence Officer) with significant 35E (Human Intelligence Officer) experience and a 6Z (Strategist). He began his career as an Armor officer with the 1st Armored Division (1 AD) at Fort Hood, Texas. After Vietnam, he served with the "Big Red One" at three Reforger exercises, 32d Army Air Defense Command (AADCOM), 1 AD, in Germany; special mission units in the U.S. Army Intelligence and Security Command (INSCOM); U.S. Central Command J5 operations in DESERT SHIELD and STORM; and the Allied Military Intelligence Battalion in Bosnia. Readers may contact the author via E-mail at jerry.jones@hua.army.mil and by telephone at (520) 533-6869 or DSN 821-6869.

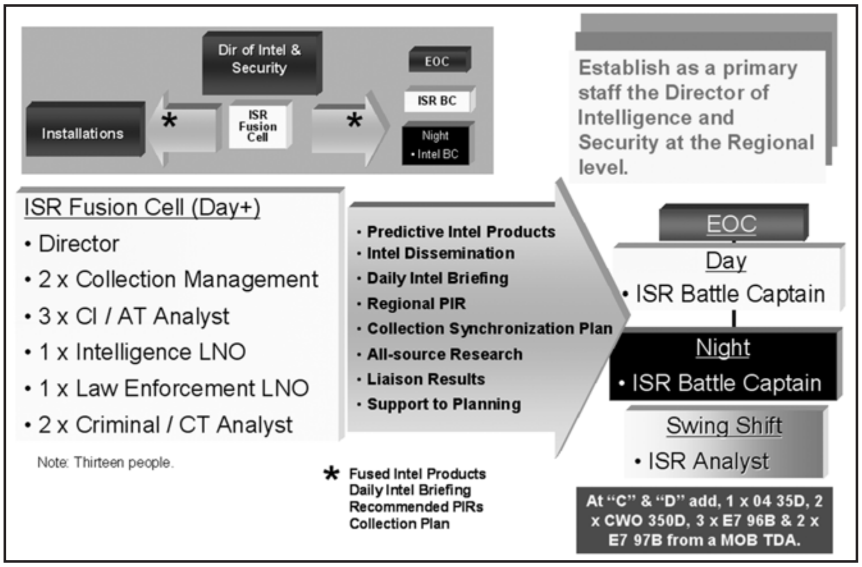


Figure 7. Regional Fusion Cell.

Force Protection at the Installation Level

by David L. Koch

Terrorists attack targets that are vulnerable, have a high psychological impact on a society, produce significant publicity, and demonstrate a government's inability to provide security. Both critical facilities and prominent individuals are potential terrorist targets.....Military facilities are a symbol of national power; a source of arms, ammunition and explosives; and a prestigious target that adds to the terrorist's reputation.

—CJCS Handbook 5260[1]

We hear almost daily on every major news network stories about "force protection" (FP) and "Homeland Security" (HLS). To a few, these words may just be the latest buzzwords to hit the airwaves but to many more of us they are about protecting and securing our future while preserving our way of life. Those topics and several innovative programs represent a renewed and bolder approach to protecting our national interests at home and abroad.

These new programs and direct information-sharing between agencies are a direct result of the 11 September 2001 attacks on the United States. They are a critical element in our Global War on Terrorism and will continue to influence this nation and its people for many years to come. Gone are the days of thinking such events only happen in Third World countries, Europe, or the Middle East. We, the United States of America, the mightiest nation in the world, now fully understand just how vulnerable we are as a nation to terrorists. With terrorism at our door, intelligence-collecting, information-processing, and information-sharing among agencies continues to be some of our greatest tools to combat terrorism.

The events of September 11 have placed a far greater emphasis on FP and HLS. Furthermore, the manner in which we respond to emergencies and crisis management has changed significantly during the last year. Force protection is not a passive program, it is about being proactive, constantly alert, and aware of our surroundings. Our leaders have been dealing with FP and related issues for years. Only now some of the rules have changed and we are much more focused and vigilant. We have more closely balanced standards, procedures, and requirements to the overarching mission of the organization and the military installation. This article will focus on FP at the installation level.

Force protection is everyone's duty and applies across the entire command structure, from the newest private to our Commander in Chief. FP is a security program designed to protect soldiers, civilian employees, family members, facilities, and equipment in all locations and situations from threats which include terrorists, criminals, disaffected persons, hostile intelligence collectors, paramilitary forces, protesters, and saboteurs. To accomplish this goal, an organization must have an effective program that is proactive and prevents, deters, defends, and can respond to any threat or situation. Such a program is centralized and focused on a holistic management approach at the command, installation, and unit or activity level. This program identifies, consolidates, and synchronizes detailed FP requirements with a current risk assessment and prioritizes a distribution list of resources. Each organization must continuously monitor and validate its force protection program (FPP). In order to be effective, the FPP must advance at the same rate as major advancements in technology and intelligence collection.

SIPRNET capability available for the Battle Captain (Robert Bass, Jr.) and the G2.

Photographs courtesy of Holly R. Sickels, Installation Ops (G3).

Weekly Battle Update Brief (BUB) involves the entire Crisis Action Team (CAT).

Force Protection at the Installation Level

As stated above, FP applies across the entire organizational structure. Since 11 September 2001, the military Services have developed, written, revised, and published numerous manuals and regulations emphasizing the new procedures and changes required to protect our military installations. Some of the more critical requirements appear below:

- □ Appoint a force protection officer.
- □ Develop, implement, and maintain an overarching installation FPP that synchronizes the five existing security programs:
  - ● Physical security.
  - ● Information security.
  - ● Protective services.
  - ● Law enforcement.
  - ● Antiterrorism.
- □ Establish a force protection committee (FPC). The FPC should have at a minimum representation from the following agencies, directorates, and sections: law enforcement, G3/S3 plans and training, G2/S2 security and intelligence, engineer, information management, logistics, medical, legal, safety, resource management, and public affairs.
- □ Conduct FPC meetings twice annually and incorporate the responsibilities of the physical security (PS) council required by **AR 190-13**, **The Army Physical Security Program**.
- □ Ensure FP requirements have a high budget priority and maintain a strict audit trail for FP funds.
- □ Ensure the aggressive management of FP in compliance with Department of Defense (DOD), Department of the Army (DA), and U.S. Army Training and Doctrine Command (TRADOC) plans, policies, and guidance. (Fort Huachuca is a TRADOC installation.)
- □ Conduct an annual FP exercise that includes a mass casualty (MASCAL) exercise.
- □ Incorporate FP special-interest inspection items in the Command Inspection Program. (Each installation develops its inspection items.)
- □ Publish and maintain an installation force protection plan.[2]

Force Protection Program

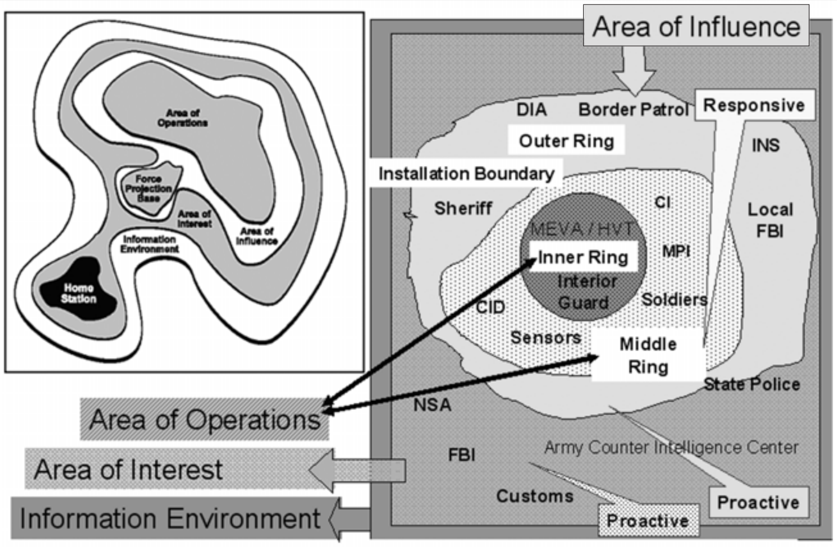
The installation or unit commanders do not develop the FPP alone. The installation commander develops and maintains the FPP with coordination and input from all agencies involved in the execution of the program. At the installation level, this should include all directorates, major organizations, and tenants. The program development must fully integrate non-DOD agencies at the local, state, and federal levels.

The goal of the FPP is to provide protection to the installation personnel, facilities, and critical assets, as well as to safeguard information. The development of high-risk personnel (HRP) and mission-essential vulnerable areas (MEVAs) lists meet this requirement. Updated annually, those lists should become part of the commander's critical information requirements (CCIRs).

The FPP must address units and individuals going outside the United States for deployments and mobilization operations. Since the absolute and continuous protection of all the personnel, structures, activities, and equipment under the commander's control is unrealistic, he and his staff must prioritize the resources and assets and clearly specify the required level of protection during various periods.

Furthermore, the program must look beyond the installation's physical boundaries. Monitoring and linking local government agencies and the plans and procedures are critical. The installation and local community rely on one another, and a sound working relationship between the two is essential for any plan to be successful.

A good example to illustrate this point would be the need to evacuate a portion of or the entire installation. Are plans in place with the community and have they practiced them? What are the egress routes? Where are the rallying points? Where are the shelters? Are they on or off the



Key:

CI – Counterintelligence
CID – Criminal Investigation Detachment
Customs – U.S Customs Service
DIA – Defense Intelligence Agency
FBI – Federal Bureau of Investigation
INS – Inmigration and Naturalization Service
MPI – Military Police Investigation
NSA – National Security Agency

Figure 1. Installation Battlespace.

installation? Who are the community Red Cross and community emergency coordinators? This information exchange between the installation and the community is critical. Developing a sound working partnership means understanding that neither is able to sustain itself fully without the other. Installations and communities should exercise this partnership at least annually with the goal of sequentially and successively building upon each other's capabilities. The training value and knowledge gained through a combined exercise builds trust and teamwork and identifies each group's limitations and capabilities.

The Installation Battlespace

A military installation is comparable to a medium-size city with its countless service members, families, employees, and critical facilities. Like many cities where a mayor runs the community's day-to-day business, the military assigns an installation commander to manage these and the other complex installation operations. The installation commander is ultimately responsible for force protection and everything that does and does not happen on the installation; he accomplishes this through the garrison commander. Unit commanders on the installation are responsible for FP at their levels and within the scope of their commands. The installation commander clearly defines and assigns responsibilities to the installation operations center (IOC) and the post directorates, much the same way tactical commanders apply their forces on the tactical battlefield.

The critical element at this level is an intelligence, surveillance, and reconnaissance (ISR) cell fully integrated into the IOC. The primary function of the ISR cell is to keep the commander apprised of the current situation and its impact on the installation. Compiling and analyzing data from numerous sources accomplishes this. This integration of the IOC and ISR cell enables the IOC to remain focused on the situation at hand and eliminates developing unnecessary courses of action (COAs).

Figure 1 provides a graphic illustration of converting a tactical battlespace to an installation battlespace. The installation boundary is the area of operation (AO). The AO consists of an inner, middle, and outer ring. The inner ring includes consists of the critical elements that must receive protection (e.g., high-risk targets [HRTs], MEVAs, and HRPs). The middle ring includes the remainder of the installation confines such as housing, ammunition storage areas, etc.

The outer ring does not have a finite boundary so the installation commander must define it as the area of influence (AI). The AI includes areas that the commander can directly influence through such activities as contacts with local government officials, law-enforcement agencies (LEAs), and emergency management agencies through public affairs command-information channels.

The area of interest (AOI), although not specifically addressed in an FPP is of concern to the installation commander. The AOI may include areas distant from the installation, in which events may occur indicating changes in the threat to the installation. It may also include contacts or information received from national and state LEAs, and intelligence or emergency-management agencies relating to the AI or AO of the installation. All of these are relevant to the installation commander and influence his decisionmaking process.

Once the commander has clearly defined the battlespace, the installation can maximize all five critical elements programs to protect the installation and its inhabitants—

□ Physical security.
□ Information security.
□ Protective services.
□ Law enforcement.
□ Antiterrorism.

All aspects of the battlespace are critical; the two outermost areas (AI and AOI) are the most critical to the commander and the ISR cell. Any advance warning and knowledge gained by the cell greatly enhances the commander's ability to select the

The "Smart Sympodium," an interactive lectern integration module allows the user to create an interactive presentation with projection of electronic notes on any of the IOC's scrrens.

best COA to allay the threat. Remember, one of the first goals in FP is to deter and mitigate the threat.

FP Training Plan

A training cycle is essential and must focus on the most probable means of attack and the "what if" scenarios. When it comes to the means of attack, the G2 and ISR cell are good places to start, just make sure that your CCIRs and priority intelligence requirements (PIRs) are up to date. A proven training mixture of weekly special-subject briefings, monthly "tabletop" exercises, with two or three full-scale exercises is a full load and works well during most of the year. This approach allows you to do the "walk, crawl, and run" steps with each exercise building on the previous one, and it works well regardless of an organization's size. Additionally, this approach allows all tenants to it develop their internal training objectives in conjunction with the installation mission, thus balancing the mission with the exercise. Also, when developing a training plan, go beyond just control of access; access control is a primary concern and the focal point for many installations; however, it is only the start.

Look at the major sources of utilities on the installation and how they individually affect it. View the installation and facilities from a terrorist's viewpoint. Where do I get the biggest bang for my efforts? Are gas lines, water-pumping stations, and major electrical plants easily assessible? Once identified, conduct a tabletop exercise with the IOC personnel and tenants involved. Assess the impact and resources needed to restore service. A possible training scenario could be eliminating a power substation near the commissary, or a MEVA for 24, 36, or 48 hours. What effect will it have on the installation, nearby units, soldiers, and residents? A primary player, the Directorate of Installation Support (DIS) understands the impact perhaps more than any other organization on the installation. However, other tenants need to be involved, such as the public affairs office (PAO) and should be included in the exercise.

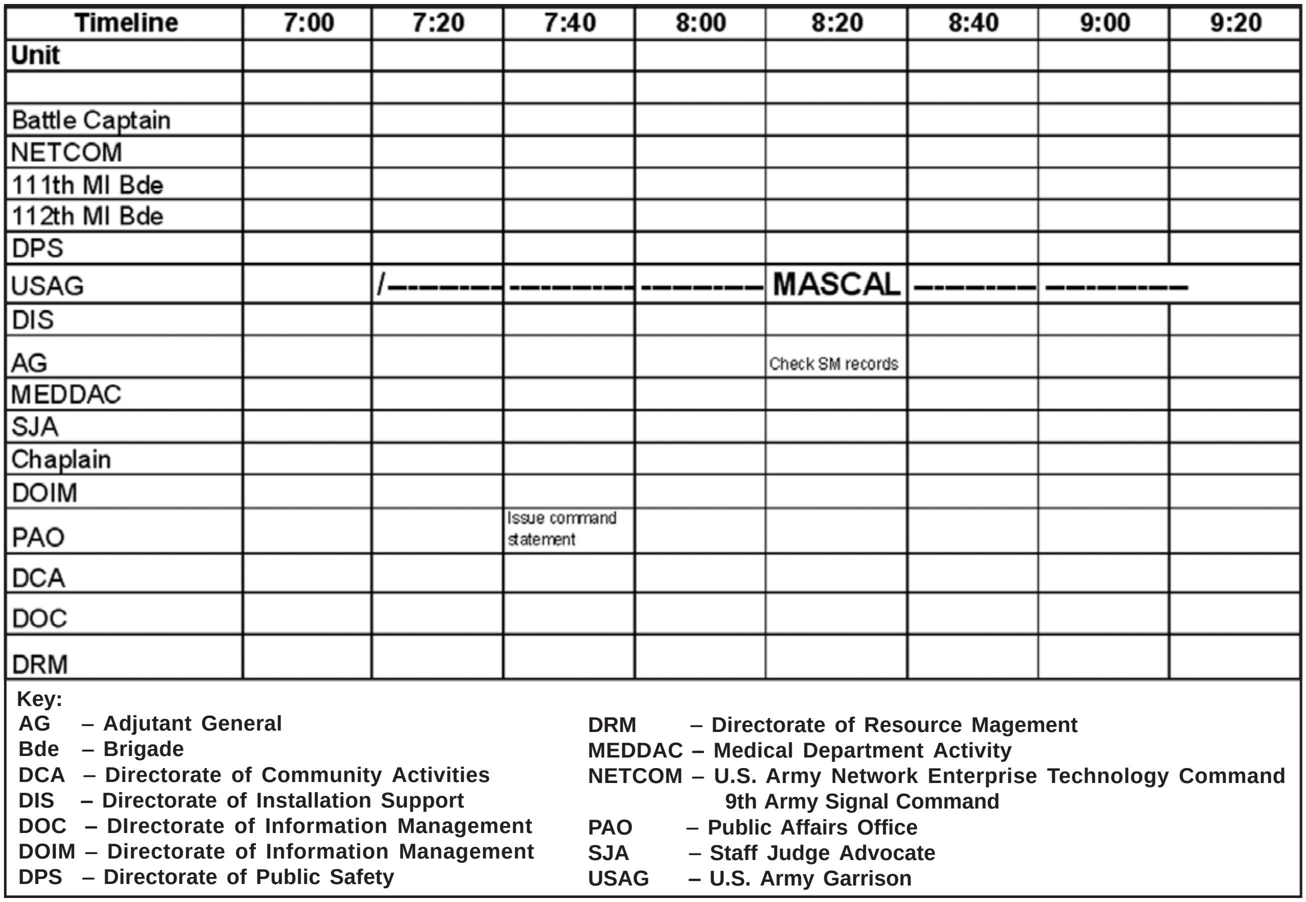
Other scenarios to consider would be a notional bomb threat to a building, especially if it is a very large and prominent structure, or a simple fire drill in the same building. Does the building coordinator have rally points identified far enough away from the building? Is there an accountability procedure?

Exercise Apache Gold

Fort Huachuca recently conducted a postwide, one-day exercise with six major events consisting of—

- ❑ Force protection procedures.
- ❑ An airplane crash.

The results of the "Smart Sympodium" appear on the big screen.



Timeline	7:00	7:20	7:40	8:00	8:20	8:40	9:00	9:20
Unit								
Battle Captain								
NETCOM								
111th MI Bde								
112th MI Bde								
DPS								
USAG		/-------	--------	-------	MASCAL	-------	--------	
DIS								
AG					Check SM records			
MEDDAC								
SJA								
Chaplain								
DOIM								
PAO			Issue command statement					
DCA								
DOC								
DRM								

Key:

AG – Adjutant General
Bde – Brigade
DCA – Directorate of Community Activities
DIS – Directorate of Installation Support
DOC – DIrectorate of Information Management
DOIM – Directorate of Information Management
DPS – Directorate of Public Safety

DRM – Directorate of Resource Magement
MEDDAC – Medical Department Activity
NETCOM – U.S. Army Network Enterprise Technology Command 9th Army Signal Command
PAO – Public Affairs Office
SJA – Staff Judge Advocate
USAG – U.S. Army Garrison

Figure 2. Sample Exercise-Planning Matrix.

❑ A MASCAL event.
❑ Emergency evacuation plan (EEP).
❑ Emergency evacuation drill (EED).
❑ Hostage scenario.
❑ Seventy-five additional smaller events.

The Exercise, similar to one conducted at the beginning of the year with the Battle Command Training Program (BCTP), stressed the IOC and validated two new programs: the EEP and EED. These two programs are internal to Fort Huachuca. (Installations interested in these plans should E-mail or call the author.) The EEP is essentially the evacuation procedures used to relocate or evacuate family members on the installation from the threat area and, if necessary, evacuate them to a safe area off the installation, similar to noncombatant evacuation operations (NEOs) overseas. The EED is a list of procedures and local guidance to evacuate and account for all employees of a building. This is similar to a fire drill but contains additional information with a set timetable. The Exercise called for an EED to test the plan and procedures. Several directorates conducted their own internal drills in conjunction with the Exercise. The Exercise highlighted several pitfalls in our plan and the directorate's procedures; as a result, we have done more planning and revising to improve our plans and procedures.

The Exercise was a resounding success in part due to the planning and our ability to locate the "white cell" (controllers) a few doors down from the IOC. The controllers' cell, staffed by four individuals, injected the core scenario and other small events to the various participants inside the IOC. Figure 2 is an example of the chart used during the Exercise. It lists the units and tenants on the left side and across the top are time blocks broken down into 20-minute intervals. As in any exercise planning, the objectives started the planning process, which allowed the planners to develop the major events. Once they enter the major events into the chart, they added additional training objectives to the scenario to drive each directorate to conduct planning and problem-solving. This chart is a great tool and allows for crosswalking of each event, shows the time needed for completing each event, and helps identify problems before the exercise starts.

The chart cannot consider the unexpected as was the case when we had a real-world range fire divert our attention. The fire, small in comparison to the others in Arizona this year, consumed approximately 50 areas of range and diverted fire and LEA personnel to the scene. The impact was in dealing with the exercise and the fire simultaneously. One of our revised planning considerations was that if

Cordless headset telephones allow hands-free operations and reduce noise in the IOC.

real-world events happen during the exercise, we would postpone the exercise as needed.

In using this planning matrix, the user would enter any major events such as a MASCAL or hostage scenario first, followed by additional events that cause other important members in the IOC to perform additional tasks. For example, during a MASCAL exercise, the planners could enter an additional inject for the Adjutant General (AG) to review service members' records for next-of-kin and insurance data or for the PAO to produce and post an official press release. This verifies not only the IOC procedures but also the internal AG and PAO procedures. In addition to using the planning matrix for planning the exercise and critical events, it is also a great tool to identify who should be doing what and when.

Lessons Learned

Fort Huachuca has taken great strides to improve upon every aspect of its FP program. The installation has conducted extensive planning, implemented construction projects, upgraded its IOC, increased training exercises, and invested in technological enhancements. Combined, they continue to increase our ability to prevent, deter, and improve our ability to respond to any threat or situation.

It has not been an easy road for the installation. However, the lessons learned during the previous year provide insight that could help other installations enhance their training and preparedness for the future.

Without exception, Fort Huachuca saw more than its share of unforeseeable events during 2002, starting with the Ryan fire. The Ryan fire, which started southwest of the installation, worked its way across the countryside to 1,800 acres on our installation. The result was a complete loss of power to the installation for nearly 24 hours, as both primary and alternate powerlines and poles burned to the ground. Talk about crisis management! We had a large uncontrollable fire spreading across the installation and were faced with the possibility of evacuating some, if not all, of the installation residents. There are far too many lessons learned to discuss them all, and the threat of fire might not be as prevalent at other installations as at Fort Huachuca. However, the loss of electrical power is a real possibility everywhere. Is your installation prepared to deal with the following if electrical power is lost?

- □ Directing traffic, as traffic and street lights will not work.
- □ Emergency power capabilities in the operations center.
- □ Cold food-storage procedures (commissary and homes).
- □ Alarm systems in arms rooms and in sensitive compartmented information facilities (SCIFs).
- □ A postwide curfew for safety reasons.
- □ Communications capabilities (computer servers and telephones).
- □ The post cannot restore electric power until the area is safe and has obtained clearance from the controlling agency, whether that is the forestry service or some other state or local agency.

Another unexpected situation, a civilian brandishing a handgun, forced a limited evacuation of family members from their quarters and the immediate area. Issues of how and what do we do with the families during the cold night become immediately apparent. Fortunately, due to extensive training and scenario-driven exercises, the installation was able to bring the situation under control quickly and without implementing our emergency evacuation procedures.

These two examples are just the beginning of the endless variety of unexpected situations any installation could face. Twice within a year, Fort Huachuca had to respond quickly to developing dangerous situations.

Although, an FPP might not cover fires or other disasters, it provides a solid foundation that enables the installation to deal with the unexpected situations. This installation was able to adapt the existing plan to the situation at hand. The training conducted periodically throughout the year reinforced the standards and procedures. Another positive lesson learned is that the real-world incidents allowed us to see our strengths and weaknesses and will help as we modify and improve our plan.

Conclusion

The installation is continuing to develop and update its IOC to handle such events. Additionally the ISR cell and FPP are making improvements daily with a combined team of experts. As the photographs of the IOC show, it is clear that force protection is a priority and a holistic management approach is in use on this installation. Technology enhancements will continue in the near future with the additions of a video matrix system, a reverse 911-telephone notification system, and additional digitized maps, which integrate the installation utilities and service schematics to the command center. Nevertheless, the core effort will be our training and planning events focused on present and most probable emergency events in the near future.

Endnotes

1. CJCS (Chairman, Joints Chiefs of Staff) Handbook 5260, Commander's Handbook for Anti-Terrorism Readiness (Washington, D.C.: Department of Defense, 1 December 1996).

2. This list comes from two sources:

□ **Army Regulation 525-13**, **Military Operations, Antiterrorism** (Washington, D.C.: Department of the Army, 4 January 2002).

□ **TRADOC Regulation 525-13, Force Protection Program (FPP)** (Fort Monroe, VA: Training and Doctrine Command, 12 December 1997).

The list emphasizes the major points that this article needs to address. Additionally, several of the items mentioned above have manuals devoted to their procedures such as physical security, information security, protective services, law enforcement, and antiterrorism. This is not a complete list, and you should review both references before developing your program.

David Koch is an Operations Officer in the Directorate of Installation Operations (G3), U.S. Army Intelligence Center at Fort Huachuca, Arizona. Readers may contact him via E-mail at david.koch@hua.army.mil and telephonically at (520) 533-7471 or DSN 821-7471.

Free Training for DA Civilians

As a Department of the Army (DA) civilian registered in the Army Knowledge Online (AKO) system, you are eligible for this program provided by the Army Chief Information Officer/G6. (If you are not a DA Civilian, you may still be eligible and should update your status code in AKO. Due to a lack of funds, retirees and contractors are not authorized users. They can acquire a special license for unlimited use.)

This distance learning material includes personal mentoring and covers business skills, interpersonal skills, computer user skills, and information technology (IT) certification coverage. You can access this system from anywhere at any time. All authorized personnel can access about 1,500 IT business and interpersonal skills courses and have access to personal mentoring for all certifications and many other programs—all at **no cost** to the individual or the unit. Promotion points, retirement points, and college credit are all possibilities. We will continually update the library of courses. Specific recommendations for GS-2200 (IT series group) and CP-34 (Information Management Career Program) will soon be available.

The Army Training Requirements and Resources System (ATRRS) offers automated registration. ATRRS verifies your eligibility for the program and also posts successfully completed courses to the user's official ATRRS training record, and it also produces certificates.

If you want to receive the free monthly SmartForce Army Newsletter to keep abreast of the latest updates, please request it by E-mail and provide the E-mail address you wish used. In addition, a copy of the Program Listing (course catalog) is available upon request by E-mail. (AKO will send it as an attachment.)

□ To access the new system, go to www.us.army.mil and follow the link to Self Service > My Education > Army CBT.

□ For assistance with AKO, access the web site FAQs/Help, or call 1-877-256-8737 (DSN 654-3791).

□ For assistance with any difficulty in ATRRS, please logon to http://www.atrrs.army.mil/help or call 703-695-2060 (DSN 225-2060).

□ For assistance with program registration or any other difficulty you are experiencing, call 1-800-275-2872 (DSN 826-3666) or email help@atsc.army.mil

□ For assistance with computer-based training (CBT) program or contract management, please contact the Army CBT contracting officer's representative (COR) at cbtcor@secbmail.belvoir.army.mil (703-806-3671, DSN 656-3671).

□ For assistance after registration with logon and password, call SkillSoft Tech Support at 1-800-938-3247 or E-mail support@smartforce.com.

□ For customer assistance with questions other than registration and password, logon to MySmartForce and use the Help buttons throughout the site or E-mail Army@smartforce.com.

G2 Contributions to the Threat and Vulnerability Assessment

by MI Doctrine Writing Branch

The threat and vulnerability assessment (TVA) is a complete staff product, combining a threat assessment and a vulnerability assessment. The preparation of the terrorist threat assessment is a continual process of compiling and examining all available information to identify terrorist targeting of U.S. interests. A vulnerability assessment is a continual process of compiling and examining information on a facility's security posture. The assessors then pair the threat analysis with the facility's vulnerability analysis to create the threat and vulnerability assessment.

The TVA analyzes all the aspects of physical security, personnel security, information security, and communications security. It measures the current threat capabilities against emplaced security measures and operating procedures to identify vulnerabilities.

Background

The provost marshal (PM) function provides command policy and oversight of the command security program. The security program is one of several security-related programs that fall under the overarching umbrella of force protection (FP) and law enforcement.

The command high-risk personnel (HRP) program encompasses the following subordinate functional areas:

- ❑ TVA.
- ❑ HRP designation.
- ❑ Personnel security vulnerability assessment.
- ❑ Implementation of HRP-specific security measures.
- ❑ HRP training and awareness.

Ideally, upon request, the local Federal Bureau of Investigation (FBI) field office and other local law-enforcement agencies (LEAs) will provide periodic intelligence to the installation commander. The PM is a crucial player in the installation commander's FP mission and is the focal point for receipt of domestic threat information from the domestic LEAs. The PM is the conduit for domestic threat information-flow between the FBI and the installation commander. Normally, the PM must initiate a request for intelligence information from these outside agencies to formulate a "local threat analysis."

G2 Responsibilities for the TVA

The installation G2 is responsible for the oversight of intelligence operations (IO) and the maintainance of current information on the threat. Once the commander directs the conduct of a TVA, and the G3 has tasked the appropriate organizations, the G2 begins assembling all information concerning the threat or threats (within the guidelines established by **AR 381-10**, **U.S. Army Intelligence Activities**) affecting the installation for which the TVA is under development. Essential to the assessment is a continuous analysis of the local threat. This threat assessment will provide the basis for the security planning and measures to be implemented.

The G2 supports the Army's antiterrorism and force protection (AT/FP) program by collecting, analyzing, producing, and disseminating intelligence on a wide spectrum of foreign threats to the Army. By identifying and assessing international threats and threat levels, intelligence provides early warning and enables commanders to designate an appropriate force protection condition (FPCON). In continental United States AT/FP operations, MI provides the foreign aspects of local threats, while law enforcement collects, analyzes, and disseminates domestic criminal and terrorist threat information.

Threat, when used in terms of the TVA, can be opposing military forces, paramilitary forces, terrorist organizations, criminal organizations, foreign governments, threat intelligence operations, and local nationals, just to name a few. The G2 must accurately identify and articulate the exact threat that each organization or group poses to the installation and its soldiers.

The G2 uses the intelligence, surveillance, and reconnaissance (ISR) plan through his knowledge of all the assets capable of gathering information, developing requirements, and recommending information requirements as the tool with which to update information concerning the threat constantly. This information comes not only from the traditional MI assets but also from all organizations through the reporting of combat information. The G2 also uses "reach" to obtain information concerning the threats. To prepare the assessment, the G2 will integrate threat information prepared by the intelligence and law-enforcement communities, local and host-nation sources of intelligence, technical information from security and engineering planners, and other sources as deemed appropriate to the local situation.

The G2 provides a written assessment addressing all potential threats. Those products the commander requires for the AT/FP program support the assessment. Supporting products will vary depending on the location of the installation for which the staff is conducting the TVA.

Having covered the G2's contributions, it is equally important to dis-

(Continued on page 61)

Force Protection In Korea: A 2d Infantry Division Perspective

by Chief Warrant Officer Three Wayne S. Miller

The views expressed in this article are those of the author and do not reflect the official policy or position of the 2d Infantry Division, U.S. Army, Department of Defense, or the U.S. Government.

The events of 11 September 2001, served as a wake-up call and a paradigm shift of drastic proportions for the United States of America and its military forces. For the first time since World War II, a foreign entity had successfully attacked the United States on its home soil. Force protection (FP), on both a practical and an ideological level, changed drastically.

Post-September 11 Activity

Across the globe, U.S. forces immediately took stock of their situations, identified local FP issues, and scrambled to correct those shortcomings they were able to influence. Immediately following the September 11 attacks, the Department of Defense elevated the force protection condition across the Korean Peninsula to the highest FPCON, "Delta."

While there was no evidence of a terrorist threat to U.S. service members in Korea, the FPCON remained elevated until a clearer picture emerged concerning the actual threat. During this period, the 2d Infantry Division (2 ID) had essentially "locked down" its various base camps, with no civilian employees allowed on post and only mission-essential U.S. personnel allowed off post. Before September 11, 2 ID had never elevated its FPCON to Delta, and the change presented a steep learning curve. While 2 ID had elevated its alert status during periods of heightened tension (e.g., when two U.S. officers were bludgeoned to death in a melee with North Korean border guards in the Joint Security Area on 18 August 1976), it had not elevated the FPCON (formerly called THREATCON) since this system of threat designation has been in use.

By its very nature, FPCON Delta dictates that all missions halt except for base security. This includes training, administrative functions, and all but the most critical maintenance issues. Because of this and security considerations, no unit can maintain FPCON Delta indefinitely.

After ten days at FPCON Delta, 2 ID reviewed the local threat and, in coordination with Eighth United States Army (EUSA) and U.S. Forces, Korea (USFK), decreased the FPCON to "Charlie" with some antiterrorism (AT) measures included for FPCON Delta. This essentially left 2 ID at "Charlie+"; even FPCON Charlie+ severely affected the missions and activities within 2 ID when compared to those at FPCON "Normal" before September 11. Due to the increased guard and security requirements, the Division still had to curtail its missions and training severely. Soldiers were still confined to base camps except for official business, and all movement between camps was limited to official U.S. Government transportation only, to include contracted buses and AAFES taxis. The Division placed all off-post clubs and shops off limits and personnel residing off-post with their families had to have a "buddy" accompany them when traveling to and from work.

Once the FPCON lowered to Charlie+, 2 ID did a scrub to determine which civilian employees working at the camps were "essential" and which were just "nice to have." Due to this scrub, 2 ID was able to determine what services provided by local nationals were truly vital and concluded that some of these services enjoyed by 2 ID personnel were simply not essential for day-to-day operations. This scrub resulted in the development of a matrix dictating exactly who would be allowed on post during any given FPCON.

Increased Need for Augmentation

Before September 11, the security of 2 ID camps was the sole purview of the military police (MPs). Even though the Korean Security Guards (KSG) augmented the MPs and they have the assistance of the Korean National Police (KNP) for exterior security issues, they did not have sufficient personnel to meet the security requirements levied upon them by the elevated FPCON. Because of this, soldiers throughout the Division received training in proper social procedures and began performing vehicle searches, searching individuals desiring entrance into camps, executing perimeter security patrols, and taking care of various other camp security issues. Soldiers also formed a quick reaction force (QRF) for each camp to act as first or immediate responders in the event of a serious incident. This became especially critical for those installations lacking on-post MP support. In some cases, depending upon the traffic congestion, the MPs may not be able to respond quickly to some

Photographs courtesy of Vic Lowe, CRC/USAG FP Officer.

Korean Police fight off protesters at Camp Red Cloud Visitors Booth.

of the satellite camps after they call; on the best days, it may take as long as 30 to 40 minutes to travel 6 kilometers due to the heavy traffic.

In addition to the personnel strain placed on 2 ID due to FPCONs Charlie and Delta, the Division also expended a great deal of unprogrammed funding. The higher FPCON levels dictated the emplacement of barriers and other devices to restrict vehicle movement through and around the gates and critical buildings throughout the Division, necessitating construction or emplacement of additional barriers to meet these requirements. The September 11 attacks also pointed out the need for additional lighting, mirrors used for vehicle inspections, better intra-agency communications, closed-circuit television cameras, and numerous other items. Several construction and repair issues, such as fences and walls, received an elevation in priority and 2 ID accomplished them with a renewed sense of urgency.

While it would be difficult to imagine anything good coming from the attacks of September 11, they did force 2 ID to take a hard look at its security posture and identify some shortcomings that needed addressing. This close scrutiny prepared the Division for the events and challenges that it would face during the summer of 2002.

Protests Beginning in June 2002

As horrific and significant as the events of September 11 were, it may be argued that the string of events that began on 13 June 2002 has more directly affected FP for U.S. forces in Korea, specifically for those soldiers serving in the 2d Infantry Division. On that date, two young Korean school girls, Shim Mi-Son and Shin Hyo-Sun, were killed in a tragic accident when a U.S. Army tracked vehicle involved in convoy operations struck them from behind while they were walking along Highway 56 in Kyong-gi Province. This accident, and the subsequent investigation, sparked a firestorm of protests. The first of these protests took place on 20 June at Camp Red Cloud, the home of 2 ID headquarters.

Protests in the Republic of Korea (ROK) are allowed and, in some respects, encouraged as a method of expressing free speech in this relatively new democracy. Protesters must submit a request to hold a demonstration to the local police, and the demonstration permits often cover a period of several weeks. Demonstrations are not to be violent, and they must occur during daylight hours. The protest on 20 June was sanctioned and began peacefully. It was also quite small, with fewer than one hundred protesters, to include several relatives of the victims. While it started peacefully, it soon escalated and turned violent, resulting in a significant disruption of military operations and damage to U.S. Government property. Both the Korean Police and U.S. military personnel in charge of the main gate were completely unprepared and overwhelmed.

The protest that followed on 26 June was also violent, resulting in several injuries to U.S. personnel. Protesters, acting with military precision, distracted the riot police with a rush at the main gate of Camp Red Cloud while others surreptitiously cut a hole in the fence 30 meters north of the gate, thus gaining access to the installation. Security forces quickly apprehended those protesters who gained access to the installation. While waiting for a fire hose and concertina wire, U.S. personnel outfitted with riot-control gear fought with protesters and guarded the hole in the fence. Seeing their newly created entrance blocked, protesters assaulted the U.S. soldiers with a hail of kicks, rocks, bricks, and bottles. Intent on drawing blood, protest leaders instructed the rioters to throw rocks and bricks at the soldiers' feet and shins to make them lower their riot shields, exposing their heads. Their tactic was successful and several U.S. soldiers were struck in the head and face, injuring them.

Liaison with Korean LEAs is Crucial

One of the greatest FP assets available to U.S. forces is our relationship with these Korean law-enforcement agencies (LEAs). Because of this close relationship, liaison is constant, resulting in a superb flow of information. It is a rare event when a protest occurs without prior notification to U.S. forces. Liaison occurs within law-enforcement and military intelligence (MI) channels, allowing the corroboration of information from more than one source. They analyze, evaluate, and quickly distribute this information to unit commands and unit AT officers (ATOs) to ensure soldiers are aware of any imminent protests or rallies.

In addition to the free exchange of information, this close relationship with the KNP has resulted in their assistance in dealing with violent protests. KNP riot police have been on hand to quell violent protests at several 2 ID installations, including Camps Red Cloud, Casey, Page, and Howze. Hundreds of KNP riot police in full armor met the protesters at Camp Red Cloud in June 2002. This KNP presence undoubtedly reduced the number of injuries to U.S. MPs and other soldiers.

After 2 ID and the KNP realized the size and severity of the protests, the KNP increased the riot-police presence accordingly. When the protests turn violent, this large ratio is welcome and necessary. If the protesters manage to get past the riot police, a cadre of MPs and soldiers in riot gear and body armor meet them.

Protesters' Campaign to Increase Support

All of the protests held as a result of the June 2002 accident had one thing in common: regardless of whether the protest was peaceful or violent, the protesters ensured the presence of a video camera, whether private or from the news media. Through liaison contacts, 2 ID found out early that the protesters wanted to film a protester struck or mistreated by a U.S. soldier. They believed that such an event would help shore up their popular support with the South Korean people and move them closer to their ultimate goal: the removal of U.S. forces from the Korean Peninsula.

It is important to note that until this time, the dissident groups and nongovernmental organizations (NGOs) organizing and leading the protests had little popular support. Almost everyone participating in the demonstrations were NGO group members or relatives and schoolmates of the deceased girls. What the dissidents and NGOs needed to do was move the protests from the realm of dissidents and NGOs to that of common citizens. They proceeded to conduct an extraordinarily well-conceived information operations campaign that eventually led to demonstrations by fifty thousand people in the streets of downtown Seoul.

Korea is the second-most "wired" nation in the world, and protest groups use anti-U.S. websites extensively to post articles, photographs, and short "news" clips depicting what they see as "atrocities" perpetrated by U.S. military personnel. The protesters usually edit these video clips to show a decidedly anti-U.S. bias and designed to stir up their fellow protesters—not necessarily to show events in a factual light. Protest groups have proven that they are not above provoking or attacking U.S. personnel and filming the U.S. soldiers defending themselves. They then edit this video footage to make it appear as if the soldier was the instigator—acting like the quintessential "Ugly American."

For the most part, this tactic has not worked to the protesters' advantage as the majority of U.S. soldiers are circumspect while on the Korean economy and they rarely travel alone. USFK established an extensive training program for all its personnel that emphasizes the benefits of being good neighbors, a familiarization with Korean culture, and what to do in the unlikely event that they are attacked or provoked. Throughout all of the training and briefings, one theme remains constant: the U.S. soldier **always** retains the right of self-defense. While trainers and commanders remind soldiers of this fact, they also emphasize using the minimum level of force necessary and not letting the situation get out of hand.

Korean police fight off protesters at the Camp Red Cloud main gate.

While attacks are very rare, they **have** occurred, to include an altercation on the Seoul subway between protesters and three 2 ID soldiers that resulted in the abduction of one of the soldiers, and another attack against an EUSA officer outside Yongsan Garrison in Seoul that resulted in a knife wound. This last attack, however, may have been criminal in nature rather than protest-related.

Since the accident in June 2002, there have been nearly 350 demonstrations against U.S. forces in Korea, ranging in size from one or two peaceful individuals holding signs or candles (commonly referred to as "one-man protests") to crowds numbering in the tens of thousands. Most of these protests have been peaceful, but almost one-fifth of them have been violent, resulting in injuries and damage from thrown rocks, bottles, bricks, and paint. In a handful of instances, the protesters have gone so far as to resort to surprise attacks using Molotov cocktails. In these cases, the intent appeared to be gaining attention through coverage rather than to cause any significant property damage.

In virtually all cases, information flowed freely between U.S. forces, South Korean police, and the intelligence agencies, resulting in minimal injuries and minimal property damage. We have also been able to use this communications flow to ensure the protesters understand our position on certain issues. At one point during the protests in the summer of 2002, organizers entertained the idea of ramming the main gates with vehicles at several 2 ID installations as a form of protest. These protest organizers were told, via liaison contacts, that such an attack was clearly "crossing the line" and would not be viewed as a method of protest; rather, 2 ID would view it as a blatant terrorist attack and security forces would respond accordingly. Thanks to the clear communications and liaison channels, we averted a potential tragedy and no one was hurt or killed.

Outlook

During January 2003, the pro-U.S. silent majority began holding pro-USFK rallies in Seoul, led mostly by Korean veterans' groups and religious organizations. This appears to be leading to a return of the normally warm relations between the South Korean people and U.S. forces in the Republic of Korea. Regardless, U.S. forces on the Korean Peninsula and in the 2d Infantry Division will continue the day-to-day business of training, soldiering, and working to ensure that those Koreans who protest our presence here enjoy the right to freedom of speech guaranteed by the Government of the Republic of Korea—a government we respect and support.

The author would like to thank Mr. Victor Lowe, Camp Red Cloud Garrison and Area I Anti-Terrorism Officer, and Chief Warrant Officer Two Randy Rogers, 2 ID G2 Force Protection Analyst, for their invaluable assistance in the preparation of this article.

Chief Warrant Officer Three Wayne Miller is a Counterintelligence Technician (351B) with more than 20 years' experience in the intelligence field. He is currently serving as the Counterintelligence Operations Officer and the Assistant Battalion Antiterrorism Officer for the 102d Military Intelligence Battalion at Camp Essayons, ROK, with the 2d Infantry Division. Readers may contact the author via E-mail at wayne.s.miller@us.army.mil.

DOD photo by Senior Airman Jeffrey Allen, U.S. Air Force.

Specialist D. Shewfelt, 4th Squadron, 7th Cavalry Regiment, practicing decontamination after gunnery training at the Korea Training Center.

A 31st Marine Expeditionary Unit amphibious assault vehicle "splashes" from the well deck of U.S.S. Juneau during the combined amphibious landing off the coast of Tok Sok Ri, Korea, during Foal Eagle '02.

U.S. Navy photo by Photographer's Mate 3rd Class James Davis.

Intelligence Support to Law Enforcement in Peacekeeping Operations

by Major Jeffrey E. Jennings and Captain Jennifer V. Gaddis

Previously published in the Center for Army Lessons Learned (CALL) "News From The Front (NFTF)," July-August 2002. Reprinted with permission.

The Military Police are an invaluable partner in Kosovo; I am convinced that the steps that we have taken together to share intelligence and provide mutual support will be retraced in other places around the world.

—Donnie Hensley,
UNCIVPOL Regional Commander

Military intelligence (MI) support to law enforcement during peacekeeping operations is a necessity and a combat multiplier. Success for the peacekeeper is a reduction in violence and a return to normalcy, the creation of an environment in which the rule of law has primacy and people feel safe in their homes. During Operation JOINT GUARDIAN, elements of the 10th Mountain Division (Light) deployed to Kosovo to provide a safe and secure environment where people could live peacefully.

Integrating Criminal Intelligence Into the ACE

Paramount to continued stability in any country or state is a functioning and honest police force. As elements of the 10th Mountain Division (L) became Task Force Falcon (TFF), our commanding general (CG) focused the Task Force (TF) on preventing acts of violence and ensuring freedom of movement for honest citizens, while preventing that same freedom to insurgents and criminals. This type of focus allowed the TF Intelligence battlefield operating system (BOS) to look at crime as a destabilizing factor. MI soldiers assigned to the TFF Analysis and Control Element (ACE) were not accustomed to collecting on or analyzing crime. Given the commander's focus, we made some adjustments to our intelligence analysis techniques and methods of operation, allowing us to employ crime experts, and share critical intelligence with the law-enforcement agencies (LEAs) for use in combating crime in MultiNational Brigade-East (MNB-E).

The intelligence cycle is relevant in the peacekeeping operational environment. Directing, collecting, assessing, and disseminating in a continuous cycle allows the commander to maintain flexibility and prevent violent activities that destabilize his area of operation (AO). In Kosovo, given the commander's intent, as well as a flexible Intelligence BOS and an aggressive military police (MP) battalion, we expanded our collecting, assessing, and disseminating capabilities through the inclusion of LEAs.

As the Kosovo AO continues to stabilize and the rule of law matures, crime and crime prevention clearly are a focus of our commander. By focusing on crime as a destabilizing factor within the MNB-E, our Commander put the Intelligence BOS on a path of closer information-sharing and cooperation with not only the MPs but also the civil police authority—the United Nations Civil Police (UNCIVPOL). As trained intelligence analysts, soldiers within the TFF ACE know how to identify trends, research historical data for comparative analysis, and produce products based on potential courses of action. In peacekeeping, these efforts typically identified areas of inter-ethnic strife that might manifest itself as violence. Adding crime analysis to the ACE was critical in answering the commander's critical information requirements (CCIRs).

Organization of the ACE

The organization of the TFF ACE was not unlike our wartime organization. One unique change made in Kosovo was the addition of two criminal investigation detachment (CID) agents as liaison officers and crime experts. These agents worked directly with the Human Intelligence (HUMINT) Analysis and Requirements Cell (HARC) and greatly increased our HUMINT collection capability by giving us first-hand understanding of crime-scene analysis and direct access to the investigative information. These professionals allowed us to take a more informed approach to crime analysis. We learned what to seek with respect to crime in the volumes of information collected by our HUMINT, signals intelligence (SIGINT), and imagery intelligence (IMINT) collection platforms. By learning about the crime investigations, we learned which indicators to look for in our own reporting that, with further investigation, we could turn into evidence.

...in the HUMINT-rich environment of Kosovo, we found that one of the most flexible collectors we had was the military police

Turning intelligence into evidence was and remains the challenge. By adding the CID agents to our analytical efforts, we learned to identify crime trends better and focused on the destabilizing effects of crime that affected the secure environment

DOD photo by SGT Brendan Stephens, U.S. Army.

Soldiers from the U.S. Army's Bravo Company, 3d Battalion, 504th Parachute Infantry Regiment, and United Nations' police move down a muddy alley in Mitrovica, Kosovo, as they conduct a house-to-house search for weapons. Attached to the 82d Airborne Division, the soldiers deployed to Kosovo as part of KFOR in 2000.

within MNB-E. Our next challenge was to take this information and analysis and put in into the hands of the police.

Support to Criminal Intelligence

The first step in our support to criminal intelligence (CRIMINT) was in place once we integrated CID into the ACE. The second step included fully using all collectors in the sector. National and theater collection platforms provided critical information; maneuver battalions provided their collected intelligence and analysis through daily intelligence summaries (INTSUMs); and TF-level assets helped complete the picture for the command. As we gained experience in the HUMINT-rich environment of Kosovo, we found that one of the most flexible collectors we had was the military police. As a general support (GS) asset, they had free reign throughout the sector. Each squad contained not only trained law-enforcement observers (in itself a critical asset) but also digital cameras for taking photos of personnel and locations for further analysis and comparisons. We learned to rely heavily on the MPs and their flexibility to confirm or deny information for us across the sector, day or night.

❑ Adding crime analysis to the ACE was critical in answering the CCIRs.

❑ One of the most flexible collectors was the military police. As a GS assets, they had free reign throughout the sector.

❑ One unique change made in Kosovo was the addition of two CID agents as liaison officers and crime experts to the ACE. These agents provided first-hand understanding of crime-scene analysis and direct access to the investigative information.

Figure 1. Lessons Learned.

> **[MNB-E]...established a system [to] downgrade relevant... information...and provide it to UNCIVPOL stations chiefs....**

The third step was increasing cooperation and information-sharing with UNCIVPOL. Without it, the analyzed CRIMINT would not get into the hands of the civil authorities for prosecution in the courts. This step began within the first month, as the 504th MP Battalion collocated MP substations with UNCIVPOL police stations, creating a closer working relationship. This effort also established a new level of trust and cooperation between the Kosovo peacekeepers and the police, who shared the responsibility of maintaining stability. Next, the MP Battalion established a weekly Police Intelligence Collections and Analysis Council (PICAC) that became the critical link between the MI analytical assets and the investigative and judicial mandate of the police. This law-enforcement forum allowed for greater cooperation in policing activities within MNB-E. Furthermore, as a primary participant, the TFF ACE used the PICAC to provide the analyzed intelligence with the support of CID agents working in the HARC. We quickly established a system by which we could downgrade relevant law-enforcement information collected by TFF assets and provide it to UNCIVPOL station chiefs for their use in law-enforcement operations throughout the sector. This weekly PICAC meeting allowed TFF and the civil police authority to coordinate joint military and police operations and to expand our collective abilities to search for known and suspected criminals.

(Continued on page 41)

U.S. DEPARTMENT OF HOMELAND SECURITY

by Bernadette Harris

On 24 January 2003, the Department of Homeland Security (DHS) officially came into existence as the 15th Executive Department of President George W. Bush's cabinet. To head the organization, Vice President Dick Chaney swore in Thomas Joseph Ridge, the former Governor of Pennsylvania, as its first Secretary.

During the swearing-in ceremony, President Bush stated that the Department of Homeland Security "…*begins a vital mission in the defense of our country*."[1] With the assumption of this mission to protect the U.S. homeland from terrorism and other ongoing threats, Secretary Ridge takes on the momentous task of pulling together an amalgam of preexisting agencies to build the internal workings of a new department. Within this task, Secretary Ridge will have to mobilize and refocus the resources of the Federal Government to work in concert with state and local governments, the private sector, and the U.S. populace to accomplish the mission of his new department.

Mission

The mission of the Department of Homeland Security will be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.[2] To ensure achievement of this mission, the DHS will perform several functions necessary to carry out this mission to detect, prepare for, protect against, respond to, and recover from terrorist attacks within the United States.

DHS Functions

These functions, twelve in all, include—

- ❑ National strategy.
- ❑ Detection.
- ❑ Preparedness.
- ❑ Prevention.
- ❑ Protection.
- ❑ Response and recovery.
- ❑ Incident management.
- ❑ Continuity of government.
- ❑ Public affairs.
- ❑ Cooperation with state and local government and private entities.
- ❑ Review of legal authorities.
- ❑ Development of legislative proposals and budget reviews.

Highlighted below are seven critical functions of interest to intelligence support personnel.

National Strategy. The function of the national strategy is to ensure that the United States is able to "detect, prepare for, prevent, protect against, and respond to and recover from terrorist threats and attacks within our borders." The DHS will coordinate this function with other executive departments, agencies, state and local governments, and private agencies.

Detection. The detection function will coordinate efforts of federal, state, and local agencies, as well as private agencies as appropriate for prioritizing the collection and analysis of intelligence within the nation relating to threats of terrorism and terrorist activities.

Preparedness.The preparedness function will coordinate national efforts of the federal, state, and local governments and private agencies when appropriate to prepare for and diminish the effects of terrorist threats or attacks within the United States.

Prevention. The prevention function will coordinate efforts of the federal, state, and local governments and private agencies when appropriate to prevent terrorist attacks within the country.

White House photo by Paul Morse.

President George W. Bush watches Vice President Dick Cheney swear in Tom Ridge as the Secretary of the Department of Homeland Security in the Cross Hall on 24 January 2003.

Protection. The protection function will coordinate efforts of the federal, state, and local governments as well as private agencies when appropriate to protect our critical infrastructure from the consequences of terrorist attacks.

Response and Recovery. The response and recovery function will coordinate efforts of the federal, state, and local governments and private agencies to respond to and assist in the recovery from terrorist threats or attacks within the United States.

Incident Management. The incident management function will coordinate the domestic response efforts of all departments and agencies in the event of an imminent terrorist threat as well as during and in the immediate aftermath of a terrorist attack in the nation.

The DHS Secretary is the principal point of contact for the President with respect to coordination of such efforts.[3]

Organization

In order to stand up the Department of Homeland Security, many of the existing government agencies will transfer under the newly formed department and undergo a reorganization. As of 1 March 2003, some of the essential agencies scheduled to transfer to the DHS are—

- ❑ Federal Bureau of Investigation (FBI) National Infrastructure Protection Center (NIPC), National Communications System, Department of Commerce Critical Infrastructure Assurance Office, National Infrastructure Simulation and Analysis Center, Department of Energy (DOE) Energy Assurance Office, and the Federal Computer-Incident Response Center of the General Services Administration.
- ❑ U.S. Coast Guard.
- ❑ U.S. Customs Service, Transportation Security Administration, Federal Protective Service, Office of Domestic Preparedness, Federal Law Enforcement Training Center, and functions of the U.S. Immigration and Naturalization Service.
- ❑ U.S. Secret Service.
- ❑ Department of Defense (DOD) National Bio-Weapons Defense Analysis Center.
- ❑ Federal Emergency Management Agency (FEMA).

On 1 June 2003, additional agencies will finish a second wave of transfers. By 30 September 2003, the DHS organization will be complete.

Sharing Information and Intelligence

Critical to the success of Homeland Security (HLS) will be the role of sharing information and intelligence. To accomplish this, we must put aside the old ways of handling business and establish new ways of sharing information and intelligence among the Armed Forces and federal, state, and local law-enforcement agencies (LEAs). If the country implemented such a national network of sharing information and intelligence, it would help to create a common operational picture (COP). There are some regions in the country where a relationship of sharing information and intelligence already exists between the military and the LEAs; however, we need to expand and use this concept on a national level.

Intelligence Support to Homeland Defense

Intelligence support to the DHS will occur on several fronts. In the joint arena, **Joint Publication (JP) 3-26, Joint Doctrine for Homeland Security,** published under the direction of the Joint Chiefs of Staff, provides the principles and doctrine to guide the armed forces in the conduct of HLS operations in joint, multinational, and interagency environments. **JP 3-26** also describes the HLS framework, mission areas, mission sets, and related incidents and it sets forth the overarching doctrine to govern the joint activities and performance of the armed forces of the United States in joint operations.[4]

On the U.S. Army Training and Doctrine Command side of the house, TRADOC published the **Installation Commander's Force Protection (FP) Handbook**. Published in July 2002, the

White House photo by Tina Hager.

Marking the anniversary of those who fought against terrorists on Flight 93 during the terrorist attacks 11 Septenmer 2001, Governor Ridge travel to his home state for memorial services in Shanksville, Pennsylvania, on 11 September 2002.

handbook is an excellent reference that provides an additional tool for commanders to deter, defend against, and respond to FP threats. Published in a pocket-size format, the handbook serves as a quick reference for TRADOC installation commanders and their staffs and walks them through the procedural guidelines on implementing an installation FP program.[5]

Army Regulation 525-13, Military Operations: Antiterrorism, published in January 2002, prescribes policy and procedures and assigns responsibilities for the Army Antiterrorism (AT) Program. The AT program implements **DOD Directive 2000.12, DOD Antiterrorism/Force Protection (AT/FP) Program**, and **DOD Instruction 2000.16**, **DOD Antiterrorism Standards**, and provides guidance and mandatory standards for protecting Department of the Army personnel, information, and critical resources from acts of terrorism.[6]

Closer to home, Fort Huachuca's Doctrine Division is currently staffing **Special Text (ST) 2-91.2, Intelligence Support to Installation Commander's Antiterrorism Program and Force Protection (AT/FP)**. The ST establishes the initial doctrinal foundation for intelligence support to AT/FP and provides the basis for the organization and structure of AT/FP.

*See the Doctrine Corner on page 57 for further discussion of **ST 2-91.2**.*

The ST is the first of its kind and describes the processes, procedures, and techniques used to produce all-source intelligence in support of AT/FP. Each chapter offers excellent information ranging from the definition of AT/FP; commander and staff responsibilities; intelligence, surveillance, and reconnaissance (ISR) cell responsibilities; intelligence support to AT/FP operations to the AT/FP targeting process. **ST 2-91.2** gives the installation commanders information on how to finish, plan, resource, train, exercise, and execute AT/FP measures to furnish security to their installations.

In addition to the excellent information available in each chapter, several of the ST's appendixes supply useful samples of an AT/FP installation plan; indications and warnings (I&W), major Army command (MACOM), or installation AT/FP matrixes; intelligence crisis-plan checklist; and other practical information.

Conclusion

ST 2-91.2 will be available shortly; please check the doctrine website at http://doctrine.futures.hua.army.mil or https://www.futures.hua.army.mil/doctrine for an announcement of its availability. The U.S. Army Intelligence Center and Fort Huachuca Doctrine Division will continue to develop STs and field manuals (FMs) to impart guidance on mission and standards that affect MI professionals in the field.

Endnotes

[1] "Ridge Sworn In Friday as Secretary of Homeland Security" at http://www.whitehouse.gov/news/releases/2003/01/20030124-5.html.

[2] "Executive Order Establishing Office of Homeland Security" at http://www.whitehouse.gov/news/releases/2001/10/20011008-2.html.

[3] *Department of Homeland Security Reorganization Plan* (Washington, D.C.: Department of Homeland Security, 25 November 2002) at http://www.whitehouse.gov/homeland/.

[4] **Joint Publication 3-26, Joint Doctrine For Homeland Security**, Draft dated 18 December 2002 at http://www.dtic.mil/doctrine/pubstat/stat326.htm.

[5] Installation Commander's Force Protection Handbook, July 2002, at http://doctrine.army.mil/default.htm.

[6] **Army Regulation 525-13, Military Operations: Antiterrorism** (Washington, D.C.: Department of the Army, 4 January 2002).

Bernadette Harris is a doctrine writer for the Doctrine Division at the USAIC&FH. Mrs. Harris is a subject-matter expert on homeland defense and urban operations. She has earned a Master of Arts degree in Education from Boston University and a Master of Arts degree in Educational Psychology from the University of Arizona. As a civilian, she has attended and graduated from the MI Officer Transition Course and the MI Captains Career Course. Readers may contact Mrs. Harris via E-mail at bernadette.harris@hua.army.mil and telephonically at (520) 538-0978 or DSN 879-0978.

White House photo by Eric Draper.

Accompanied by Governor Ridge and White House Chief of Staff Andrew Card, President Bush visits the Homeland Security Complex in Washington, D.C., 19 September 2002.

S2 Support to the Brigade Targeting and Synchronization Meeting

by Major James D. Sisemore

After mission analysis and presentation of the operations order (OPORD), one of most important things S2s do at the brigade task force (TF) level is to furnish their input to the brigade targeting and synchronization meeting. At the brigade level, these meetings either look 24 to 72 hours into the future or support a specific event (counterreconnaissance fight, destruction of the forward detachment, etc.). The constantly changing threat on the battlefield requires these meetings to ensure the brigade's combat power remains centered on the commander's intent for the mission. The end state of a targeting meeting is the fragmentary order (FRAGO). This FRAGO is the basis on which a subordinate unit focuses its combat power to accomplish the brigade mission. This article will review several techniques that proved successful for a brigade S2 during home training and during a combat training center rotation.

In the purest form, the targeting meeting uses the methodology of Decide, Detect, Deliver, and Assess (as found in **FM 6-20-10, Tactics, Techniques, and Procedures for the Targeting Process**[1]) as its guide. It is not the targeting meeting itself, however, that makes a brigade successful. The brigade must conduct planning and coordination before the beginning of these critical meetings; no member of the targeting team can show up at this meeting unprepared and expect to contribute effectively to the unit's mission (see Figure 1 for a sample attendee list). This is especially true for the S2, who sets the conditions for the success or failure of the TF by his actions.

Preparing for a Targeting Meeting

In preparing for a targeting meeting, at a minimum, the S2 must bring the following completed items:

- □ Current enemy situation overlay.
- □ Battle damage assessment (BDA) roll-up.
- □ List of current and proposed targets.
- □ Current and proposed priority intelligence requirements (PIRs).
- □ Current reconnaissance and surveillance (R&S) overlay.
- □ List of current collection assets.
- □ Other products.

Current enemy situation overlay. (This can be the current enemy situation overlay from the S3/S2 tracking board.) Little work should be necessary on this product if the assistant S2 or S2 noncommissioned officer in charge (NCOIC) maintains and corrects it. Developing a second current situation template for the meeting would be a waste of valuable time and personnel.

BDA roll-up. The BDA roll-up helps to review what threat forces have been destroyed to date and what we project is still in the brigade's area of operations (AO). This should be the current roll-up from the S3/S2 tracking board. Combining the BDA chart with a line-and-block chart of the expected threat force is useful in displaying the enemy capability in an understandable picture. This chart will give you (the S2) something to use as a reference when briefing the commander and staff (see Figure 2 for a combined BDA/enemy line-and-block chart used during a Joint Readiness Training Center (JRTC) rotation to display the Cortinian Liberation Front (CLF) forces).

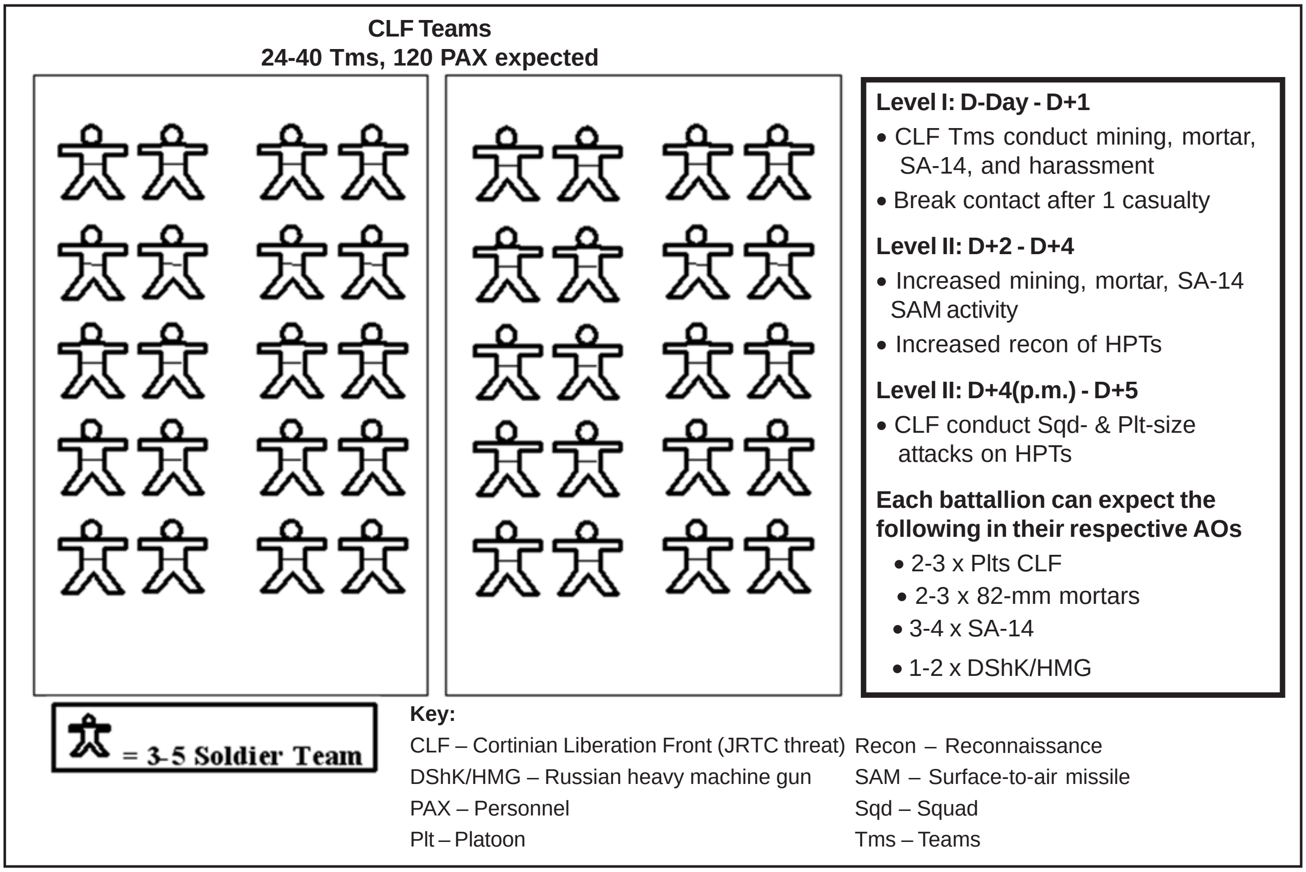
List of current and proposed targets. The brigade established the

- Brigade Executive Officer (XO) (serves as the arbitrator and keeps the meeting on track)
- Brigade S3
- Brigade Fire Support Officer (runs the meeting with the S3)
- Brigade S2
- Brigade Fire Support Coordinator
- Brigade S3 Plans Officer
- Brigade Engineer Officer
- MI Direct Support (DS) Company Commander
- Brigade Aviation Liaison Officer
- Brigade S3 Air (depending on mission)
- Brigade Judge Advocate General (the brigade's rules of engagement [ROE] expert)
- Brigade Air Defense Officer/DS Company Commander
- Brigade psychological operations (PSYOPs)/Civil Affairs Officer
- Brigade Chemical Officer

Include representatives from attached elements when possible:

- Marine Ground Liaison Team Chief
- Air Force representative if the Brigade has attached close air support (CAS) assets
- Long-Range Surveillance (LRS) Detachment representative if used in brigade area of operations

Figure 1. Sample Targeting Meeting Attendees at the Brigade Task-Force Level.



Level I: D-Day - D+1

- CLF Tms conduct mining, mortar, SA-14, and harassment
- Break contact after 1 casualty

Level II: D+2 - D+4

- Increased mining, mortar, SA-14 SAM activity
- Increased recon of HPTs

Level II: D+4(p.m.) - D+5

- CLF conduct Sqd- & Plt-size attacks on HPTs

Each battalion can expect the following in their respective AOs

- 2-3 x Plts CLF
- 2-3 x 82-mm mortars
- 3-4 x SA-14
- 1-2 x DShK/HMG

Key:

CLF – Cortinian Liberation Front (JRTC threat)	Recon – Reconnaissance
DShK/HMG – Russian heavy machine gun	SAM – Surface-to-air missile
PAX – Personnel	Sqd – Squad
Plt – Platoon	Tms – Teams

Figure 2. CLF BDA Line-and-Block Chart.

current high-payoff targets (HPTs) at the previous day's targeting meeting or from the initial OPORD. The staff should coordinate the proposed high-value targets (HVTs) with the brigade fire support officer (FSO); and the S3 or executive officer (XO) should confirm them before the meeting. Then they present them to the commander and forum in the targeting meeting as the recommended HPTs for the next planning cycle. (If possible, brief the commander before the meeting to obtain his guidance and to save time. This option may not be possible due to time constraints.)

Current and proposed PIRs. The initial order establishes the PIRs, but the targeting meeting must review them as part of the process for possible updates or changes. PIRs should work with the HPTs and decision points. While the commander is responsible for establishing PIRs, normally the S2 proposes changes and updates at the targeting meeting or in a discussion with the commander and XO. As with HPTs, you save time if you present them to the commander, in at least draft form, for approval prior to the execution of the targeting meeting.

Current R&S overlay. Use the most updated R&S overlay of the TF AO in the targeting and synchronization meeting. In addition to this overlay, the Military Intelligence (MI) direct support (DS) company commander should provide an intelligence and electronic warfare (IEW) synchronization matrix for the brigade's collection assets. This matrix lists all current intelligence collectors and their coverage times. This matrix becomes critical when tracking QUICKFIX or unmanned aerial vehicle (UAV) coverage during important periods of the battle or when showing periods of down time when an MI asset is scheduled to displace to a new position. During day-to-day activities, the IEW matrix gives the commander or battle captain something to refer to when asked questions on coverage times.

List of current collection assets. In conjunction with the R&S overlay, the S2 must present an updated list of current collection assets. While the S2 and S3 may know all the current assets, this list will assist in spurring suggestions on employment or usage of assets from the audience. Additionally, they use this list to identify any new assets or assets lost since the last meeting (see Figure 3 for a sample list).

Other products. Depending on the current battle (the offense, defense, search or attack, and the wishes of the commander), bringing a modified combined obstacle overlay (MCOO), infiltration routes overlay, or a lines-of-drift and lines-of-communication overlay, as well as other products may be useful. The commander or

MI Company Assets

TRQ-32 TEAMMATE (SIGINT collector)
TLQ-17 TRAFFIC JAM (SIGINT collector/jammer)
LLVI Teams (SIGINT collector)
PPS-15 (movement classification)
Remotely monitored battlefield sensor system (REMBASS) (movement classification)
HUMINT Teams (including IPW teams)
UAV (when attached or in general support of the brigade)

Aviation Assets (not a preferred collector on point NAIs, but can provide area coverage depending on terrain)

OH-58D/Apache (used for NAI coverage; infiltration routes, etc..)
UH-60 (specific overflight NAI can be requested through the Brigade ALO; limited effectiveness)
QUICKFIX (SIGINT collector)
AC-130 (when attached)

Other Brigade Task Force Systems

AN/TPQ-36 Firefinder radar (countermortar radar)
Air Defense Artillery Teams (as part of their area ADA coverage)
Military police platoon (as part of their battle field circulation mission)
Engineer elements (as part of their overall mission)
Chemical platoon (mission dependant)
COLT team
Civil affairs teams
PSYOP teams
Convoys (when debriefed by fire support battalion S2)
Battalion scouts

Key:

ALO – Air liaison officer
COLT – Combat observation lasing team
HUMINT – Human intelligence
IPW – Interrogation, prisoner of war
LLVI – Low-level voice intercept
UAV – Unmanned aerial vehicle

Figure 3. Sample Brigade TF Collection Asset List.

XO will define the requirements if they require a change.

Targeting Meeting Execution

The targeting meeting should be a subprocess of the military decision-making process (MDMP). As stated above, members must come to the meeting ready to discuss their specialties as they affect the brigade mission. Meetings lasting more than 1.5 to 2 hours due to unprepared participants become counterproductive, and it is the brigade XO that will keep the meetings focused and moving toward the goal of a timely FRAGO to the subordinate units.

Figure 4 shows a sample agenda for targeting meetings. It is important to note that the S2 is the first briefer after the XO and does not have time to "make fixes" once the meeting begins. While the S2 briefs several products, the group will refer to the event template most often when developing the targeting synchronization matrix (TSM).

The TSM, using the approved HPTs, will drive the targeting process. The S2's role is critical in ensuring the portrayal of a correct threat picture. If the event template is not a quality product using the best threat information available, the targeting process will result in "Blue" forces "stomping through the woods" looking for an enemy that is elsewhere. Depending on the strength of your S2 section, or your own strengths, this is where you should spend most of your time preparing to ensure that what you present gives the participants the who, what, when (future), where, and why of an enemy's actions. Using the current situation template as a reference for the meeting (as many S2s do) will fail to relay what the enemy future plans may be and, more importantly, fail to give the necessary support the TF needs in the targeting process.

For an example of a TSM, see Figure 5. Usually maintained by the brigade FSO, the presentation of the TSM is normally at poster size or larger to allow the entire audience to observe it during the meeting. Once approved by the commander or XO, listing the HTPs on the TSM begins the **Decide** portion of the meeting.

A common practice is to set up a mapboard to the side of the TSM for easy reference. The brigade FSO will facilitate the meeting and, to save time, the S2 should stand to the right or left of the mapboard to indicate templated locations and the named areas of interest (NAIs) and target areas of interest (TAIs) to the audience.

Decide. At this point in the meeting, the event template will become critical. Using it as a guide, the group confirms the NAIs and TAIs (depending on the amount of the work the S2 has time to do before the meeting) or it develops them to locate HPTs. It is also during this period that the S2 defines when the NAI/TAI coverage will be active. For example, if the NAI is covering an infiltration route and the enemy moves only at night, the NAI should be active in periods of darkness. If the NAI or TAI will confirm the location of a templated command and control (C2) node, it should remain active until the node moves.

The basis of the period of coverage is not only on the target but also on availability of the collection assets. If a supporting aviation battalion is to cover a given point NAI/TAI, it cannot maintain 24-hour coverage due to other requirements and to the capabilities of the aircraft. If an air defense artillery (ADA) Stinger team is to cover an NAI on a known aircraft-ingress route, it would be able to provide 24-hour coverage as part of its

Brigade XO	- Roll Call - Focus of meeting (time period or event covered)
Brigade S2	- Current enemy situation - BDA of attacked targets - Status of R&S plan (losses/moves of assets) - Probable COA of enemy for time period (verbal) - Proposed HPT for meeting - Event template for time period (most critical item of the meeting; used to focus Blue plan) - Proposed changes to PIRs
Brigade S3	- Review of commander's intent/mission statement and current FRAGO in effect - Review changes to task organization down to battalion level (will effect collection planning) - Review of current operations - Status of available forces - Plans for future operations (outside period covered)
Brigade FSO	- Status of indirect assets - Review of current TSM (from the previous meeting or from OPORD) - Present proposed TSM of period of meeting. Proposed HPT are listed as the Decide phase of the targeting process.
All Participants	With the XO as lead, the meeting goes through the crosswalk of Decide, Detect, Deliver, and Assess using the listed HPTs, or new HPTs developed by the group (and approved by the Commander or XO. The Brigade FSO or targeting warrant officer acts as recorder on TSM

Key:

BDA – Battle damage assessment	OPORD – Operations order
COA – Course of action	PIRs – Priority intelligence requirements
FSO – Fire support officer	R&S – Reconnaissance and surveillance
HVT – High-value target	

Figure 4. Sample Brigade Task Force Targeting Meeting Agenda.

combat mission. Planners must include this aspect when deciding what assets to task for coverage of specific NAIs or TAIs.

The S3 makes decisions and renders guidance for the Detect and Deliver phases of the targeting process. While the S2 remains the subject matter expert (SME) on the threat force, the S3 has the final tasking authority on coverage assets with input from the group.

Detect. In the Detect phase, the staff determines the asset tasked to cover an NAI or TAI and support locating an HTP. Depending on the mission, and the task-organization of subordinate units, the number of NAIs and TAIs assigned to a given collector must be supportable within its capabilities.

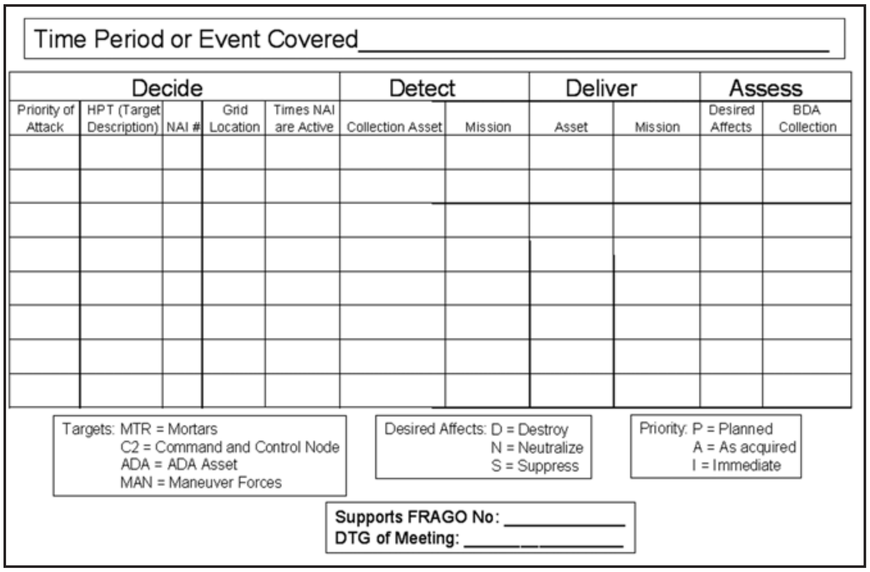
A full-strength scout platoon can cover only three point NAIs or TAIs at a time; after 24 hours, that coverage degrades due to fatigue. At the brigade level, assigning three NAIs for coverage by a battalion scout platoon robs that battalion of its organic trained surveillance assets. To better manage taskings, if three point NAIs or TAIs need coverage in a battalion sector, assign the NAIs or TAI to the battalion and let the battalion's S3 and S2 determine the best coverage.

If the brigade templates an enemy surface-to-air missile (SAM) team on every hilltop in a battalion's AO and then assigns an NAI to each hill, the number of NAIs will result in ignoring many NAIs due to the limits of time and resources. The brigade S2 must use his best guess based on the current situation to template only those areas with the greatest criticality or highest probability of success. In this case, task the brigade's organic air defense officer to validate the enemy ADA template or recommend changes to the template. This concept of "reverse IPB" (intelligence processing of the battlespace) is an excellent way to get assistance from an SME when developing an event template.

The final check on whether one has over-tasked a subordinate element in the targeting process is to total the number of NAIs or TAIs assigned to each subordinate unit at the end of the meeting. The brigade S3 or XO using his experience can determine if this is a manageable number and decide if a reallocation of coverage is necessary.

Deliver. In the Deliver Phase of the targeting process, the asset tasked to find an enemy element (Detect) may also be the tasked Deliver asset. This is true for most maneuver elements when tasked to cover NAIs and TAIs. If several "hits" from a signals intelligence (SIGINT) collector confirm an NAI or TAI for a templated C2 node, the brigade must task a ground force or indirect fire asset with a "be prepared" mission to destroy that C2 node. Assigning a mission to each subordinate unit on the TSM for the Detect and Deliver phases will assist the S3 plans officer, who will write the FRAGO for dissemination at the end of the meeting.

Part of the mission tasking must include requirements for negative reports. Sending a report to the brigade of "negative contact at NAI B12" will further assist in developing an accurate threat picture. If a maneuver element reports a hill as clear of the enemy after the S2 templated an enemy ADA asset there, that information must make it back to the brigade S2 so he can adjust the event template for the next targeting



Time Period or Event Covered ________________________________

Decide					Detect		Deliver		Assess	
Priority of Attack	HPT (Target Description)	NAI #	Grid Location	Times NAI are Active	Collection Asset	Mission	Asset	Mission	Desired Affects	BDA Collection

Targets: MTR = Mortars
C2 = Command and Control Node
ADA = ADA Asset
MAN = Maneuver Forces

Desired Affects: D = Destroy
N = Neutralize
S = Suppress

Priority: P = Planned
A = As acquired
I = Immediate

Supports FRAGO No: ____________
DTG of Meeting: ________________

Figure 5. Sample Targeting Synchronization Matrix.

meeting. This step is the one most often lost in the execution of daily missions. Continuous reporting is equally important in determining accurate BDA.

Assess. The Assess phase of the process revolves around the BDA of the located target. If an AN/TPQ-36 Firefinder weapons-locating system detects a mortar position, and the brigade tasks the DS artillery battalion (as the Deliver asset) to carry out counterbattery fire, it must determine the BDA by some method. Either the brigade must task a ground element to move into that area and look for the remains of the mortar team, or the TF can wait and see if any additional mortar attacks originate from that area (not the preferred option). The BDA for a target is often the hardest part of the targeting process, especially if direct maneuver forces were not the Deliver asset. Normally, the S2 is the officer tasked with tallying the enemy BDA. It is important for the Deliver asset (no matter what element that is) to report to the S2 the results of his direct action. If the maneuver force destroyed the enemy element, a tally of what was destroyed needs to reach the brigade. If they found nothing or if they observed a mortar team but it was able to egress from the area without casualties, they must report this as well. Every piece is necessary to paint an accurate threat picture for the brigade during the next targeting cycle.

Targeting Meeting Products. For the brigade S2, the primary products from the targeting meeting for dissemination are updated or revalidated PIRs, an updated collection plan, and approved HPTs. When the brigade disseminates the FRAGO, the brigade S2 should also disseminate an updated event template. The revised event template is often the piece lost or not included in dissemination.

These four items, when disseminated, will synchronize the intelligence effort in the TF and allow its S2s to talk from “one sheet of music.” This circulation of products gives the subordinate S2s an updated brigade picture as well as something to further refine during their targeting meeting preparations.

Conclusion

The use of the targeting meeting to synchronize and focus the combat power of a brigade task force after the initial OPORD is an important element in mission success. The S2 has a crucial staff role in this effort. The S2 must develop and present an integrated threat picture for the targeting team since this picture is what the TF uses to make decisions that result in its success or failure. While S2s are responsible for a variety of tasks within the task force, support to the targeting meeting is the highest payoff day-to-day action they perform.

Endnote

1. **FM 6-20-10, Targeting, Tactics, Techniques, and Procedures for the Targeting Process** (Washington, D.C.: Department of the Army, 8 May 1996).

References

FM 34-8-1, Intelligence Officer Handbook, “Appendix F, Targeting” (Washington, D.C.: Department of the Army, 1 May 1998).

Pritchett, Colonel Scott and Lieutenant Colonel Steve Hawley, “Synchronizing the Brigade Combat Team at the JRTC,” ***CTC Quarterly Bulletin****, Number 00-03*, March 2000,

Barefoot, Major Wayne, “Keys to S2 Success at JRTC,” ***Military Intelligence***, Volume 24, Number 1, January-March 1998.

“Search and Attack! Tactics, Techniques, and Procedure, Appendix A, Example Targeting Meeting Agenda,” ***CALL Newsletter,*** Volume 97, Number 8, August 1997.

Peterson, Jay and Rob Haycock, “Targeting the Enemy,” **CTC Quarterly Bulletin**, Volume 99, Number 3, January 1999.

“The Targeting Process,” **CTC Quarterly Bulletin**, Volume 97, Number 1, October 1997.

Major Jim Sisemore is currently working on a Master of Military Arts and Sciences degree at Fort Leavenworth, Kansas, under the School of Military Arts and Science (SAMS). In his last assignment, he served as Chief, Joint Assignments in the U.S. Total Army Personnel Command. He has served as a Battalion S2, Brigade S2, and MI DS Company Commander at Fort Drum, New York. He holds a Bachelor of Arts degree in History and a Master of Arts degree in Defense and Strategic Studies from Southwest Missouri State University. Readers can contact the author via E-mail at james.sisemore @us.army.mil.

Taking the Mystery Out of the Brigade Targeting Process: The Rakkasan Targeting Process[1]

Reprinted with permission from the Center for Army Lessons Learned from "Targeting the RAKKASAN Way: A Complete Guide on the Brigade-Level Targeting Process," CALL Newsletter Number 02-3, by Lieutenant Colonel Patrick J. Sweeney, Chief Warrant Officer Two Chris Atkinson, and Major Dennis Yates.

It is 12 hours after a brigade combat team's (BCT's) air assault to seize a flight landing strip (FLS), and the brigade commander is pondering what has turned into a frustrating experience. What seemed like a flawless operation has become a nightmare for the commander and his staff.

At first light, the engineers, who had begun clearing and repairing the FLS, received a heavy mortar attack and sustained numerous casualties and the loss of critical equipment. Other engineers had ventured out to treat the wounded and to continue clearing the FLS and they, too, came under mortar attack. The infantry battalion commander responsible for clearing and opening the FLS reported to the brigade commander that he would not be able to accomplish his mission. He reported that the enemy seemed to have eyes all around the FLS, that every time his clearing force attempted to move, mortars would hit it. He requested that the artillery shoot a smoke mission, and asked for a smoke platoon to lend a hand. The brigade commander wondered why his staff hadn't planned for this contingency.

Immediately following the infantry battalion commander's report, the battalion commander responsible for the outer ring security fight reported that the main supply routes had been mined during the night, thus completely stopping all movement in the brigade's area of operations. He reported numerous vehicles lost in minefields and mortar rounds landing on friendly convoys. As if this weren't enough, he also reported that civilians had shut down the landing zone designated to receive critical supplies. In response, the battalion commander requested civil affairs teams to assist with the civilians.

All the brigade commander could do was shake his head and ask himself why his combat power is so diffused. The brigade executive officer mumbles something about not having the time to properly complete the targeting process, which he feels is solely a fire support responsibility.

The vignette above highlights the importance of the targeting process in focusing and synchronizing combat operations. The maneuver commander uses the targeting process to focus all of his collection and delivery assets (battlefield operating systems [BOSs]) to attack enemy targets that he decides are critical to the success of the operation. The targeting process also allows the commander to visualize the enemy's capabilities, functions, and intent 24, 48, and 72 hours in advance, thereby focusing his resources to attack crucial enemy functions and to set the conditions for success in subsequent fights. Extending the targeting process into the future allows maneuver commanders to anticipate future operations. In turn, this allows them to prepare orders, acquire additional resources, and position assets to accomplish upcoming missions, such as attacks on critical enemy functions. The maneuver commander's operations then become proactive, rather than reactive, allowing him to seize the initiative. In summary, the targeting process provides the commander the means to seize, exploit, and maintain the initiative by focusing combat power and all BOSs, in both time and space, on critical enemy functions, limiting the enemy commander's ability to act.

The targeting process has four phases. They are **Decide, Detect, Deliver,** and **Assess.**[2]

In the **Decide** phase, the maneuver commander determines which enemy functions and capabilities he must attack and specifies the effects (delay, divert, disrupt, limit, destroy, and damage) that are essential to ensure success. This is the most important phase of the process, because it serves to focus the BCT's operations on attacking those critical enemy capabilities that will set the conditions to accomplish the mission.

In the **Detect** phase, the staff allocates resources to locate and track those critical targets selected by the commander in the **Decide** phase. Redundancy in detection assets is important. Also, the staff should task a given detection asset for a specific period of time, based on the brigade S2's analysis of when the target will arrive on the battlefield.

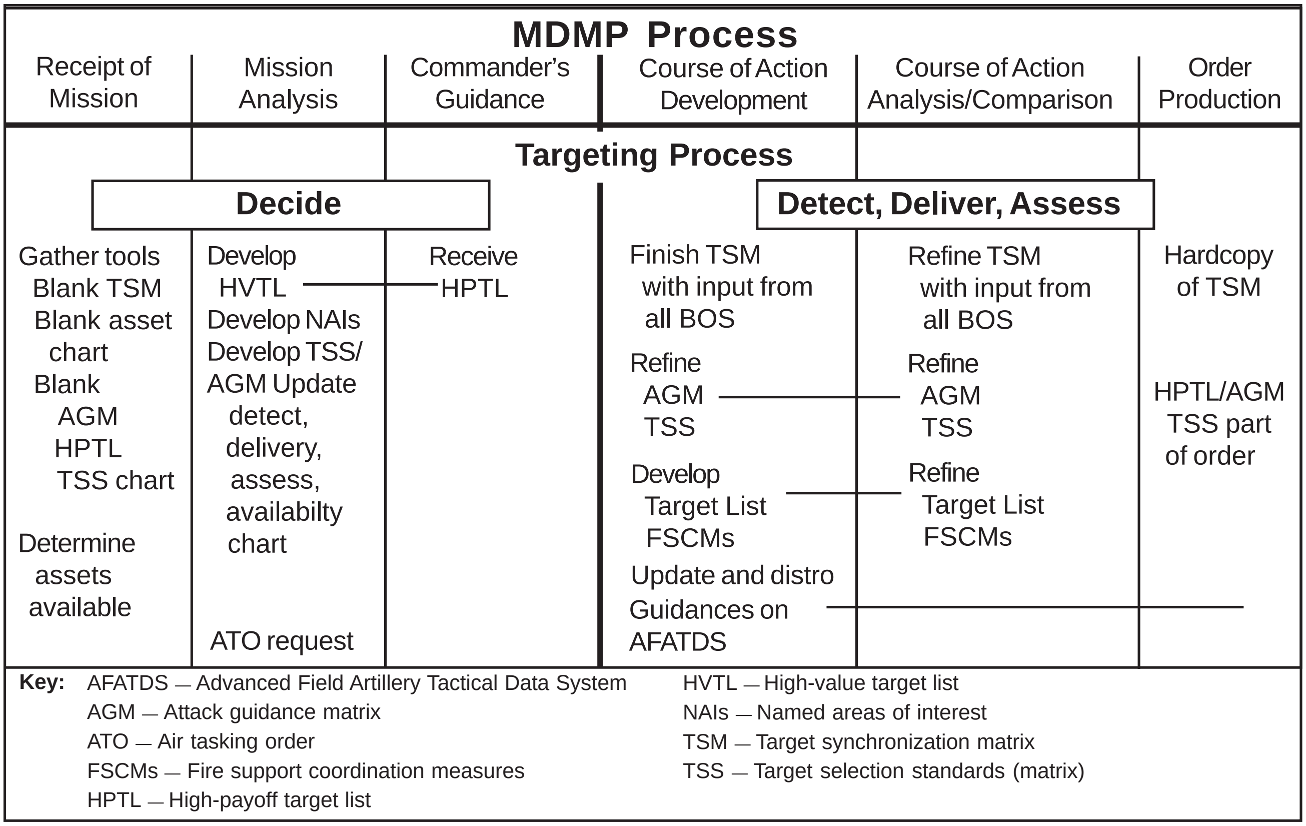
In the **Deliver** phase, the staff conducts analysis and determines which asset can best attack a given target to achieve the results specified by the commander. It is important to remember that attack assets can be both lethal and nonlethal. For instance, if one were to target the local civilian population for the purpose of obtaining their cooperation, then it might be correct to assign a civil affairs team to "engage" the local mayor. The staff must ensure that it allocates redundant systems to attack the target and that at least one of these systems is not weather-dependent.

Assess is the fourth phase of the targeting process. For each critical target for which the commander must have a damage assessment to make a future decision, the staff must allocate a resource to collect this information; these resources will assess either actual battle damage or the capacity of the enemy function to accomplish its mission. The staff must specifically task each resource specifying when it must make an assessment and have systems in place to receive, process, and analyze this information. For example, if the brigade commander wants the enemy's ZSU-23/4 antiaircraft gun destroyed before authorizing an air assault, the staff would task the attack aviation battalion to assess after it has located and engaged this target. After the engagement, the attack aviation battalion would fly the gun-camera tapes to the brigade tactical operations center (TOC) where the brigade commander can then use them to determine whether the conditions have been met for the air assault. The brigade staff must remember that not all targets require assessment after attacks. Only those high-payoff targets (HPTs) on which the commander needs to make future decisions need allocated resources for assessment. The commander should clearly identify which HPT he needs assessed in guidance to his staff.

Integrating Targeting Into the Military Decisionmaking Process

How do you integrate the targeting process into the military decision-making process (MDMP)?[3] The targeting process begins when the brigade receives the first warning order from the division. The brigade S2 and the brigade targeting officer meet to conduct initial mission analysis and to evaluate, identify, and list the enemy's high-value targets (HVTs) for the upcoming operation. HVTs are capabilities or functions that provide the enemy commander a distinct advantage or which are crucial to his success. Once this initial list is complete, the brigade S2 and the targeting officer meet with the fire support coordinator (FSCOORD), executive officer (XO), brigade S3, and brigade fire support officer (FSO) to review it. The S2 then begins working on his reconnaissance and surveillance (R&S) plan to detect these HVTs. The brigade XO and S3 also begin to understand what the upcoming operation will have to accomplish with regard to attacking enemy capabilities. This informal targeting team meeting will help focus the staff and ensure the full integration of the targeting process with the MDMP (see Figure 1).

The brigade continuously refined the HVT list (HVTL) during subsequent warning orders and after receipt of the division order. During formal mission analysis, the staff


MDMP Process

Receipt of Mission	Mission Analysis	Commander's Guidance	Course of Action Development	Course of Action Analysis/Comparison	Order Production
		Targeting Process			
Decide			Detect, Deliver, Assess		
Gather tools Blank TSM Blank asset chart Blank AGM HPTL TSS chart Determine assets available	Develop HVTL Develop NAIs Develop TSS/ AGM Update detect, delivery, assess, availabilty chart ATO request	Receive HPTL	Finish TSM with input from all BOS Refine AGM TSS Develop Target List FSCMs Update and distro Guidances on AFATDS	Refine TSM with input from all BOS Refine AGM TSS Refine Target List FSCMs	Hardcopy of TSM HPTL/AGM TSS part of order

Key:
AFATDS — Advanced Field Artillery Tactical Data System
AGM — Attack guidance matrix
ATO — Air tasking order
FSCMs — Fire support coordination measures
HPTL — High-payoff target list
HVTL — High-value target list
NAIs — Named areas of interest
TSM — Target synchronization matrix
TSS — Target selection standards (matrix)

Figure 1. Integration of the Targeting Process into the MDMP.

refines the HVTL, and the brigade S2 and targeting officer nominate critical targets to become HPTs for the commander's approval during the mission analysis brief. During or after this brief, the commander must give his guidance regarding the enemy functions (HVTs) on which he wants to focus his attack resources and the effects (delay, disrupt, limit, destroy, divert, damage) that he would like to achieve for each function. The commander's guidance for HVTs is the most critical input into the targeting process because it provides focus to the process and influences the development of courses of action (COAs). The HVTs that the commander selects then become HPTs. A target is considered an HPT if the commander deems that the particular enemy function or capability must be acquired and successfully attacked for the friendly mission to succeed.

The development of the HPT list (HPTL) provides focus and sets priorities. It assists the brigade S2 in the development of his intelligence collection plan. The S2 should develop recommended priority intelligence requirements (PIRs) to determine when and where on the battlefield the BCT team will see the HPTs. The targeting officer begins filling out the target synchronization matrix (TSM)[4], the target selection standards (TSS) matrix, and the attack guidance matrix (AGM), and starts preparing for COA development.

Next, the brigade staff develops COAs to accomplish the mission and to attack the HPTs selected by the commander during the mission analysis brief. As they develop each COA, the battle staff must determine, by phase, which assets are the best to **Detect** and **Deliver** against the HPTs. The staff must be specific about what they want the reconnaissance elements to detect, so that the brigade S2 can complete their order and deploy them as soon as possible. As COA development progresses, the targeting officer and the brigade S2 ensure that the brigade S3 considers how they will detect each HPT and which delivery system will target it. This ensures that they develop the COA with consideration of detecting and attacking the HPTs, thus linking the targeting process with the MDMP. The COAs must also ensure that detection and delivery assets are in the area of operations, in position and ready to detect or deliver during the expected time that the HPT will appear on the battlefield. For instance, if the commander is concerned about enemy mortars interdicting an air assault, then the staff must develop a COA that puts a detection asset, such as an AN/TPQ-36 Firefinder radar in place early in the airflow.

Throughout COA development, the targeting officer continues to complete the TSM, TSS matrix, and AGM. The brigade S2 continues to refine his reconnaissance and surveillance plan, and the FSO starts to develop the scheme of fires. One technique to help keep the staff focused on the TSM and on targeting is to post an enlarged copy (4' x 3') of the TSM so that it is plainly visible to everyone. The targeting officer fills in the enlarged TSM as COA development progresses and keeps the S3 and XO focused on the HPTL.

COA analysis and wargaming is an important step in integrating the targeting process with the MDMP. A proper COA comparison will ensure the full incorporation of the targeting process into the MDMP. As the brigade staff prepares for wargaming, the targeting officer ensures that the enlarged TSM is visible in the front for everyone to see. In addition, the targeting officer posts a chart listing all detection and delivery assets available for the operation and the times that each system is available.[5] As the brigade staff wargames each critical event, the FSCOORD and the brigade FSO ensure that the brigade S2 identifies approximate times and locations on the battlefield that he expects the selected HPTs, allocating detection assets to each. The brigade staff must focus only on those HPTs that can influence the brigade's COA, otherwise it runs the risk of attempting to locate and attack too many HPTs. This dilutes the focus of the brigade's combat power.

This is also the time for the staff to determine the priority of the individual HPTs on the HPTL. For example, if there are two suspected mortars operating within the area of the brigade's objective, the staff will determine which of them represents the greater threat and make that a higher priority on the HPTL. They designate a primary and alternate detection asset for each HPT; if possible, they should also assign a specific time period to the asset tasked to detect the HPT to ensure its use to its maximum effect.

Once they choose the detection assets that are to detect HPTs, the S3 specifies delivery assets based on the staff input. Again, the XO, S3, FSCOORD, and FSO must ensure that they task a primary and alternate delivery asset to attack each HPT. Also, the FSCOORD and FSO must ensure that at least one of the delivery assets for each HPT is an all-weather asset. Finally, the S3 must ask if battle damage assessment (BDA) of a particular HPT is critical for the commander to make a decision. If the answer is "yes," then they must task assets to make assessments (BDAs) on the HPT. Remember, not all HPTs need BDAs. As mentioned earlier, the commander should specify HPTs requiring assessment in his guidance to the staff.

This **Detect-Deliver-Assess** process occurs for every HPT during each critical event wargamed. If the wargame does not address an HPT, the targeting officer and the FSO must ensure that the battle staff will address it before the end of the wargame on that particular event. After the wargame, the brigade FSO and the targeting officer should have a complete scheme of fires at the brigade level; a complete TSM, AGM, and TSS; and a target list for publication in both a fire support and a fragmentary order (FRAGO) and the brigade order.

Targeting Meetings—The Power of a Name

The authors strongly believe that it is time to update the name of the brigade targeting meeting. Calling it a "targeting meeting" does not fully and accurately portray the function it serves. The word "targeting" also misleads many inexperienced staffs into believing that this is solely a fire support responsibility. Nothing could be further from the truth. The targeting meeting is the process by which the brigade staff revisits the MDMP each day (mission analysis, COA development, and wargaming) to **synchronize its combat power** for the next 72 hours against enemy functions. Both the S3 and the S2 produce event templates depicting how they think friendly and enemy forces will be arrayed 24, 48, and 72 hours into the future. This allows the staff to visualize the battlefield and to develop plans to set the conditions for future success. By using the event templates and the TSM to drive the targeting meeting, the staff focuses the plan and synchronizes future combat operations to eliminate the enemy's freedom of action by attacking his HVTs. The end state of the daily targeting meeting is a FRAGO for future operations; thus, the targeting meeting accomplishes much more than a mere attack of targets by indirect systems.

In addition, when most combat arms officers hear mention of targeting, they immediately think of field artillery. They conclude that a targeting meeting must be an artillery or fire support meeting. This parochialism prevents many maneuver commanders from taking ownership of this critical function, choosing instead to delegate it to the fire supporters.

Given the reasons stated above, the authors propose the renaming of the targeting meeting to "**Combat Power Synchronization Meeting**" (**CPSM**). This title better captures the scope and the important functions that this meeting achieves; it helps ensure that maneuver commanders and staffs take ownership of it.

Preparing for the Meeting

The brigade targeting officer, in coordination with the S2, develops a suggested HPTL for 48-72 hours into the future. The basis of the HPTL is enemy capabilities and the staff's estimate of the enemy's intent. The targeting officer uses the suggested list to prepare the first column of the targeting synchronization matrix for this period.[6] After coordinating with the direct support (DS) battalion S3, the targeting officer updates, as needed, the AGM and TSS for each time period: 0-24 hours out, 24-48 hours out, and 48-72 hours out. The TSM time period should cover 0001-2400 Zulu, thus corresponding to the times used in the air tasking order (ATO). Next, the targeting officer annotates the margin of the TSM with the critical friendly maneuver events that will occur during the period. This keeps the staff focused on critical friendly maneuver events as they complete the TSM. The targeting officer updates the lists showing which detection and delivery assets will be available for each time period covered, based on input from the staff elements.[7] It is very important that these lists be large enough that all participants can read them during the meeting. Finally, the targeting officer

Unite: 3 BDE				Effective: 160600Z - 170559Z			Phase: I			As of: 171500ZAUG01	
Decide				Detect			Deliver			Assess	
PRI	Target Description	Location	NAI	Asset	Time PD	When (I, A, P)	Asset	Time PD	Effects (D, N, S)	Asset	Time PD
1	RDS-70	DR486534	14	BRC, ATK, AVN	1200 1400	A	ATK, AVN, NSFS	1200 1400	D	BRC, ATK, AVN	1200 1400
2	SA-18	DR454542	16	BRC	0500 2200	A	105, BRC	0500 2200	S	BRC	0500 2200
3	SA-18	DR456511	12	BRC	0500 2200	A	105, BRC	0500 2200	S	BRC	0500 2200
4	DShK	DR469547	15	BRC, ATK, AVN	1400 2000	A	ATK, AVN, NSFS	1400 2000	S	BRC, ATK, AVN	1400 2000
5	DShK	DR436517	10	BRC, ATK, AVN	1400 2000	A	ATK, AVN, NSFS	1400 2000	S	BRC, ATK, AVN	1400 2000
6	81 MTR	DR468515	13	Q36, LLVI, ATK, AVN	1200 2400	A	105, TLQ17, ATK, AVN	1400 2000	S	BRC	1400 2000
7	81 MTR	DR440520	11	Q36, LLVI, ATK, AVN	1200 2400	A	105, TLQ17, ATK, AVN	1400 2000	S	BRC	1400 2000
8	Civ pop	DR465460	14	TM Ville (CA Team)	0500 2300	P	CA Team	0500 2300	Influence	CA Team	0500 2300

Figure 2. Targeting Synchronization Matrix for 0-24 Hours.

produces copies of the TSM for the next 24 and 48 hours for the primary leaders.

The brigade S2 updates the collection plan, provides the targeting officer with the status of collection assets and their availability over the next 72 hours, provides BDA information, updates the enemy event template for the next 24 and 48 hours, and develops an enemy event template for 72 hours out. These enemy event templates are critical to the success of the combat power synchronization meeting because they will depict what the enemy is capable of doing, what he may attempt to do, and when and where his HVTs will appear on the battlefield. This event template helps the staff ensure it is focusing combat power against enemy functions, not just weapon systems, throughout the next 72 hours.

The S3 updates the friendly forces' concept of operations overlays for the next 24, 48, and 72 hours. These overlays help to ensure the synchronization and focus of the brigade's combat power to support maneuver operations into the future. For the 48-72 hour time period, the S3 may have to use a verbal briefing to explain the concept of operations.

Executing the Meeting

The brigade XO, with the FSCOORD serving as an advisor, chairs the combat power synchronization meeting. The targeting officer opens the meeting by taking attendance.[8] Essential players who must attend are the brigade XO, FSO, S3, S2, and FSCOORD; air liaison officer (ALO); attack aviation liaison officer; air, naval, ground, liaison, integration, and coordination officer (ANGLICO); psychological operations and civil affairs (PSYOP/CA) officer; and the Military Intelligence (MI) company commander. The XO begins by stating the purpose of the meeting, reviewing the posted agenda, and outlining time periods or events under discussion. Next, the commander provides the staff with his view on what the enemy will do in the next 24, 48, and 72 hours and, most importantly, provides his guidance and intent for future operations and which HPTs to target. The commander's guidance provides a focus for synchronizing the brigade's combat power.

Review of the Target Synchronization Matrix: 0-24 hours

Next, the S3 provides an operations update by reviewing guidance from higher echelons, the commander's intent (if the commander is not present), the combat assets available for delivery during each period, the current friendly situation, and any additional operations for the next 24 hours. The S2 provides the intelligence update by covering the current enemy situation, reviewing the current collection and R&S plans, reviewing BDA on HPTs since the last meeting, outlining the enemy's most probable COA for the remainder of the next 24-hour period using the event template, and addressing proposed changes to the PIRs. Next, the targeting officer reviews the TSM for the next 24 hours and highlights any BDA from HPTs that have been engaged.[9] In the sample TSM in Figure 2, combat operations have destroyed the RBS-70 air defense missile system, one SA-18 surface-to-air missile (SAM), and a heavy machine gun (DShK). The targeting officer has crossed them off the TSM. Now the XO adjusts the priorities for the HPTs, and the targeting officer facilitates the staff's review of the remainder of the TSM under execution to determine necessary refinements. It is very important to note that the XO must consider unit reaction time of the detection and delivery assets when approving refinements to the current TSM under execution. Otherwise, units or elements may not have sufficient reaction time to plan for, rehearse, or execute operations.

Review and Refinement of the Target Synchronization Matrix: 24-48 hours

The S3 places the friendly operations overlay for this time period on the map and briefs the friendly scheme of maneuver. The S2 annotates the enemy's event template on the map and updates the enemy commander's intent and capabilities, and the time and location that HPTs will appear on the battlefield. The targeting officer reviews the HPTs and their priority to determine if changes are necessary. Once the XO approves the HPTs and their priorities, the targeting officer facilitates a BOS crosswalk of the TSM to verify the detection, delivery, and assessment assets (if needed) for each HPT.[10] The purpose of this review is to refine the focus of the detection and delivery assets based on the successful or unsuccessful execution of the current TSM. This early review and refinement allows time for the S3 to transmit FRAGOs. This, in turn, gives units time for planning and for troop-leading procedures prior to executing detection, delivery, or assessment taskings.

Developing the Target Synchronization Matrix: 48-72 hours

After the review of the 24-48 hour TSM, the S3 briefs the projected friendly concept of operations for the 48- to 72-hour period and the S2 outlines the enemy commander's intent and likely concept of operations from his event template for this period. The targeting officer then reviews the proposed HPTs for the XO's approval. Once the HPTs have been approved, the targeting officer facilitates the BOS crosswalk to determine the best detection, delivery, and assessment assets for each HPT.[11] In the sample TSM in Appendix G, the targeting officer proposes a list of HPTs and priorities for the time period. First, the combat power synchronization group (CPSG) determines the validity of the HPTs, their priorities based on the commander's guidance, and the influence each target can have on friendly operations. Once the XO approves the HPTs and their priorities, the **Decide** phase of the targeting process has ended for this period. After prioritizing the HPTs, the targeting officer leads the staff through a crosswalk of the TSM, identifying redundant detection, delivery and, if necessary, assessment assets for each HPT on the TSM.

Next, the CPSG selects the optimal assets from the posted assets status chart (both primary and alternate)[12] based on their availability to detect the HPT. The S2 provides his best estimate of when and where he thinks the HPT will appear on the battlefield. This allows tasking of de-tection assets for specific time periods and provides a focused location (named area of interest [NAI]) to search. After the group has assigned a primary and alternate detection asset to locate each HPT, the **Detect** phase of the targeting process is complete for this time period.

The CPSG next considers and selects the best delivery asset to achieve the ***effects*** the commander has specified in his guidance and to meet any rules of engagement (ROE) constraints. The effects desired must be specific regarding percentage of damage, time, or both. For instance, the commander may want and need suppression of the SA-18 SAM—which can influence the last leg of his unit's air assault flight route for the six minutes it takes the aircraft to move beyond the weapon's effective range.[13] Thus, the TSM would task the delivery system (artillery battalion) to suppress the SA-18 SAM templated at NAI 12 from H-6 to H-Hour.

Furthermore, if the CPSG members task a delivery asset to destroy an HPT, then they must express the desired effects in percentage of destruction. For artillery, destruction effects mean 30-percent casualties or physical damage; for maneuver assets it would be 70 percent. Specifying effects and time periods for delivery assets reduces confusion and provides focus and efficiency. Again, they identify redundant assets to attack each target based on the BOS representative's input. It is imperative that at least one delivery system be all-weather for the engagement of each HPT. Once every target has a primary and alternate delivery asset, then the **Deliver** phase of the targeting process is complete for the time period.

Finally, for those HPTs on which the commander wants an assessment, the CPSG allocates assets (primary and alternate) to conduct the assessment after the attack. The group must specify the type of BDA needed for the selected HPTs. **Physical damage assessment** reports the extent of actual damage to the target; **functional damage assessment** estimates the ability of the target to perform its mission or function after attack. The CPSG must ensure that the tasked assessment asset can get the information to the commander in time for him to make his decisions. Once they have tasked to assess the HPTs identified by the commander, then the last phase of the targeting process—**Assess**—is complete.

It is important that the BOS crosswalk be a dynamic process in which the BCT considers all of its resources and uses them in a synergistic means to locate and deliver against enemy HPTs. Each BOS representative must proactively present how his specific BOS can contribute to attacking the HPT. On the other hand, each member must let the group know when his elements are getting overtasked. The brigade XO and the FSCOORD must pay particular attention to the attack aviation assets because these assets tend to get overtasked for detection and delivery on HPTs, distracting them from other missions. The BOS crosswalk continues for each HPT until the matrix is complete.

The CPSG must learn to feel comfortable planning when limited information is available, such as when completing the TSM 72 hours out. The brigade can set conditions (e.g., position assets, get ammunition, issue FRAGOs) **now** for the future successful engagement of enemy HPTs. The group must remember that it will refine this TSM at the 48- and 24-hour review. Also, it is critical that the CPSG identifies Air Force assets needed 72 hours out so that the request can be in the ATO cycle in a timely manner.

Actions After the Meeting

After the CPSM, the brigade XO, FSCOORD, S3, and S2 brief the results to the brigade commander for his approval. After he approves the TSMs, the S3 immediately issues a FRAGO. If the S3 does not transmit this FRAGO to all units, then the CPSM was for naught. The quick issuing of a FRAGO addressing changes to the next day's taskings (24-48 hours) and new taskings for the 48- to 72-hour period provides units time to plan and rehearse for these upcoming missions. The brigade FSO immediately updates the target list and commander's guidance in the Advanced Field Artillery Tactical Data System (AFATDS), sends the TSM to the DS field artillery battalion S3, and ensures that the brigade S3-Air submits the close-air support (CAS) nominations to the division. The brigade S2 updates the collection and R&S plan and sends changes to the brigade reconnaissance company commander.

Conclusion

In summary, the combat power synchronization meeting is critical for focusing and synchronizing all brigade's combat power against the enemy's critical functions. This meeting allows the staff to seize the initiative by setting the conditions for the next day's engagements and limiting the enemy commander's options.

The RAKKASAN combat power synchronization procedures outlined above, and the tools in the appendixes listed in the endnotes, will help units efficiently focus and synchronize their combat power. RAKKASAN, TIME ON TARGET!

Endnotes

1. This article shares tactics, techniques, and procedures (TTPs) for targeting refined and successfully used by the staff of the 3d Brigade Combat Team (RAKKASANS), 101st Airborne Division (Air Assault), during a rotation at the Joint Readiness Training Center. It contains information on how to integrate the targeting process into the MDMP, how to conduct daily targeting meetings, and tools for organizing and synchronizing targeting data.

2. Appendix A, The Targeting Process, at http://call.army.mil/products/newsltrs/02-3/02-3appa.htm.

3. Appendix B, Integration of the Targeting Process Into the MDMP, at http://call.army.mil/products/newsltrs/02-3/02-3appb.htm.

4. Appendix C, Targeting Synchronization Matrix, at http://call.army.mil/products/newsltrs/02-3/02-3appc.htm.

5. Appendix D, Assets Status Chart, at http://call.army.mil/products/newsltrs/02-3/02-3appd.htm.

6. Appendix G, Targeting Synchronization Matrix: 48-72 Hours, at http://call.army.mil/products/newsltrs/02-3/02-3appg.htm.

7. Appendix D, Assets Status Chart.

8. Appendix H, Combat Power Synchronization Meeting, at http://call.army.mil/products/newsltrs/02-3/02-3apph.htm.

9. Appendix E, Targeting Synchronization Matrix: 0-24 Hours, at http://call.army.mil/products/newsltrs/02-3/02-3appe.htm.

10. Appendix F, Targeting Synchronization Matrix: 24-48 Hours, at http://call.army.mil/products/newsltrs/02-3/02-3appf.htm.

11. Appendix G, Targeting Synchronization Matrix.

12. Appendix D, Assets Status Chart.

13. Appendix G, Targeting Synchronization Matrix.

Intelligence Support

(Continued from page 26)

Through the working relationships established at the substations and the PICAC, we quickly established procedures by which we worked together to reduce crime in the sector. For example, when the police were searching for or investigating a particular individual, they would provide the individual's name to the ACE through the MP UNCIVPOL liaison or CID agent. The ACE would then check that individual against our databases, declassify relevant information, and provide it to UNCIVPOL at the PICAC, or directly if the information was time-sensitive. On one particular occasion, an UNCIVPOL station commander brought to the PICAC the name of an individual who was wanted for attempted murder. The station commander did not have a picture of the individual and, therefore, was unable to identify him; within an hour, the ACE provided a photograph of the criminal from our databases to the station commander, who instantly recognized him. The criminal was arrested the following day and is currently serving his sentence. This is just one example of many where the PICAC forum created conditions by which shared information facilitated justice. This type of cooperation also increases our collective ability to identify and arrest known or suspected criminals. We routinely shared information on who was wanted by our respective organizations, effectively doubling the number of people looking for that individual.

When the police are searching for a criminal, they only need to bring his picture or description and personal data to the PICAC, and all forces within MNB-E become involved in the search. In each case, the MPs immediately put out a "be on the lookout" (BOLO) bulletin for the individual and we added him to the TFF detain list, effectively focusing every soldier in MNB-E on finding the criminal. This cooperation increased arrests within MNB-E and was a factor in not only reducing crime but also supporting the success and integration of UNCIVPOL into the local community.

Conclusion

Since the events of 11 September 2001, demands on the U.S. military have increased. As the United States prepares for current and future operations in support of President George W. Bush's Global War on Terrorism, we will continue to work with our partners around the world in multinational peacekeeping operations. As a member of the United Nations, we will also work with UNCIVPOL in other countries, helping to create stability where families can live in their own homes without fear. Lessons learned from Kosovo (see Figure 1) during the 3B mission are an excellent reminder of the importance of using all available assets. Building strong working relationships with civil police, sharing information, and building trust are essential ingredients in combating the destabilizing effects of crime.

Major Jeff Jennings is currently the Executive Officer, 110th MI Battalion, 10th Mountain Division (Light). His last assignment was as Analysis and Control Element Chief, 10th Mountain Division (L), during which he deployed to Kosovo for KFOR 3B. MAJ Jennings has also served as G2 Operations Officer and 1st Brigade S2, 25th Infantry Division (L), and S2, 4-22 Infantry Battalion, 25th ID (L). Readers may contact the author via E-mail at jeffrey. jennings@us.army.mil and by telephone at DSN 772-8088.

The Case for the MI Ranger

by Captain Thomas W. Spahr

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

Few combat commanders will deny the importance of reconnaissance to the success of tactical operations. The opposing force (OPFOR) at the National Training Center (NTC) will attest that the success of any visiting unit operation depends largely on the success of the "Blue" force's (BLUFOR) division and regimental reconnaissance teams. Military Intelligence (MI) soldiers—in particular military occupational specialty 98G (Cryptologic Linguist) and MOS 96R Ground Surveillance Systems Operator) soldiers—can be an essential part of the low-level voice intercept (LLVI) and ground surveillance radar (GSR) and Improved Remotely Monitored Battlefield Sensor System (I-REMBASS) reconnaissance teams, respectively. They serve as the "eyes" and "ears" of the commander and, like other reconnaissance units (such as long-range surveillance units [LRS] and scouts), should benefit from the best training and equipment available.

Insufficient Training and Equipment

In my experience, however, these MI teams are neither properly trained nor equipped. They enter combat alongside infantry troops but they do not receive the same tactical training and equipment as infantry soldiers do. The direct support (DS) MI companies receive late-model nightvision devices and lack access to critical training such as attendance at the Ranger Course. The result is consistent failure to achieve their full potential in contributing to the combined arms fight.

I witnessed this mismatch of training and equipment during a recent rotation at the Joint Readiness Training Center (JRTC) at Fort Polk, Louisiana. Our LLVI platoon supported an airborne brigade through two weeks of operations. One mission required the brigade to cross Fort Polk on foot and seize the Shughart-Gordon urban complex from an entrenched enemy force so two LLVI teams and a scout platoon transported by helicopter into the vicinity of Shughart-Gordon. Their collective mission was to determine the whereabouts and activities of enemy forces around the town. In addition, the LLVI teams had the critical task of reporting the enemy's call for reinforcements to counterattack.

Watching the scouts and LLVI teams board helicopters, I noticed an obvious mismatch in experience, training, and tools. Both scout team leaders were staff sergeants while the LLVI team leaders were a sergeant (E-5) and a corporal. The scout team leaders were Ranger-school graduates with more than five years of practical experience in tactical units. The LLVI team leaders had less than two years of tactical experience and little-to-no patrolling training; their MOS (98G) disqualified them from attending the Ranger Course. The scout team leaders carried powerful AN/PVS-14 nightvision goggles, while the LLVI team leaders used worn-out 1980s-model AN/PVS-7As.

Despite these differences in background, training, and equipment, the infantry and MI teams shared a similar mission. They both faced the common challenge of reporting intelligence from vantage points along a constantly changing and ill-defined front line. Both were forced to maneuver close enough to the enemy to enable line-of-sight (LOS) sensors and systems (the scouts' eyes, the LLVI teams' radio sets) to work effectively. No less important, the teams had to approach and withdraw from these vantage points on foot without detection.

How Did This Happen?

How did the MI soldiers wind up in this predicament? Consider training first. LLVI soldiers are linguists who typically attend the Defense Language Institute for up to a year to acquire mastery of a language such as Arabic, Farsi, or Korean. They also go through basic and advanced individual training to learn how to use their specialized electronic eavesdropping equipment. By the time LLVI soldiers begin their first field assignments in a unit, they are often senior privates first class or specialists. Owing to an Armywide shortage of soldiers in MOS 98G, some of them quickly find themselves occupying team leader positions normally filled by noncommissioned officers (NCOs).

Next, consider the teams' equipment. LLVI teams carry AN/PRD-12 or PRD-13 radio-receiving sets. By doctrine, these radios perform voice intercept and radio direction finding over a range of five to ten kilometers. In practice, however, the PRD series rarely is effective beyond three to four kilometers, a function of geography, terrain, and the weak signals generated by many target enemy radios. The result is that to be effective, LLVI teams have to approach the enemy forces and operate closer to them than Army doctrine describes.

Despite this fact, MI companies that field LLVI teams are consistently at the bottom of allocation priority lists for patrolling equipment such as nightvision devices. LLVI teams should use the best patrolling equipment available in the Army. These MI soldiers also need outstanding training in patrolling and small-unit tactics—probably more than their infantry counterparts at the same stage in their careers.

Infantry and LRS units encourage their small-unit leaders to attend the Ranger Course. In many organizations, possession of the Ranger Tab is effectively a prerequisite to leadership. In divisions and corps, however, this training is unavailable to MI soldiers, even though they execute tactical missions of comparable complexity and risk.

Change in DA Policy Needed

In September 1994, a change in Department of the Army (DA) policy effectively barred MI soldiers—and other non-combat-arms MOS holders—from attending the Ranger Course. The exception to this policy is soldiers in 96R and 98G MOSs. Some 96R soldiers can qualify for Ranger school; also, 98G soldiers can qualify if they sign up for the Special Forces. Citing budget constraints as the primary reason for the change, the Army redefined the Ranger Course from a small-unit-leadership school to a combat-skills school reserved only for "*personnel whose mission is to engage in close-combat, direct-fire battle*" and for those in select MOSs that habitually support infantry battalions. The Army strictly limited the list of specialties that support infantry battalions, and MI was not among them. There was a strong suspicion that the real reason for the change was to deny admission to female soldiers at a time when females were greatly expanding their access to combat positions across the military.

At the present time, women are allowed to serve on LLVI teams. Based on my observations of MI units at JRTC, 98G soldiers who are members of LLVI teams serve in direct combat positions. DA should recode these positions as P1 (highest propensity for direct combat) and place them out of bounds to women. Earlier this year, the Army undertook a similar reclassification for all positions within the new reconnaissance, surveillance, and target acquisition (RSTA) squadrons in the Stryker brigades for similar reasons. Using the same logic, we should reevaluate selected positions in the division MI battalions. Once reclassification is complete, MI soldiers who fill LLVI teams should receive admittance to the Ranger Course. The Army also needs to designate LLVI team-leader slots as Ranger-coded positions, reflecting the real nature of their tactical responsibilities.

LLVI teams are not the only MI units that confront a similar tactical challenge. I-REMBASS teams composed of soldiers in MOS 96R carry remotely emplaced sensors into areas occupied, or soon to be occupied, by the enemy and they also deploy motion-detecting GSRs along likely enemy avenues of approach. The sensors provide early warning of the advance of enemy troops and vehicles. I-REMBASS and GSR sergeants have to be just as accomplished as infantry small-unit leaders in combat-related skills, including infiltration, exfiltration, and tactical evaluation of terrain. The 96R MOS is not on the list of MOSs accepted in Ranger school (although some may qualify) but a realistic assessment of the 96R's role in combat suggests that it should be.

More Than Training Changes Are Necessary

Training is a significant part of the solution for the skills and equipment mismatch between MI and infantry teams in the Army division but it cannot resolve it alone. The Army needs to funnel the best patrolling equipment, such as nightvision and ground-positioning system devices, to selected MI units no less than it does to infantry battalions. MI leaders must do a better job of—

❑ Educating infantry leaders on how MI teams work with their infantry partners on the battlefield.

❑ Explaining MI technical systems and their capabilities so that the tactical operations properly integrate the equipment. The S2 should not be the only member of the battalion or brigade staff who understands and knows how to use these teams.

❑ Integrating their training with the combat arms battalions. Among other things, the LLVI teams must train with scouts.

Given their current levels of training and equipment, our MI voice-intercept and ground-sensor teams enter tactical operations at a severe disadvantage. Many combat arms commanders will not deploy the teams forward to where they can be most effective because they think the teams will be captured or killed. That is not the MI teams' fault. In my experience, our LLVI, GSR, and I-REMBASS soldiers do a superb job with the equipment and training they have. Now it is time for the Army to provide these MI teams the schooling and gear they need to achieve their potential as full partners of the infantry on the combined arms battlefield.

My special thanks to Lieutenant Colonel Robert Whalen and Captain Michael Jeffress for their assistance with the research and writing of this article.

Commissioned through the ROTC program, Captain Tom Spahr received a Bachelor of Arts and Science degree in History from the University of Delaware. He served as the Assistant S2 of the 325th Airborne Infantry Regiment and 2-325th Battalion, and Collection and Jamming Platoon Leader, B Company, 313th MI Battalion, 82d Airborne Division. His next assignment was as the Collection Management and Dissemination Officer, 75th Ranger Regiment, where he participated in combat operations in southern Afghanistan from October to December 2001. After completion of the MI Captains Career Course, he will serve as an Assistant S2, 7th Special Forces Group at Fort Bragg, North Carolina. He is Jumpmaster and Ranger qualified. Readers may contact the author via E-mail at thomas.spahr@us.army.mil and by telephone at (706) 464-7789.

Is the Road in Georgia Too Perilous?

by Second Lieutenant
Jake M. Miller, USAF

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

As the United States continues to press on with the Global War on Terrorism, regional stability in the Caucasus should be of paramount concern. Strategically located between two major hotspots—Chechnya and the Middle East—Georgia is one of the critical countries in consolidating peace and the rule of law. However, as Georgia remains plagued by internal divisions and is a major transit point for the trafficking of arms and supplies to the surrounding conflicts, finding stability might be a difficult endeavor.

Precarious Situation

Exacerbating the situation is the fact that the Russian Federation—which has been crossing Georgia's borders in the chase of Chechen militants—is now threatening Georgia's sovereignty, thus facilitating the possibility for Georgia to fall into the "protectorate womb" of a greater foreign power. The Bush Administration has not declared its intentions to take on this role. However, given the Western interests at stake in Georgia, and the ever-expanding war on terror, increasing a military presence in Georgia must remain on Washington's conscience. Pending a move in this direction, what kind of environment awaits, and which longstanding problems would the United States inherit?

Georgia's president, Eduard A. Shevardnadze, once a first secretary of the Georgian Communist Party and later a minister of foreign affairs for the former Soviet Union, currently has plenty of troubles on his plate. He lingers consistently in single digits in popularity polls.[1] One-third of Georgia's territory remains practically outside the state's jurisdiction, with decade-old ethnic conflicts in the separatist regions of Abkhazia and South Ossetia. The Autonomous Republic of Ajaria, a monocracy located on Georgia's Black Sea coast with a predominantly Muslim population, remains in open confrontation with the Georgian Parliament and sustains close ties with Moscow. On 11 October 2002, after President Shevardnadze delivered his annual address to the parliament, five leading opposition factions walked out in protest, calling for his resignation.[2] The President, whose second and final presidential term ends in 2005, has refused repeatedly to resign.

Shevardnadze's latest problem, which has brought Georgia into the international spotlight, concerns Chechen rebels slipping across Georgia's northeast border into Russia to hide and regroup in the rugged Pankisi Gorge, home to a population of "Kists"—ethnic Chechens. Already a haven for refugees fleeing both the Russian Army and pro-Moscow Chechen paramilitaries, the gorge (see Figure 1) has become a hot spot for Moscow which has been quick to point fingers at Georgia, accusing the country of harboring terrorists, and has threatened to send the Russian Army into Georgia.[3]

In March 2002 at Shevardnadze's request, the United States began Operation TRAIN AND EQUIP, a $64 million program that sent U.S. special forces personnel to Georgia as military advisors to help create and train an elite antiterrorism (AT) force. This mission has provided an opportunity for the United States to establish a lasting foothold in the Caucasus, thereby presenting Shevardnadze with other problems:

□ Should he strive to align Tbilisi closer with Washington, providing security for his government and economic infrastructure while also proving to the world that Georgia has finally weaned itself fully from Russia?

□ Should he warm relations with Russia and the loosely organized Commonwealth of Independent States (CIS), and keep U.S. assistance to a minimum until the Chechen war finally ends?

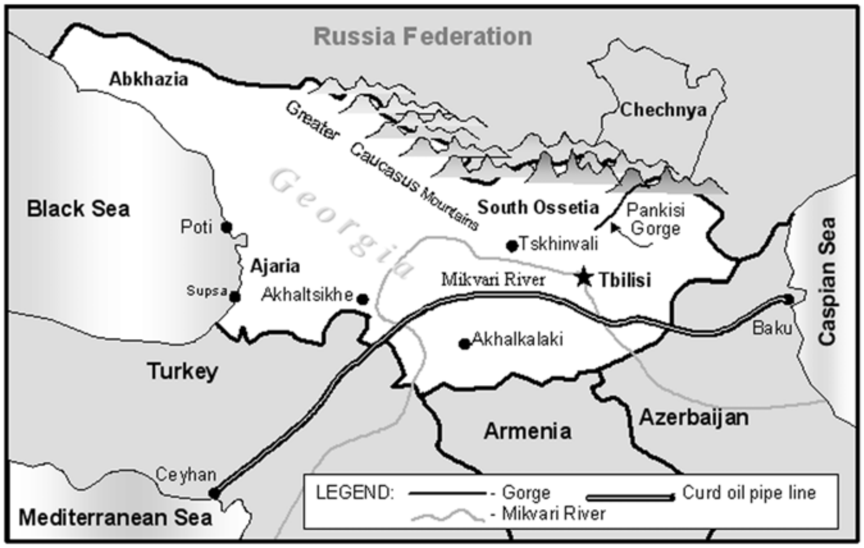


Figure 1. Map of Georgia showing the Pankisi Gorge and the BTC Oil Pipeline.

Georgia's condition is steadily worsening. With the United States already holding a stake in the existing infrastructure, including vital energy investments such as the Baku-Tbilisi-Ceyhan (BTC) oil pipeline, which began construction in September,[4] it cannot afford to allow the threat of instability to increase. However, should the United States decide to expand its military presence in Georgia, it will face rampant crime and corruption, ethnic conflicts to include a spillover war with Russia, and possible strained tensions with neighboring countries.

Crime and Corruption

Georgia's war-ravaged condition resulting from the chaotic end of the Cold War facilitated epidemic government corruption and an established presence of organized crime. Its six-decade-old economic and social system, stable throughout the Cold War, imploded with the collapse map of the Soviet regime. Then came the *matryoshka* effect—the trickling down of a desire for ethnic independence—which led to smaller conflicts such as in Abkhazia and South Ossetia. These breakaway regions, swathed in an environment of general lawlessness, provided a playground for criminals. Washington's South Caucasus policies before 11 September 2001 aimed at—

- ❑ Political stability (through third-party mediation).
- ❑ Oil (in creating an East-West corridor for Caspian pipelines).
- ❑ Democracy (achieved through the United States Agency for International Development [USAID] program).[5]

Now our policies must also extend to countering narcotics and other illicit activities that fund anti-U.S. and apocalyptic organizations.

Corruption and crime play a powerful role in countering national stability. Shevardnadze has not been able to control either. The problem is imbedded within the government apparatus, where local bosses, government officials, and police officers frequently supplement their incomes from the population by tactics like shaking down motorists for imaginary violations.[6] The Caucasus have also witnessed a rising number of kidnappings, frequently orchestrated by Chechen crime groups or guerrillas as a funding tactic.[7]

Georgia's prime location at the crossroads between the Middle East, Western Europe, and Eastern and Central Asia makes the country a popular trafficking route. Organized crime groups, spearheaded by the Russian Mafia and gangs from Chechnya, Georgia, and the Ukraine, continue to move former Soviet weaponry to militants, including weapons of mass destruction (WMDs).[8]

Ethnic Conflict

The potential for ethnic flare-up poses the most perilous threat to stability in Georgia and the greatest hindrance and seed of failure to a sustained U.S. presence. Ethnic regions fragment Georgia, including two autonomous ones, Abkhazia and South Ossetia, both created by armed conflict. A detailed study of the history of ethnic conflicts in Georgia is beyond the scope of this article. However, one should note that the entire Caucasus region has been undergoing dramatic effects by the seemingly interminable war in Chechnya, in which many ethnic Chechens are seeking independence from Russia. Significantly, religion is a major variable in this conflict, as the Chechens propagate an ideology centered around Islamic values and cultural norms in order to legitimize their cause and to attract Muslim support from around the world.[9] The Chechen war exemplifies the potential for ethnic conflicts to become never-ending bloodbaths, as recounted by Russian journalist Anna Politkovskaya.

> *Our losses are immeasurable and we let the army get out of hand and degenerate into anarchy. By allowing such a war to be fought in our own country, without any rules, not against terrorists but against those who hate their own bandits perhaps even more strongly than we do, we are the losers and the loss is irreversible.*[10]

An end to the war is not in sight as it enters its fourth year. Moscow is far from accomplishing its two goals of restoring constitutional order and suppressing the violence of Chechen insurgents.[11]

Recent tension as a result of the spillover from Chechnya has ignited between South Ossetia and Tbilisi. In early October when Shevardnadze was directing the Chechen guerrilla sweep in the Pankisi Gorge, he raised the possibility of expanding the sweep into the Tskhinvali District of South Ossetia, where Georgian officials accuse Ossetians of harboring rebels and engaging in narcotics trafficking. The Ossetians responded with a mobilization of reservist troops.[12]

As proven by the examples of Abkhazia and South Ossetia, or in Chechnya, the devolution of power along ethnic lines is not a viable solution. Once granted a taste of limited independence, nationalistic movements only continue to swell until there is a full-fledged push for secession. Other large minorities in Georgia not granted autonomy have blended more calmly into Georgian society.[13]

For example, the Georgian-Armenians who compose an ethnic majority in the Samtskhe-Javakheti region bordering Armenia have been somewhat supported by a foreign protector, the Russians, who presently maintain a military base in the Javakheti regional center of Akhalkalaki. Although the Armenians have abundant access to arms, no popular movement for secession has risen. This is largely due to the mitigation by the Armenian Government, wanting to preserve stable relations with Tbilisi.[14]

However, the situation with the Javakheti Armenians requires a cautious approach. Should Moscow oppose an increased U.S. presence in the South Caucasus, this region could see tensions erupt into violence, as predicted by political analysts for the past ten years.

The Russians also maintain two other bases in the most sensitive areas of Georgia. One in Abkhazia is believed to be a support point for Abkhazian separatists. Another base is in the southwestern region of Ajaria at the port city of Batumi, although Ajarians appear to be content with their current situation since Ajaria's prime location on the Black Sea makes it the most popular tourist destination in Georgia. Georgian officials are insisting that the Russians withdraw their bases in Akhalkalak and Batumi within three years.[15]

Given the perilous implications posed by ethnic conflict, Washington should remain wary of Russia. Undermining local governments to inspire ethnic insurrections would not be difficult for Moscow, as it retains superiority over the information war in Georgia.[16] The past ten years do not inspire confidence in the Georgians' ability to handle insurgency problems independently, and they presumably do not want help from Moscow, the very reason they requested the assistance of the United States in the Pankisi Gorge. In a stark turn-around emanating from the October CIS talks, Washington, Moscow, and Tbilisi are currently considering a trilateral agreement for policing the Pankisi Gorge.[17] The details of this agreement still remain cloudy.

The Pankisi Tinderbox

In a review of President Bush's emerging strategy, another critical element affecting the situation in Georgia is the defining of national sovereignty. In fighting the war on terrorism and countering potential security threats, the United States has declared that it must be ready to intervene preemptively, even at the risk of jeopardizing a country's sovereignty. As the world's primary influencer of global policy—the so-called definer of terrorism, brander of rogue states, self-appointed finger-pointer of good and evil in this unipolar world—it should not surprise those in Washington when other states commit to the same preemptive and intrusive policies.

The events of September 11, combined with Russia's failure to end the second war in Chechnya, provided the catalysts to moderate U.S. military assistance to Georgia in the form of Operation TRAIN AND EQUIP. The Georgian Government was concerned about war refugees from Chechnya pouring into the Pankisi Gorge, bringing in a large number of radical Wahhabis. *Wahhabism*[18]—born in Saudi Arabia and practiced by the Al Qaeda—has been known to foster an aggressive, expansionary kind of Islam, with cells present in each of the nations bordering Chechnya, many of which nurture subversive agendas.[19] The Arab-Al Qaeda influence and support began under mercenary warlord Emil Khattab, and Saudi-born Abu-Valid al Kamidi continued it after Khattab's death.[20]

Since Boris Yeltsin's Administration, the Russians have accused Georgia of harboring Chechen terrorists in the Pankisi Gorge—this sentiment stemming from Tbilisi's refusal to allow the Russians to use their bases to launch attacks into Chechnya.[21] Georgia feared being drawn into the war, one in which the Russians have provided a prime example to the world of how **not** to conduct an AT operation[22] (their concept of fighting urban warfare still being to level cities). Russia used President Bush's rhetoric against "nations harboring terrorists" as justification to launch several military strikes against Chechen rebels inside Georgia in the fall, but pulled back at pressure from Washington. Georgian critics have accused Moscow of using this action as a ruse to destabilize the country.[23]

Tensions between Russia and Georgia have eased. On 6 October, Russian President Vladimir Putin and President Shevardnadze began a series of bilateral meetings, ushering in the annual presidential summit of the CIS. Although President Shevardnadze labeled the talks a "*historic event*," the claim appears to be a premature declaration by an over-eager statesman. Even Putin's followers admitted it was too early to make assumptions as to the result of the agreements;[24] only time can tell how successful their negotiations will be. Furthermore, the war of words between Putin and Shevardnadze demonstrates the complexities of Washington's war on terrorism.

However, these eased tensions stand poised to enflame again. According to Georgian officials, their U.S.-trained counterterrorism force has detained as many as fifteen Al Qaeda operatives in the Pankisi Gorge, and several are rumored to have been extradited to the United States.[25] Moscow has been working for months to have detained Chechen rebels extradited to Russia, only to meet staunch resistance from Tbilisi.

The primary implication of an international flare-up in the gorge is the breakdown of regional stability. With Tbilisi out of Moscow's favor, ethnic conflicts that Moscow had previously supported, to include Abkhazia and South Ossetia, could erupt again.[26] As previously stated, ethnic or religious conflict poses the threat of driving Western investors away from Georgia, damaging vital energy investments such as the BTC pipeline project. This would significantly benefit Russia, which seeks dominance over Caspian oil exports and desires pipelines to run through territory under their control.

The BTC pipeline will run 1,800 kilometers from Baku, the capital of Azerbaijan, through Tbilisi, and down to the Mediterranean port of Ceyhan, Turkey. Washington feels this pipeline represents the best commercial and environmental option for Caspian Sea oil exports as it narrowly reduces the risks posed by increasing shipping in the narrow and vulnerable Bosphorus Strait. Strategically, Washington views the successful exploitation of gas and energy in this region as the key to independence and prosperity for Georgia and Azerbaijan.

Since its inception, the BTC project has been clouded in anxiety over regional instability, especially along the ten-kilometer shared border between Armenia and Azerbaijan. Too much conflict could result in the outright collapse of the endeavor.

Whatever path they take, the Georgians must have assistance. The $64 million invested by the United States in training and equipping the Georgian military is four times Georgia's annual defense budget. Their military is ill-equipped and ill-trained, with underpaid soldiers and corruption in the higher ranks.[27] The current U.S. two-year plan to transform 2,000 elite personnel into a multitasked specialized outfit may not be enough, as perhaps the best way to contain ethnic conflicts is to target what might stimulate conflict and focus on that in a proactive manner. The Georgians do not have the resources to contain these threats alone.

Into the Turmoil

Thus far during the past ten years, Russian and neighboring states have displayed a tolerant form of acceptance toward the United States' economic endeavors and minimal military presence in the Caucasus. However, the road ahead appears far more challenging, clouded in crime and corruption, ethnic conflict, and stressed political relationships.

The United States should expect to continue to face anti-U.S. sentiment by the Georgia populace, a distrust carried over from the Soviet days. A strong protector bringing stability and economic growth could make the Georgians ultimately more accepting. The same is true with Prime Minister Putin, who has aimed his foreign policy primarily at economic development. This might not have been the case five years ago when Russia was doing its best to keep the judgmental West away from Chechnya, but now Putin has internationalized the conflict with the situation in the Pankisi Gorge.

Despite the precarious situation awaiting a military increase, Washington should proceed with this route. The paramount priority of a sustained U.S. presence is to prevent further bloodshed in an already volatile region, while at the same time helping to combat terrorists and transnational criminal networks that have formed as a result of a decade of ethnic and civil unrest.

Endnotes

1. Baran, Zeyno, "The Caucasus: Ten Years after Independence," ***The Washington Quarterly***, Winter 2002, page 230.

2. "Opposition Protests President's Annual Address," accessed at www.civil.ge on 13 October 2002.

3. Myers, Steven Lee, "Russia Recasts Bog in Caucasus as War on Terror," ***The New York Times***, 5 October 2002.

4. Sutanova, Aida, "Work Begins on Baku-Ceyhan Pipeline," Associated Press, 17 September 2002.

5. Baran, page 222.

6. Fairbanks, Jr., Charles, "Disillusionment in the Caucasus and Central Asia," ***Journal of Democracy***, December, 2001, page 50.

7. Makarenko, Tamara, "The Changing Faces of Terrorism Within the Russian Federation," Cornell Caspian Consulting, accessed at www.cornellcaspian.com/pub/18_0107Terrorism.html on 5 November 2002.

8. Friedman, Robert, **Red Mafia** (New York: Little, Brown and Company, 2000), page 156.

9. Miller, Justin, "The Case Of Chechnya," **Civil Society and the Search for Justice in Russia**, edited by Christopher Marsh and Nikolas Gvosdev (New York: Lexington Books, 2002), pages139-153.

10. Politkovskaya, Anna, **A Dirty War** (London: The Harvill Press, 2001), page 85.

11. Abdullaev, Nabi, "Chechen War Goes Into Its Fourth Year," ***Moscow Times***, 24 September 2002.

12. Devdariani, Jaba, "Georgia's Turmoil Heightens Tension in Separatist Regions," accessed at www.eurasianet.org on 15 October 2002.

13. Cornell, Svante, "Autonomy as a Source of Conflict" (Baltimore, MD: The Johns Hopkins University Press, January 2002), page 270.

14. Ibid, page 274.

15. "Tbilisi Doesn't Rule Out New Base Pullout Timetable," ***Pravda***, 10 January 2001, accessed at www.pravda.ru on 10 October 2002.

16. "Russia Tries to Defeat BTC Oil Pipeline Construction, Georgian Daily Writes," Caspian News Agency, accessed at www.caspian.ru on 29 July 2002.

17. Bakhtadze, Revaz, and Jaba Devdariani, "Summit Georgia-Russia Heralds Time-Out, Not a Breakthrough," accessed at www.civil.ge on 10 October 2002.

18. *Wahhabism* is a puritanical brand of reform Islam based on Hanbali school of law in Sunnism. It focuses on removing all traces of idolatry, forbidding the veneration of saints, and severely punishing all who go against its strict interpretations of the **Koran** and *hadith*.

19. Baran, Zeyno, "United States Will Help Georgia Fight Terrorism and Strengthen Internally," accessed on Georgia Update from the Center for Strategic International Studies at www.csis.org on 2 August 2002.

20. Falkov, Michail, "Profile of Abu-Valid," accessed at www.agentura.ru/timeline/2002/nord-oct/abu-valid on 5 November 2002.

21. Ingram, Judith, "Russian Accuses Georgia of Rebel Aid," Associated Press, 14 August 2002.

22. According to the U.S. State Department report, **Patterns of Global Terrorism 2001**, *Executive Order 13224* does not identify Chechen fighters as a terrorist group.

23. Ingram, Judith, "Russia, Georgia Try to Reconcile," Associated Press, 6 October 2002.

24. Bakhtadze and Devdariani.

25. Walsh, Nick Paton, "Al Qaeda Men Handed to U.S., Says Georgia," ***The Guardian***, 23 October 2002.

(Continued on page 57)

Changes on the Horizon for 98G BNCOC

by James H. Thornby

The Basic Noncommissioned Officer Course (BNCOC) for 98G cryptologic linguists is undergoing several significant changes. All of these changes will take effect in October 2003 with the start of the fiscal year 2004 (FY 04) training year.

Course Length

The first change deals with the course length. The new course will be 7 weeks and 2 days, which equates to 37 training days. By contrast, the current course is less than 4 weeks.

Language-Based Technical Training

The second and perhaps most significant change is that the 98G linguists will experience language-based technical training as part of their BNCOC. The decision to include language training was a relatively easy one. All parties concerned understood the need for such training; putting all the pieces together to make it happen was a bit more challenging. Although the final details are not in place, the course will have three modules.

- ☐ Module A will consist of skill level 3 critical-task training that is common to all 98Gs, regardless of language. A few examples include collection management, site selection, reporting, and TROJAN operations. We estimate 9 to 10 days of training in this module.
- ☐ Module B will focus on mission-related foreign-language training. Depending on the language and the critical task list (CTL) for that language, this training will focus on military drug and counternarcotics vocabulary. The content of Module B provides the foundation of Module C. Preliminary estimates for Module B project about 10 days of intensive language training.
- ☐ Module C, estimated at 17 days, will consist of real-world traffic with "cuts" that represent transmissions the 98Gs will encounter in the performance of their actual duties. The cuts are representative of the tasks found on the CTL. Based on the cuts, the training developers will identify the vocabulary required for success. This vocabulary, which is critical to success in Module C, will be the basis for the training in Module B. Module C will also contain a situational training exercise (STX); the details for the STX are still in development. However, the student noncommissioned officer (NCO) will encounter challenging, real-world situations that require problem-solving. We are also exploring the possibility of an integrated STX with initial entry training (IET) soldiers.

Qualification Criteria of 2/2

Overall, the training will be intensive with extensive practical exercises and actual application of foreign language skills. It is imperative that soldiers start now to prepare for this training. With the start of the new training strategy, soldiers will encounter a requirement to possess a 2/2 rating on a current Defense Language Placement Test (DLPT) in their control languages. Soldiers must bring a validated DA Form 330, Language Proficiency Questionnaire, as verification of the 2/2 requirement. This requirement is necessary in that it supports both **Army Regulation 350-16**, **Total Army Language Program** (March 1998), and **AR 611-6**, **Army Linguist Management** (February 1996). Both regulations require a DLPT minimum of 2/2 for 98G linguists. In addition, given the course's relatively brief time for training the skill level 3 tasks and the complexity of language training, soldiers must be at the 2/2 level to enroll and complete the course.

Move to Goodfellow AFB

One more change to the 98G BNCOC: again effective with the FY04 training year, the 98G BNCOC will move to Goodfellow Air Force Base (AFB), Texas. The reason for the move is actually quite simple. The 344th MI Battalion at Goodfellow already does an outstanding job of training the skill level 1 soldiers. So why not copy their success and use that same formula for training the skill level 3 NCO? The cadre and all matters related to the training will still be the U.S. Army Intelligence Center NCO Academy's responsibility. We will assign or attach cadre NCOs and student NCOs as appropriate to the NCO Academy. The Intelligence Center is optimistic that the shared training environment to include equipment and facilities will prove beneficial to NCO training.

Jim Thornby is a Training Specialist with the MI Noncommissioned Officer Academy at Fort Huachuca, Arizona. Readers may contact him via E-mail at james.thornby@hua.army.mil and by telephone at (520) 533-4264 or DSN 821-4264.

Tactical Secure Wireless Networks for Intelligence Communications Support

by Michael Francis, USNR, and Troy Nolan, Ph.D.

On 28 October 2002, the National Security Agency (NSA) certified SecNet 11™, a plug-and-play Personal Communications Memory Card International Association (PCMCIA) card as a Type-1 encrypted, secure, network adapter for Secret (and below) wireless (802.11b) local-area networks (WLANs).

This card enables a computing device (laptop, tablet, etc.) with a 3.3 volts direct current (VDC) PCMCIA slot to attach to the Secure Internet Protocol Router Network (SIPRNET). The SecNet 11 card (see www.secnet11.com[1]) uses a standard AN/CYZ-10 data-transfer device to receive a key fill. Only devices with the same key, system specific identification (SSID), and network mode can connect to each other or a SecNet 11 wireless access point (AP) or bridge. These two basic configurations are shown in Figures 1 and 2.

In the peer-to-peer network configuration, analysis and control element (ACE) personnel can share classified (up to and including Secret) information directly between computing devices (see Figure 1). The effective range of the devices is a function of power and environment. Operational tests have demonstrated ranges of 100 to 300 feet (indoors) and 1,000 yards (urban canyons line-of-sight [LOS]).

The SecNet 11 antenna connection is detachable. It can support the addition of frequency converters, power amplifiers, and external antennas in order to increase the range (with more power or a directional antenna) and to use other frequencies (the standard frequency is 2.4 gigahertz [GHz], industrial, scientific, and medical band).

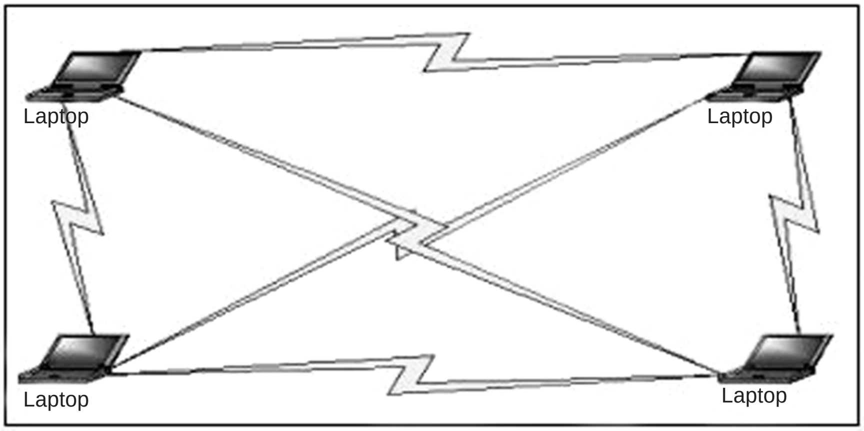


Figure 1. Ad Hoc Peer-to-Peer WLAN.

Operational exercises and fleet battle experiments will take place to demonstrate secure wireless networks at ranges of 20 to 25 miles. The actual data throughput for these configurations is typically 5 megabits per second (Mbps). Since the card is essentially an encrypted channel, from the user's perspective, the datalink function and performance are the same as any other secure fiber or cable channel. The major difference is that the user is not "tethered" to the secure network cable plant.

In the configuration shown in Figure 2, the wireless access point (WAP) is an intermediary device that connects to a SIPRNET hub or switch and provides secure wireless connectivity to laptops or other devices keyed with the same key as the WAP. This capability could serve to connect a "campus" of users in a mobile ground force tactical operations area. The addition of power amplifiers can extend the range to support forces that are within LOS. Also the AP-client configuration extends the range of the two communicating mobile nodes.

What Problems Does This Solve?

Confidentiality. One of the problems that the G2 ACE currently faces is the distribution of its

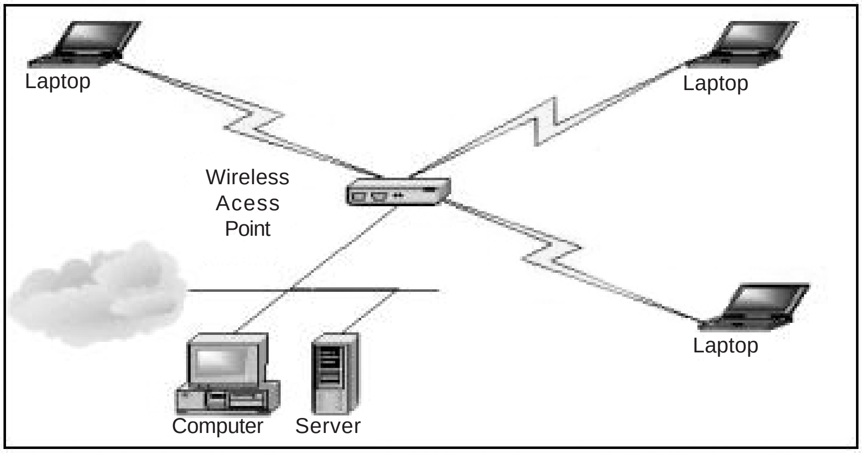
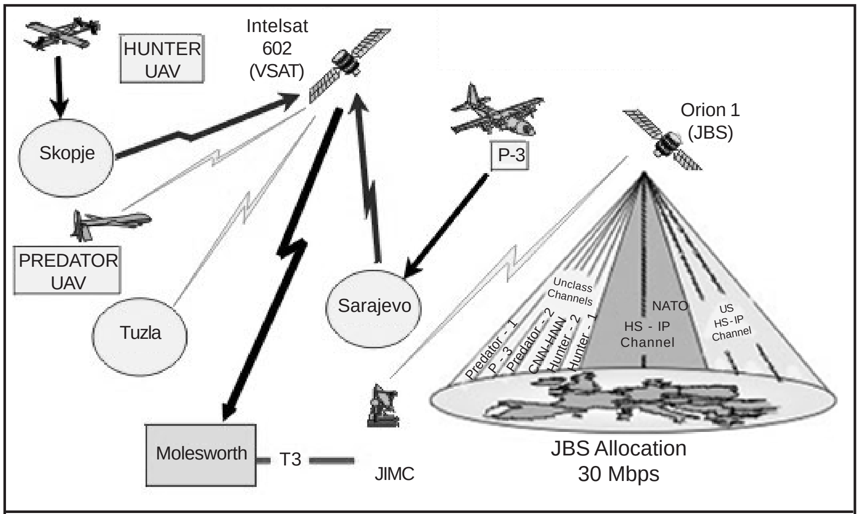


Figure 2. Wireless Access Point (WAP) WLAN.[2]



Key:

Intelsat – Intelligence satellite
JBS – Joint Broadcast Service
JIMC – Joint Intelligence Management Center
NATO – North Atlantic Treaty Organization
UAV – unmanned aerial vehicle
Unclass – Unclassified
VSAT – Very-small aperture radar

Figure 3. Architecture of the JBS-UAV Network.[3]

products to tactical operators. There is a lot of motivation to compress the sensor-to-shooter problem. The secure wireless channel enables the **secure** tactical distribution of intelligence products to "shooters" without the problematic deployment of "last mile" network (cable) infrastructure. The last mile has historically been a difficult problem, and SecNet 11 is part of the appropriate solution.

Integrity. Another problem for the G2 ACE is the actual connection to the SIPRNET. The SIPRNET is a certified and accredited network that transmits classified information. Connetions to this network require conformance to a plethora of certification and accreditation (C&A) processes. The PCMCIA card is NSA-certified as a Type-1 crypto device and, as such, the user loads the card using standard processes, procedures, and mechanisms that exist in current force organizations. In the high tempo environments of tactical operations, the unintentional cross-connect of unclassified network terminals to classified network terminals can be a problem.

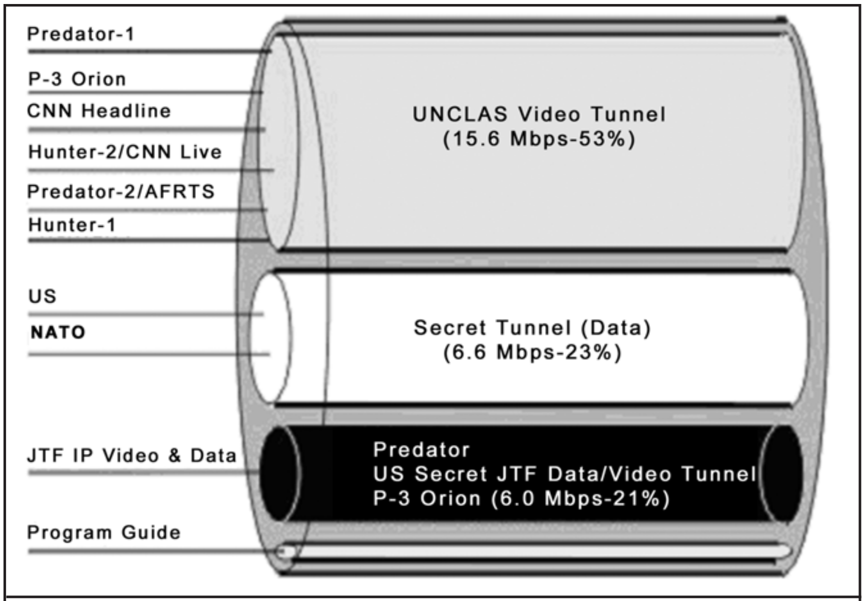
The end state effect of the SecNet 11 is that **Intelligence can move over certified and accredited secure wireless channels without the concerns associated with cable plant (secure) configurations.**

Availability. From a very practical operations mode, more than 80 percent of network problems are in the cable plant. The less cable the better, especially in the field. Deployed warfighters have been known to use the network cable for clotheslines. They have connected the SIPRNET to unclassified machines so they can "surf the net." The issues are infinite. A wireless network reduces the amount of cable and improves—

- ❑ Performance issues associated with cable faults.
- ❑ Operational security (*"Hey, where does this cable go?"*).

New Possibilities for Intelligence Architecture

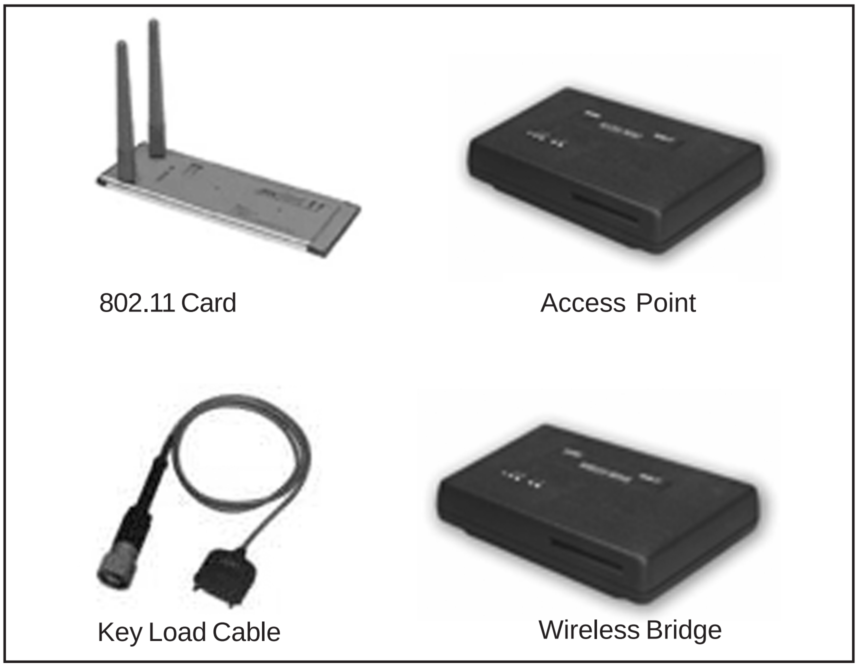
So what about sensor-to-shooter? How can we really do that? The secure wireless network enables the tactical planners to push intelligence to operating forces through a secure channel, in essentially the same format as that used at battalion level (or higher). Users can manage most of the planning products on SIPRNET with TCP/IP-based applications. Planners can push these views of the battlespace over a 5-Mbps channel to the operating forces at platoon or squad level. A 5-Mbps channel can also support voice, video, and data. Each card supports eleven channels (in



Key:

AFRTS – Armed Forces Radio and Television Service
IP – Internet Protocol
JTF – Joint Task Force

Figure 4. The Bandwidths Used by the JBS Downlink.[4]



Photos courtesy of the authors.

Figure 5. The SecNet 802.11 Hardware Components.

the continental United States), three channels (1, 6, 11) that are completely non-overlapping.

Consider the possibility of pushing live UAV imagery to tactical land components. Figure 3 provides a general view of the current architecture.

Figure 4 provides some notional distribution of required bandwidth. The Figure shows that the secure wireless channel (at 5-Mbps) is capable of pushing (at least one) live UAV video stream to tactical land components operating within LOS of an ACE distribution location.

In the article by Staff Sergeant Marvin A. Schwerzler (see endnote 3), the implied end-user is tactical intelligence. Why not push selected imagery out to the operational land components with a secure wireless channel from sensor to shooter?

Conclusions and Recommendations

As the Army better integrates Intelligence functions into combat operations, the secure wireless network capability delivers some interesting possibilities. Planned force exercises will develop operational concepts that leverage this new capability. Communicators and intelligence elements and operators have a significant capability to link the shooter with the sensor in the last mile of the tactical battlespace.

Endnotes

1. See www.secnet11.com, Harris Corporation, Melbourne, Florida. This is the source for Figure 1.

2. Ibid.

3. Schwerzler, Marvin A. Staff Sergeant, “Multiple Echelon Exploitation of UAV Imagery: Does it Work?,” ***Military Intelligence Professional Bulletin***, Volume 25, Number 4, October-December 1999, at http://138.27.35.32/mipb/.

4. Ibid.

Michael Francis is a doctoral candidate (Information Technology and Engineering) at George Mason University, Fairfax Virginia. He is a Commander in the U.S. Naval Reserve, supporting research and development in the Space and Network Warfare Programs. He is also a Senior Systems Engineer (Advanced Programs) at Harris Corporation, Chantilly, Virginia. Readers may contact him at Michael.Francis@harris.com or (703) 344-1011.

Troy Nolan, Ph.D., is an Applied Research Scientist (Advanced Programs) at Harris Corporation (Chantilly, VA.) and a subject-matter expert on wireless communications. You can reach him at tnolan@harris.com.

New *MIPB* Website Address

The ***Military Intelligence Professional Bulletin*** has a new Internet website address. The address will be http://mipb.futures.hua.army.mil and the alternate will be https://www.futures.hua.army.mil/mipb; our old address (which was http://138.27.35.32/mipb/mipbhome/welcome.htm) is no longer available although it has a hyperlink to the new address. While we transition to the new automated website, ***MIPB*** will post the issues from April-June 2000 through October-December 2002. However, readers can contact jonell.elkins@hua.army.mil or mipb@hua.army.mil about those issues in the interim period.

Global War on Terrorism:

Adaptive USAIC&FH Training in Combating Terrorism

by Stephen J. McFarland

***AR 381-10, U.S. Army Intelligence Activities**, establishes the responsibility for intelligence activities concerning U.S. persons, includes guidance on the conduct of intrusive intelligence collection techniques, and provides reporting procedures for certain federal crimes. This regulation applies to the Active Army, U.S. Army National Guard, and the U.S. Army Reserve as well as to Army intelligence components and non-intelligence components conducting intelligence activities.*

As the home of Military Intelligence (MI) training, the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH), Arizona, is prepared to step to the forefront on the war against terrorism. Considerable concern over the lack of training received by units before their rotation to Guantanamo Bay Naval Station in Cuba was the impetus behind a new training program by the 306th MI Battalion. In keeping with input from personnel currently stationed at Guantanamo Bay and the Criminal Investigation Task Force training developers in the 306th MI Battalion, the Functional Course Division created a curriculum for the immediate and long-term training of U.S. Army Reserve (USAR) and U.S. Army National Guard (ARNG) personnel called to active duty.

Deploying the Course

On 8 November 2002, a team of subject matter experts (SMEs) and training developers began planning for the mobilization and training of personnel from the 260th MI Battalion (Linguist), 300th MI Brigade (Linguist), ARNG. Personnel from this unit will arrive at Fort Huachuca on 26 January 2003 and begin training for deployment to Guantanamo Bay in support of Operation ENDURING FREEDOM. The enhanced skills and tool sets that soldiers will obtain from this training will enable them to "hit the ground running" and will facilitate a smooth transition of responsibility.

The Functional Course Division is currently developing a three-week modular course that focuses on combating terrorism. This will expand to a five-week course for the next iteration whose participants will arrive at Fort Huachuca in July 2003. Trainers can tailor modular courses to train units deploying throughout the world, and the modularity allows training developers and instructors to react quickly to short-notice requirements. This assignment-specific training will greatly enhance intelligence support for ongoing missions in the Global War on Terrorism. Additionally, USAIC&FH will serve as a focal point for incorporating lessons learned from the field regarding the Global War on Terrorism. The training will consist of familiarity with Middle Eastern cultures, the basics of Islam, the historical aspects of terrorism, an introduction to the Al Qaeda, the importance of financial tracking, and advanced interrogation and analytical techniques.

Course Structure

The Intelligence Support to Counter Terrorism Course comprises common-core training designed to familiarize students with general target knowledge and the cultural background of detainees, specific mission requirements, and an overview of operations. Instruction will then occur by military occupational specialty (MOS) during which students will receive technical training in skills tailored to the specific missions in their next units and locations.

Upon completion of the MOS-specific training, soldiers will again collectively train via a dynamic scenario, allowing them to reinforce skills previously learned and integrate their specialty training in a "real world" simulation. The scenario participants will include the role players, human intelligence (HUMINT) collectors (MOS 97E), HUMINT collection technicians (351E), Intelligence analysts (96B), and counterintelligence technicians (351B).

- ❑ **Role players** (detainees) will use a script with background information, information of "generic" intelligence value, information of specific intelligence value ("golden nuggets"), and deceptive misinformation. Role players will be fully knowledgeable of the cultural, historic, and religious geographies of the targeted countries.
- ❑ **97Es** (collectors) will interrogate the role players and try to extract as much information as possible from them with emphasis on the information requirements (IRs) that the intelligence analysts have provided. Collectors will prepare and forward the appropriate reports to the analytical cell via automated means and respond to the additional tasking and guidance provided by the analytical cell.
- ❑ **351Es** will supervise, mentor, and provide quality assurance for the 97Es. They will also act as the "release authority" for information sent to higher echelons.
- ❑ **96Bs** (analysts) develop IRs based on the priority intelligence requirements (PIRs) received from higher echelons and disseminate them to the collection cell. Analysts will receive reports from the collectors, determine the information of intelligence value, and issue appropriate re-

ports to selected customers. They will refine the IRs and direct 97Es to go after additional or more specific information of analytical value. Their activities will include link-analysis, developing association and activity matrixes, and time-event charts. They will cross-link reports with other databases and available open-source information, and develop applicable products.

- ❑ **351Bs** will supervise, advise, and maintain quality assurance for the 96Bs. In addition, they will serve as the release authority for intelligence passed to higher echelons.

This instruction will contain complex scenarios and center on the intermediate and advanced analysis techniques needed to combat current and future terrorist entities. Students will perform real-world case studies and learn force protection measures (emphasis on terrorism and other subnational threats to the force), predictive analysis, and focused threat vulnerability assessment (TVA) applications. They will learn about cyberterrorism, anti- and counterterrorism in multinational operations, collection sources available, research methodologies, variations in terrorist organizational templates, comand and control (C2) models, and insurgency and counterinsurgency operations.

Conclusion

USAIC&FH realizes that it has an important role to play in the nation's war on terrorism. We will ensure intelligence soldiers are very well prepared to collect, analyze, protect, and disseminate intelligence in a timely matter. In this endeavor, instructors are using new analytical tools, including the U.S. Army Intelligence and Security Command (INSCOM) framework for analyzing the transnational infrastructure of terrorism and software to perform data-mining in the law-enforcement database—the Investigative Information Management System (I2MS)—and the Afghan document exploitation database (Harmony). Students will learn about these tools so they will better understand how the new threat networks operate and how to best assess threat operations. Soldiers will thus be better prepared to satisfy IRs from both military and civilian agencies.

The current transformation of the Army clearly demonstrates the need to integrate our old-fashioned HUMINT capabilities with the modern high-technology systems. This will require an established cell of SMEs to develop and train effectively all levels of intelligence professionals in the skills required to combat terrorism. The Intelligence Center stands ready to ensure that future generations of intelligence specialists are ready to combat terrorism anytime, anywhere.

Sergeant First Class Stephen McFarland, U.S. Army Reserve, is an Action Officer and Instructor in the Functional Course Division, 306th MI Battalion, U.S. Army Intelligence Center and Fort Huachuca. His career has included 20 years as a Signals Intelligence Analyst at multiple echelons and 10 years of experience in the training arena. He is currently the Intelligence Center's point of contact for the 98 Career Management Field restructure, Denial and Deception, and Analysis training for the Intelligence Support to Counter Terrorism Course. Readers may contact him via E-mail at stephen.mcfarland@hua.army.mil and by telephone at (520) 538-1039 or DSN 879-1039.

Updated FDIC Websites 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 the sites under a centralized umbrella to maintain continuity and to improve the sites' appearance. Each site has a unique address in the form of **https://www.futures.hua.army.mil/<site>, http://<site>.futures.hua.army.mil,** or **http://secure.futures.hua.army.mil.**

FDIC Sites

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

Current Secure FDIC Sites (password controlled software) https://secure.futures.hua.army.mil. These sites will be active soon.

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

weather (on the https://secure.futures.hua.army.mil site)

Note: ***MIPB***'s out-of-date site available at http://huachuca-usaic.army.mil/mipb/mipbhome/welcome.htm.

Army Intelligence Master Plan

Army CI and HUMINT Support to Force Protection

by Richard I. Spence (U.S. Army, Retired)

"Force protection" is not a new term; it has been in use for several years and many normally associated it with the protection of U.S. military forces and installations. Each commander is responsible for ensuring that the command implements force protection (FP) measures. Since it would be difficult at best to discuss the totality of intelligence support to FP within this article, I will limit the scope to discussing—

- ❑ Cole Commission Report and the attack on Khobar Towers and their impact on FP.
- ❑ The evolving threat to forces in transit around the world.
- ❑ Some of the actions now underway within the counterintelligence (CI) and human intelligence (HUMINT) disciplines to support our commanders' FP programs better.

Background

In recent years, with the increased threat of terrorist attacks against U.S. interests overseas (for example, Khobar Towers, U.S.S. Cole, the assassination of U.S. officials, Department of Defense (DOD) and contractor civilian personnel), and the 11 September 2001 attacks within U.S. borders, FP programs have gained increased emphasis resulting in the identification of new requirements for heightened security actions designed to protect U.S. personnel and interests worldwide.

The Cole Commission Report served as the last in a series of significant catalysts for implementing a systematic review of our force protection policies and procedures. The report provided recommendations that not only readdressed the focus on threats against U.S. interests but also stipulated changes in how senior leaders and commanders identify and minimize, if not eliminate, the probability of such future events. The Cole Commission Report stated that operating in a new world environment characterized by unconventional and transnational threats would increase U.S. Forces' exposure to terrorist attacks and require a major effort in FP. It went on to state that changes would be necessary from national level on down, with an emphasis on awareness, training, and reorientation from a defensive to a preemptive posture. In addition, the Cole Commission recommended the refocusing of intelligence to fight the Global War on Terrorism with emphasis on collection and analysis. The report directed this new emphasis toward HUMINT and signals intelligence (SIGINT) assets.

One of the greatest challenges for FP has been accurately identifying and reporting threats in a timely manner—predictive analysis. The tendency has been to rely primarily on technical collection capabilities—with minimal or no forward-positioned HUMINT collection assets—to identify and monitor ongoing terrorist planning or activities. We now realize that to mitigate or eliminate these threats, we must use a fully functional, collaborative, multicapable collection effort to see first, understand first, and act first to defeat this asymmetric terrorist threat decisively. This multicapable collection effort would include CI and HUMINT as well as communications, electronics, imagery, measurement and signature, and open-source intelligence (COMINT, ELINT, IMINT, MASINT, and OSINT, respectively). Commanders speak with one voice when it comes to force protection; they want actionable intelligence now. They want to know the threats in sufficient time to allow them to respond with sufficient force to mitigate the threat.

Chameleon: The Changing Threat

As a chameleon adapts its color to the threat it faces, so too do the terrorists adapt their methods of operation to the environment where they operate. For example, those terrorists responsible for the attack on the U.S.S. Cole off Yemen used a small boat typical to that area, filled it with explosives, approached the Cole without drawing attention, and then detonated the explosives. This clearly demonstrates their willingness and capability to attack U.S. targets worldwide. In preparing for the attacks on the World Trade Center and the Pentagon, terrorists were able to establish legal residence in the United States where they were afforded an unimpeded opportunity to conduct training, perform reconnaissance (research airport procedures), and establish critical support. In the end, they hijacked commercial aircrafts without detection or interdiction. As an adaptive foe, terrorists learn from their own successes and failures. We can also conclude that terrorist targeting and tactics will continue to evolve. They have shown patience and a willingness to wait until the time and target are optimum to conduct an attack. Just like the chameleon analogy, Army intelligence must adapt its methods of identifying trends, capabilities, and intentions of this asymmetric threat to achieve predictive rather than historical effects.

Where Do We Go From Here?

Force protection and security can no longer solely rely on passive physical security systems. As global terrorism becomes bolder and moves from individual attacks to adaptive, sustained campaigns, intelligence support to force protection must refocus to meet the challenge. Military commanders require a predictive information network that is flexible and capable of providing greater certainty—intelligence—to influence the commander's decisionmaking process, enabling him to anticipate and preempt attacks to protect personnel and resources. The difference between physical security and full-spectrum FP lies in the employment of a first-class intelligence system capable of understanding the threat, and providing predictive intelligence fully integrated in the commander's decisionmaking process.

As the requirement for increased FP has been articulated throughout the Army, Army Intelligence has visualized and accepted an increasing role for its support to FP. To that end, the Army G2 institutionalized a new core competency, "full dimension protection," to ensure expert knowledge in physical and cyber-domains for the Objective Force.

In the near term, as a complement to our significant technical collection capabilities, we are increasing the numbers of CI and HUMINT collection assets around the world. In U.S. Army, Europe (USAREUR), we are expanding the Military Liaison Officer (MLO) program to provide FP information. In the U.S. Army South (USARSO) area of responsibility, we are developing Army Regional Liaison Offices (ARLOs) to collect on this threat. DOD is investing heavily in intelligence support to FP throughout the world with the establishment of force protection detachments (FPDs) resourced by Army, Air Force, and Navy CI personnel. These FPDs are responsible for collecting and reporting threat information which impacts the FP programs of intransit units in areas with little permanent U.S. presence. This requirement became apparent after the attack on the U.S.S. Cole. There has been an increased emphasis on expanding both technical analytic capabilities (commercial and government research and development) and increasing the number of trained, experienced analysts capable of handling and processing "metadata" to fight the Global War on Terrorism. Several U.S. Army Intelligence and Security Command (INSCOM) initiatives discussed later show clear evidence of this.

To review, FP has historically been affiliated with protection of military forces and installations. We continue to refine this supportive relationship as the threat changes. CI and HUMINT, with the other intelligence disciplines, continue to provide support to FP efforts and to provide threat situation awareness to commanders. Each discipline provides its expert capability: CI counters or neutralizes intelligence through collection, investigations, operations, analysis and production, and functional services, while HUMINT collects information in response to the commander's intelligence requirements (providing a "picture" of the enemy's strength, capabilities, intentions, and activities). Furthermore, as we continue to "transform" our intelligence corps to support the Army Objective Force, we must refine and develop our capabilities to detect, identify, and defeat terrorist threats to U.S. personnel, organizations, activities, and installations while continuing to provide the traditional tactical intelligence support to the commander.

September 11 added a new dimension to force protection. The threat was now within our borders. Army intelligence support to FP needed the ability to adapt to threats anywhere. INSCOM has answered the call. INSCOM's mission is to conduct and support dominant intelligence, security, FP, and information operations (IO) for military commanders and national decisionmakers. Evolution of INSCOM's Information Dominance Center (IDC) combines the most current, state-of-the-art technology with highly skilled analysts, to address this global terrorist threat. The IDC possesses the capability to introduce, fuse, analyze, and develop intelligence products that allow our decisionmakers to both understand evolving threats and develop strategies to counter those threats in an increasingly reduced timeline. The IDC continues to push technology, seeking new technology and capabilities that enable the collector, analyst, and consumer to collaborate not only vertically but also horizontally to "seek the ground truth."

INSCOM's 902d Military Intelligence Group possesses a long history of providing dedicated CI and FP support to Army commanders, units, and activities. Its missions include the traditional CI functions, in addition to providing focused CI analysis, terrorist threat analysis, computer-forensics support, and liaison. Additionally, it has the responsibility of providing FP support from "fort to port" to deploying forces. Since the September 11 attacks, the 902d MI Group has increased its efforts for collecting relevant threat information and providing it to the Army installation commanders. The 902d expanded its participation with national law-enforcement agencies (LEAs) in their fight against terrorism with assignment of CI agents to the Federal Bureau of Investigation (FBI) Joint Terrorism Task Forces throughout the United States.

Last year, the 902d MI Group Commander recognized a need to integrate vast amounts of collected information with data from the IDC and provide tailored support to the Army throughout the continental United States (CONUS). Hence, the Counterintelligence Integrated Analysis Cell (CIIAC) at Fort Meade, Maryland, developed to provide the analytic muscle. The CIIAC possesses established ties to the other functional activities in the areas of force protection, technology protection, support to investigations and operations, IO, and special access programs. It conducts information fusion, achieves situational awareness, and develops predictive intelligence products in support of U.S. Army personnel, units, activities, installations, and technologies. As it continues to evolve, the CIIAC is developing a capability to database CI- and counterterrorism-related incident reports, making them available to CI and terrorist threat analysts, providing a valuable source of information to national, state, and local FP and Homeland Defense activities.

Conclusion

As the Army transforms to the Objective Force and the threat to our forces around the world continues to evolve, it is imperative that Army Intelligence aggressively pursues new ways to provide the highly trained intelligence force with the most technologically advanced equipment the Army expects and deserves, focused on any threat, anytime, any place in support of the commander's mission. Crucial to that undertaking is providing predictive intelligence and expert knowledge that not only supports the combat commander but also protects the soldier. In a world where "asymmetric threats" have become the norm, it is paramount that Army Intelligence continues to enhance its capabilities in support of force protection. No longer can we accept "*should have, could have, would have*" as answers. We must live by and believe the Army Intelligence Corps motto "Always Out Front!" However, we must also remember, in all things, "SOLDIERS FIRST!"

Richard Spence (Chief Warrant Officer Three, U.S. Army, Retired) is a Futures Analyst with the Army Intelligence Master Plan (AIMP). His active duty assignments included assignments with the United States Marine Corps (with his Vietnam tour); CI Special Agent (MI) with the 513th MI Group; CI Polygraph Examiner with the 66th MI Bde and the 902d MI Group; Security Manager and Special Access Programs (SAPs) Operations Officer, 902d MI Group; Force Protection CI Team Chief and 1st Cavalry Division Security Manager; Counterintelligence Analyst, Joint Analysis Center (JAC); and S2 Staff Operations Officer, 902d MI Group. He holds a Master of Science degree in Counseling, and a Bachelor of Arts degree in Sociology. You may contact him via E-mail at Richard.Spence @hqda.army.mil and telephonically at (703) 681-3746.

Concepts Corner

Objective Force/Future Combat System (OF/FCS) C2 and ISR Experiment

by Major Robert C. Buscher

The Army's Objective Force (OF) provides revolutionary new capabilities for the U.S. Army in its ability to deploy worldwide in a matter of hours, capitalizing on information superiority and developing the situations both in and out of contact. Playing a critical role in OF development are command and control (C2) and intelligence, surveillance, and reconnaissance (ISR), which allow the commander to execute the battle with superior situational understanding, shape the battlefield with standoff precision fires, and set the conditions for contact with the enemy at the time and place of his choosing.

To test the OF's C2 and ISR concepts, the Unit of Action (UA) Maneuver Battle Lab (UAMBL) at Fort Knox, Kentucky, conducted the OF/FCS C2 and ISR Experiment in December 2002. The OF/FCS C2 and ISR Experiment served as both an educational and an experimental event, providing participants with a shared understanding of the OF concept. The focus of the exercise was to run a dynamic simulation-based experiment that enables discussion of the critical issues affecting OF development.

The OF/FCS C2 and ISR Experiment was the first in a series of experiments conducted to assess the commander's ability to conduct battle command given a proposed C2 and ISR architecture. The OF/FCS C2 and ISR Experiment provided all participants with a common understanding and a shared vision of the ability of the FCS-equipped UA to fight and win. Additionally, it presented a simulation-based environment for the examination of the UA in a tactical setting. The Experiment will serve as a combination of dynamic wargaming sessions, orders development workshops, and focused after-action reviews.

Readers can contact Major Buscher in the Concepts and Requirements Division at the U.S. Army Intelligence Center and Fort Huachuca via E-mail at robert.buscher@hua.army.mil and by telephone at (520) 538-1123 or DSN 879-1123.

Doctrine Corner

The Challenges of Homeland Defense

by Chief Warrant Officer Five Clyde Green

Homeland Defense (HLD) efforts have significantly affected the role of the Armed Forces and the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH), Arizona. Fort Huachuca's Concepts and Doctrine Divisions are influencing policy with the development of intelligence support to installation commanders' antiterrorism/force protection (AT/FP) doctrine. The Army Military Intelligence (MI) Corps is a crucial component in how the Army will develop and manage information to support the Department of Homeland Security.

This article builds upon the July-September 2002 ***MIPB*** Doctrine Corner column on page 52. USAIC&FH has developed a Special Text (ST) document to support the commander and soldiers of units conducting AT/FP support operations. STs will facilitate the dissemination of documents that will provide for a single point of reference consolidating and cross-referencing doctrine and information for individuals supporting HLD. Access for these documents will soon be available through the Intelligence Center homepage.

ST 2-91.2, Intelligence Support to Installation Commander's Antiterrorism Program and Force Protection (AT/FP), is a living manual. We will periodically revise it as necessary based on comments from the field or when other significant changes occur.

ST 2-91.2 establishes the initial doctrinal foundation and describes tactics, techniques, and procedures (TTP) used to produce all-source intelligence support to AT/FP. It focuses on intelligence production at the installation level and amplifies the doctrine contained in other AT/FP publications.

This ST comprises four chapters and ten appendixes.

- □ The first chapter covers the introduction and overview of FP.
- □ Chapter 2, Commander and Staff Responsibilities and Duties, is a consolidation of the HLD and Department of Defense guidance provided to Department of the Army for the architecture, organization, and the expectations of the installation commander and staff for AT/FP. This chapter also provides direction and recommendations for a successful intelligence, surveillance, and reconnaissance (ISR) cell and communications architecture.
- □ Chapter 3, Intelligence Support to AT/FP Operations, reinforces AT/FP concepts and focuses the MI analyst on analytical and complementary methodologies as performance tasks.
- □ Chapter 4, Antiterrorism/Force Protection Targeting Process, provides the commander and staff with the process an adversary might use for targeting an installation. They can apply this assessment to evaluate the vulnerability of the installation and to provide analytical direction in support of HLD.
- □ The appendixes provide both website addresses for additional information and samples and examples for the analyst.

Doctrine Division will continue to update ST 2-91.2 as resources and manpower are available. We will issue related materials as needed (see http://doctrine.futures.hua.army.mil).

Chief Warrant Officer Five Clyde Green is a doctrine writer at the U.S. Army Intelligence Center and Fort Huachuca. Readers can contact him via E-mail at clyde.green@hua.army.mil and by telephone at (520) 538-0993 or DSN 879-0993.

Is the Road in Georgia Too Perilous?

(Continued from page 47)

26. Lobe, Jim, "Caspian Pipeline Plan Draws Strong Protests," Inter Press Service, accessed at www.atimes.com/c-asia on 28 June 2002.

27. Brady, Thomas, "Georgia Invites United States to Chart Its Own Policy," a EurasiaNet Commentary accessed at www.eurasia.net on 18 September 2002.

Second Lieutentant Jake Miller, U.S. Air Force, is a Air Battle Manager student stationed at Tyndall Air Force Base, Florida. He received his Bachelor of Arts degree from Angelo State University and is currently working toward a Master of Science degree in Strategic Intelligence at the American Military University. His research interests include Russian foreign policy, ethnic conflict in the Black Sea region, and leftist political movements in Venezuela. Readers may contact the author via E-mail at jake.miller@tyndall.af.mil.

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, IO SIGINT, IMINT, war on terrorism and tactical operations. E-mail them to mipb@hua.army.mil or call (520) 538-0564/1005 or DSN 879-0564.

Proponent Notes

by Lieutenant Colonel Eric W. Fatzinger

In this issue we will focus on educational opportunities, initiatives, and a number of programs that are available to support you. I would draw your attention to the things that are happening in the Officer Education System (OES) in particular. They are revolutionary in the nature of how we as an Army Officer Corps approach officer education. Those initiatives and especially assignment-oriented training (AOT) are representative of where the Army is heading in the near term. While desiring to increase technical proficiency on the one hand, the Army is also very serious about reducing the amount of time we keep our soldiers and officers in school "accounts" and off field-unit rosters. The idea is to make certain that we provide what is needed—"on time training"—while not spending time in the classroom on topics that could be available elsewhere or that students will not use for some time.

Enlisted Actions

As I travel around the world and talk with our soldiers and noncommissioned officers (NCOs), I am frequently reminded that too many of us are unaware of the great technical education programs that exist for Military Intelligence (MI) soldiers. In this space, I have decided to highlight some of those programs, specifically for the NCOs in the 98 Career Management Field (CMF). I will cover the—

❑ Middle Enlisted Cryptologic Career Advancement Program (MECCAP).

❑ Military Intern Signals Intelligence (SIGINT) Analyst Program (MINSAP).

❑ Military Electronic Intelligence (ELINT) Signals Analyst Program (MESAP).

❑ Military Communications Intelligence (COMINT) Signals Analyst Program (MCSAP).

All of these programs are highly competitive and the National Security Agency (NSA) designed them to help take MI NCOs to an advanced level of understanding and proficiency within their specific military occupational specialties (MOSs). Some are open to multiple MOSs, while others are restricted to a single SIGINT MOS; all are three-year work-study programs. An announcement message usually goes out in October of each year, with an application deadline of the following January and a selection board meeting in May.

Middle Enlisted Cryptologic Career Advancement Program. MECCAP is open to the entire 98 CMF and combines classroom study and work assignments to increase participants' knowledge in their cryptologic disciplines. It also focuses on increasing the soldiers' understanding and management skills as they relate to other MI disciplines. While NSA can waive some entrance items (check the announcement message), the program is in general for soldiers in the ranks of Staff Sergeant (SSG) and Sergeant First Class (SFC) with between 7 and 12 years of service. Time on station (TOS) requirements exist for applicants both in and outside the continental Unites States (CONUS and OCONUS), and they must have a current, valid Top Secret (TS) security clearance with sensitive compartmented information (SCI) access. They must also be willing to reenlist for a 36-month remaining service obligation as a part of the program (36-month program + 36-month obligation = 6-year commitment).

Military Intern SIGINT Analyst Program. MINSAP is open only to MOS 98C (SIGINT Analyst) and combines classes and work assignments to increase participants' knowledge in their cryptologic discipline to fill multiskill, advanced, technical analyst positions after graduation. Again, while NSA may waive some items (check the announcement message), the program is generally for Sergeant (SGT) and SSG soldiers with between 4 and 12 years of service only. TOS requirements exist for both CONUS and OCONUS applicants, and applicants must have a current, valid TS clearance with SCI access and they must be willing to reenlist for a 36-month service-remaining obligation as part of the program (36-month program + 36-month obligation = 6-year commitment).

Effective FY06, the Army will delete MOS 98J and create MOS 98Y

Military Electronic Intelligence (ELINT) Signals Analyst Program. MESAP is open only to soldiers in MOS 98J (ELINT Interceptor/Analyst) and combines classes and work assignments to increase participants' knowledge in advanced ELINT signals analysis under the auspices of the Space and Weapons Science Customer Center and the National Cryptologic School. While they may waive some items (check the announcement message), the program in general is for SGTs and SSGs with no more than 14 years of service and at least 4 years of operational assignments as 98Js. TOS requirements exist for both CONUS and OCONUS applicants and they must have a current, valid TS security clearance with SCI access and must be willing to reenlist for a 36-month service-remaining obligation as part of the program (36-month program + 36-month obligation = 6-year commitment).

The Army will delete MOS 98J effective fiscal year 2006 (FY06) with a division of the ELINT skills between 98C (SIGINT Analyst) and new MOS 98Y (Signals Collector/Analyst). However, although MOS 98J will disappear, its base skill sets will still exist and will still be valuable so the expectation is that MESAP will continue but most likely will open up to 98C soldiers and possibly to 98Y soldiers as well.

Military Communications Intelligence (COMINT) Signals Analyst Program (MCSAP). MCSAP is open only to MOS 98K (Signals Collection/Identification Analyst) and combines classes and work assignments to increase participants' knowledge in their cryptologic discipline under the auspices of the Consolidated Signals Analysis Development Office and the National Cryptologic School. While they may waive some items (check the announcement message), the program is for SGTs and SSGs with no more than14 years of service, and at least 4 years experience as a 98K. TOS requirements exist for both CONUS and OCONUS applicants, and the applicants must have a current, valid TS security clearance with SCI access and must willing to reenlist for a 36-month service-remaining obligation as part of the program (36-month program + 36-month obligation = 6-year commitment).

Effective FY06, the Army will create new MOS 98Y, which will include traditional 98K skills. Since the skill set will still remain and still be valuable, we expect that MCSAP will continue and be available to 98Y soldiers.

All of these programs are excellent chances for CMF 98 NCOs to broaden their specific MOS skills and improve their understanding of other MOSs and the intelligence community. As a graduate of MECCAP, I can tell you first hand that these are quality programs that are well worth the time and commitment. Keep an eye out for the annual announcements and if you are eligible, I encourage you to apply. Normally, the messages appear on the MI Branch website at https://www.perscomonline.army.mil/epmpmilang/MI/miteam.htm.

Upcoming NCO Boards. The 2003 Master Sergeant (MSG) Selection Board met in February 2003 and, at the time of this writing, we expect release of the results in April. To view MOS input to the senior enlisted centralized boards, go to http://138.27.35.32/ocmi/EN_Info_portal.htm. If you want to know what the board members are seeking, this is the best place to start.

As always, if you have questions on career maps, courses, impact of assignments, or any other enlisted actions, feel free to contact me, Sergeant Major Walter Crossman. You can reach me via E-mail at walter.crossman@hua.army.mil and by telephone at (520) 533-1174 or DSN 821-1174.

Warrant Officer Actions

All too often, and with some justification, many of you have told me that the warrant officer (WO) professional educational system is far too limited and assumes that WOs come to their positions with the requisite knowledge and skills to achieve success and places too little attention on continuing technical education. Well the good news is that this is changing. A critical component to the Army's Training and Leader Development Program—Warrant Officer (ATLDP-WO) Study, of which you have heard me speak of before (see the July-September 2002 issue of ***MIPB***), is the intent to "up gun" the current warrant office education system. In the meantime, you do not have to wait. There are a number of great opportunities out there for us.

Civilian Education. Civilian education is an important and ever-increasing part of a warrant officer's professional and personal development. The Army's goal is for all WOs to have at least an associate degree and to earn a bachelors degree by the time they reach Chief Warrant Officer Four (CW4). MI WOs have several ways in which they can accomplish this education goal. Start with your installation education office; they can provide all the information you need on local opportunities offered by local and extension universities.

Permissive Temporary Duty (TDY) Study. AR 621-1, Training of Military Personnel at Civilian Institutions (20 August 1999, Chapter 4-1e), and **AR 600-8-10**, **Leaves and Passes** (1 July 1994, Chapter 1 and Section XVI, paragraph 5-31) cover permissive TDY for study (20 weeks or less). Under this program the commanding general (CG), U.S. Total Army Personnel Command (PERSCOM), will consider requests for permissive TDY for civilian training exceeding 31 or more days. The period of permissive TDY study must not exceed 139 days (20 weeks or less). The CG, PERSCOM, must sanction and approve civilian schooling and the commander must provide a recommendation. Participants will incur an active duty service obligation and the TDY must result in the award of a degree.

Degree Completion Program (DCP). Current policy governing the Degree Completion Program limits your time in the program to 12 months or less. Before the beginning of each academic term, students in the DCP must complete DA Form 2125, Report to Training Agency, and forward it to Commander, PERSCOM, ATTN: TAPC-OPW-D (Ms. Gregory-Williams), 200 Stovall Street, Room 6N07, Alexandria, Virginia 22332-0420. Be aware that inability to complete civilian training in the time allotted is considered adverse and your Academic Efficiency Report (AER) will likely reflect that information. Again, you must finish your degree during the time allotted.

Postgraduate Intelligence Program (PGIP) and Master of Science of Strategic Intelligence (MSSI) Degree Program. The Joint Military Intelligence College (JMIC) at Bolling Air Force Base, Washington, D.C., provides two additional education programs. This academic institution—sponsored by the Defense Intelligence Agency (DIA)—is now accepting applications for the PGIP and MSSI Degree Program. All WO applicants accepted into the program must finish the MSSI. The PGIP with MSSI is a one-year program that runs from August through the following August. The PGIP curriculum emphasizes developing the student's understanding of intelligence at the national level, military strategy, national security policy, and the planning and execution of joint and combined operations. The service obligation incurred is three times the length of schooling. You can find additional information about JMIC at http://www.dia.mil/Jmic. Normally, in order to maximize usage of newly acquired analytical skills, WOs who graduate with the MSSI degree may receive assignments to strategic or theater-level jobs upon graduation. Applications must arrive not later than 31 October each year at the PERSCOM Warrant Officer Division; they will in turn notify officers in writing of their selection or nonselection for the program by 30 January of the following year.

White House Fellowship Program. Another professionally rewarding program often overlooked is the White House Fellowship Program. Under this program, selected officers have an opportunity to serve from one to two years on one of the White house staffs. Regular Army WOs with no more than 24 active WO service years and Reserve Component (RC) WOs with no more than 16 years of active federal service may be eligible to apply. Check with your assignments officer at PERSCOM to get complete details about obtaining permission to compete for one of these prized fellowships.

Upcoming WO Boards. The next WO Promotions Board for Chief Warrant Officer Three through Five positions will be from 29 April through 30 May 2003.

The point of contact (POC) for all WO actions is Chief warrant officer of the MI Corps, CW5 Lon Castleton. You can reach him via E-mail at lon.castleton@hua.army.mil and telephonically at (520) 533-1183 or DSN 821-1183.

Officer Actions

Changes to the Officer Education System (OES). The Army is making a number of major changes to the OES. The intended goal is to reduce the amount of time officers spend in formal schools while continuing to maintain their current levels of technical competency and to provide this education to all officers. This will ensure a thorough grounding in combined arms operations and that all officers through the grade of Major have a common educational framework regardless of their career field, Branch, or functional area.

Basic Officer Leadership Course (BOLC). The BOLC will replace the current Branch-specific Officer Basic Course (OBC). The ATLDP officer study highlighted a need for changes to the current OBC training concepts. It noted that currently there is a disparity in the skills of Second Lieutenants (2LTs) from the three primary commissioning sources. Further, new 2LTs lack a combined arms perspective and have no common bond with their peers from other Branches. The intention of the new BOLC is to address both of these issues. It will have at least three phases:

- ❑ Phase I will be the precommissioning phase with officers separately trained via the U.S. Military Academy, Officer Candidate School (OCS), the Reserve Officer Training Corps (ROTC), etc.
- ❑ Phase II will be the field leadership training phase that will emphasize building confidence and leadership and developing rigor and toughness in junior officers. This phase will be at one of several locations for all new 2LTs, most likely at Fort Benning, Georgia; Fort Sill, Oklahoma; and Fort Knox, Kentucky.
- ❑ Phase III of the BOLC will be the actual Branch training conducted at the current Branch schools. This new training strategy is intended to establish a cross-Branch Army standard for leadership and to place more emphasis on hands-on, performance-oriented, Branch-immaterial generic field training rather than Branch-specific training. Implementation of these changes could come as soon as the third quarter (3Q) FY06.

Captains (CPTs) OES. Under the current Captains Career Course (CCC) model, three of every four captains graduate and go off to serve in staff positions rather than company command. The result is that much of the current CCC curriculum is spent in training for an assignment that most officers will not go to upon course completion. Therefore, in an effort to reduce the overall length of the CCC and to focus on those skills that are of immediate value, the Army is considering a new training model. The final design of this course or courses has not yet been approved but a preliminary design has begun to take shape and may occur as a pilot program as early as 2005. In accordance with current thinking, there will be two separate courses that run in parallel. The first is a 4- to

6-week Combined Arms Staff Course for the majority of officers going to follow-on staff positions. The second course is a 10- to 14-week Combined Arms Battle Command Course for officers slated to take company command. Both courses will consist of distance learning and resident phases; since the length of the courses will be considerably shorter than those of today, students can attend them in a TDY status, without requiring a permanent change of station. The Army's intent is to increase the fill of Captains in units by decreasing the amount of time they spend in school and to decrease the turbulence for families resulting from multiple short moves during these company-grade years. It will also synchronize training and education with the officers' assignments. Implementation of these changes could happen as early as the 3QFY05. Again, more work remains before implementation. We will keep you apprised in these pages as this develops.

Major (MAJ) Intermediate-Level Education (ILE). The concept behind the changes to ILE training are to ensure **all** Army Majors have the same quality, tailored educational experience. All officers will attend a common-core course either at Fort Leavenworth, Kansas, for Operations Career Field (CF) officers or a satellite campus for most non-Operations CF officers including functional area (FA) 34 (Strategic Intelligence) officers. Operations CF officers will remain at Fort Leavenworth to attend the Advanced Operations and Warfighting Course (AOWC). Most non-Operations CF officers will not attend the common-core course at Fort Leavenworth but rather will receive the same common-core course taught at a satellite location and then attend their FA qualification courses. All officers will receive Military Education Level Four (MEL-4) and Joint Professional Military Education Level One (JPME-1) upon successful completion of the common-core course. Implementation of the new ILE should occur in 4QFY05.

Upcoming Officer Selection Boards. Both the Major and Captain Promotion Boards will meet during May, Senior Service College in April, and the Career Field Designation (CFD) Board for year group 1993 in June 2003.

The POC for officers and civilians is Ms. Charlotte Borghardt. Readers can reach her through E-mail at charlotte.borghardt@hua.army.mil and by telephone at (520) 533-1178 or DSN 821-1178.

Lieutenant Colonel Eric Fatzinger is the Director, Office of the Chief, Military Intelligence (OCMI). Readers may contact him via E-mail at eric.fatzinger@hua.army.mil. Robert C. White, Jr., is the Deputy OCMI. Readers can reach him via E-mail at robert.white@hua.army.mil. You are encouraged to access the OCMI website through the Intelligence Center homepage at http://usaic.hua.army.mil/ and then link to OCMI by choosing the Training/MI Professionals area. You will be able to find information on issues ranging from enlisted career field overviews to officer, warrant officer, and civilian updates.

G2 Contributions

(Continued from page 20)

cuss those areas for which the G2 is not responsible:

- □ The TVA process—the commander initiates the TVA through the PMO or G3.
- □ Being the sole participant in the TVA.
- □ The holder of the TVA results. Per **AR 525-13, Antiterrorism** (4 January 2002), the installation must file, store, and maintain the TVA in operational channels.

Conclusion

The TVA is a complete staff product that analyzes all the aspects of security and evaluates their threat security measures and operating procedures in place. TVA results assist the commander and staff by—

- □ Providing the basis and justification for FP enhancements, program and budget requests, and the establishing of various FP condition (FPCON) measures.
- □ Establishing methodologies to protect, detect, and react to intrusions of all types, to include facilities, computers, and command and control systems.
- □ Establishing an operations security (OPSEC) program that reduces threat access to information.
- □ Employing security measures.

To contact the writers, go to http://doctrine.futures.hua.army.mil.

Security Releases Required With Your Articles

The ***Military Intelligence Professional Bulletin*** always welcomes your professional contributions! ***MIPB*** does require a release signed by your local security officer or SSO stating that your article and the accompanying graphics are "unclassified, nonsensitive, and releasable in the public domain." The release should include your name, the title of the article, and contact information for the person who signs the release. We must have a signed copy of the security release either mailed or faxed to us. If your installation or agency requires you to obtain a public affairs release as well, please do so.

TSM Notes

Update on Joint STARS, Common Ground Station (CGS), Joint Tactical Terminal (JTT), and the Distributed Common Ground System-Army (DCGS-A)

by Colonel Stephen J. Bond

Last summer the U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM) Joint Surveillance Target Attack Radar System (Joint STARS) received the added responsibilities of systems development for the centerpiece system for Military Intelligence in the Objective Force, the Distributed Common Ground System-Army (DCGS-A). While we are rapidly working the requirements for this system to meet Objective Force timelines, we continue to field the Common Ground Station (CGS) to the force and support the Global War on Terrorism. We will complete fielding CGS to Active Component (AC) units in 2003 and to U.S. Army National Guard units in 2004. The Army is currently making good use of CGS—more than 30 are in use supporting Operation IRAQI FREEDOM.

Joint STARS and CGS

In April 2003, the 10th Mountain Division (Light) was the last AC unit to receive the Joint STARS and CGS system. We have begun the final major-equipment addition to CGS, adding the Joint Tactical Terminal (JTT) to the system. JTT replaces the Commander's Tactical Terminal currently installed on the CGS; the schedule calls for completed retrofit of JTTs into all existing CGSs in March 2005. (More on the JTT appears below.)

The Joint STARS Wing redesignated from the 93d Air Control Wing (ACW) to the 116th ACW, at Robins Air Force Base, Georgia. The 116th ACW received its 14th Joint STARS aircraft in August 2002; the Air Force will receive the final three aircraft by the end of fiscal year 2005 (FY05). The 116th ACW has Joint STARS successfully supporting Operation IRAQI FREEDOM at press time.

Joint Tactical Terminal

The JTT will reside in many Military Intelligence systems. Starting in January 2003, we integrated the Joint Tactical Terminal-Senior (JTT-Senior) into the CGS. JTT-S will also be a component of Guardrail Common Sensor (GRCS), Airborne Reconnaissance Low (ARL), Tactical Exploitation System (TES), and the All-Source Analysis System (ASAS). It will also be a component of air defense artillery and aviation systems. The JTT-S is part of the JTT family of intelligence terminals with the capability to receive multiple information broadcasts, collectively known as the "Integrated Broadcast Service (IBS)."

The JTT-Briefcase (JTT-B) is a stand-alone terminal variant of the JTT with the U.S. Army Special Operations Command (USASOC) as the primary Army user. The JTT-B consists of a four-channel receive-only radio, with an embedded cryptologic module in a ruggedized laptop computer for processing data, and an accessory kit. In support of Operation ENDURING FREEDOM, we accelerated the JTT-B fielding to USASOC. The broadcast data provides units with critical threat warning, targeting, situation awareness, "Blue" force tracking, and force protection (FP) information. Reports from the field concerning system performance and user satisfaction in actual combat operations are extremely positive.

Distributed Common Ground System-Army (DCGS-A)

The requirements-determination process for DCGS-A continues on the fast track with the Army's Objective Force. DCGS-A is part of the Department of Defense-mandated Distributed Common Ground/Surface System (DOD DCGS) family of systems for joint and national intelligence, surveillance, and reconnaissance (ISR) interoperability. For the Army, DCGS-A will become the Objective Force ISR tasking, processing, exploitation, and dissemination system. It is the processing system and fusion engine for many Army ISR collection assets and the gateway for joint, national, and eventually allied and coalition as well as commercial information. It will—

- ❑ Provide the enemy, unknown or neutral, and environmental pieces to the Objective Force battle command systems common operating picture (COP).
- ❑ Furnish a wargaming and mission rehearsal capability.
- ❑ Supply the "running intelligence staff estimate."

The DCGS-A will have a central role in leveraging the national, joint, coalition, and commercial ISR into a processing architecture extending into combat elements. As a "mud to space" system, DCGS-A will have "nodes" at all Army echelons from the Future Combat System (FCS) equipped Units of Action (today's brigade and below units), to the Units of Employment (today's division and corps units), U.S. Army Intelligence and Security Command (INSCOM) elements, and designated Land Component Commands and Joint Task Forces formed around Army organizations.

The Objective Force DCGS-A consolidates the capabilities and replaces the hardware found in the following current force systems:

- □ ASAS.
- □ Counterintelligence/Human Intelligence (CI/HUMINT) Information Management System (CHIMS).
- □ TES.
- □ Guardrail Information Node (GRIFN).
- □ Guardrail Common Sensor (GRCS) Intelligence Processing Facility (IPF).
- □ Prophet Control.
- □ Joint STARS CGS.
- □ Tactical Unmanned Aerial Vehicle (TUAV) Ground Control Station (GCS).

Essentially, DCGS-A breaks the "stovepipes" and reduces the large equipment "footprint" inherent in our current systems and will further provide timely and actionable feeds to deployed tactical units. The Army's FCS has "embedded" DCGS-A requirements and capabilities, and it is the ISR processing component of the Army's future Battle Command System. DCGS-A received its first Army Staff Systems Review on 21 November 2002; during that meeting, General Eric K. Shinseki, the Army Chief of Staff, remarked that *"DCGS-A is one of the cornerstone systems of the Objective Force."*

Colonel Steve Bond is the TRADOC System Manager (TSM) for the Joint Surveillance Target Attack Radar System (Joint STARS), Common Ground Station, Joint Tactical Terminal, and the Distributed Common Ground System-Army (DCGS-A). Readers can contact him via E-mail at steve.bond@hua.army.mil and telephonically at (520) 533-3605/2480 or DSN 821-3605/2480. Visit TSM Joint STARS at their new website. Their address is https://www.futures.hua.army.mil/tsmjstars.

U.S. Army Reserve Command MI Augmentation Detachment

Military Intelligence (MI) soldiers are a critical U.S. Army asset. The nation has a real interest in preserving and employing these skills, especially as the MI soldier gains experience in using these hard-won skills. To retain these soldiers and their skills for the nation, the U.S. Army Reserve Command established the Military Intelligence Augmentation Detachment (MIAD) directly subordinate to the USARC. The MIAD's mission is to facilitate life-cycle management of MI soldiers in the Reserve Component (RC). The Detachment accomplishes its mission by assigning USAR enlisted, warrant, and company-grade soldiers to USARC high-priority MI units with vacancies. The MIAD enables MI-qualified soldiers who do not reside near a USARC Tier 1 unit to be productive members of the U.S. Army Reserve (USAR). The primary MIAD focus is the retention of soldiers leaving active duty, soldiers displaced by unit reorganizations or inactivation, and USAR soldiers relocating to an area without a USAR MI unit.

After joining the MIAD, MI soldiers have funding to attend a minimum of six 3-day trips in active-duty-for-training (ADT) status each fiscal year. These normally occur during the unit's weekend training periods. During these six ADT periods, the MIAD funds the soldiers' transportation and lodging expenses. The soldiers also must perform a minimum of 24 mutual training assemblies (MUTAs) either at a unit close to his home or through other means such as performing intelligence-related work using the World Basic Information Library. The MIAD will also fund travel and base pay for the soldier's annual training period (normally two weeks each year) if it is more than normal commuting distance of the soldier's home. Some USAR MI personnel perform their AT as overseas deployment training (ODT).

Languages Needed

Currently the MIAD needs soldiers with language skills in Arabic, Chinese-Mandarin, French, Korean, Persian-Iranian, Spanish, Russian, Serbo-Croatian, Thai, Turkish, Urdu, Vietnamese. Soldiers not skilled in critical languages may be eligible for attendance at the Defense Language Institute (DLI).

Additional MIAD Opportunities

The MIAD also manages soldiers in two other types of units. A limited number of MIAD soldiers can serve as Technical Intelligence Analysts with 203d MI Battalion at Aberdeen Proving Ground, Maryland. The 203d is a multiple-component (MultiCompo) unit and the only technical intelligence battalion in the Army. To be eligible for this assignment, soldiers must be qualified Technical Intelligence Analysts. Most of these positions are at the Sergeant, Staff Sergeant, and Sergeant First Class levels. MI NCOs can also serve with one of the five Army Reserve Total Army School System (TASS) units as MI Instructors. These soldiers have the important job of instructing RC soldiers in MI subjects.

Contacting the MIAD

Active duty soldiers leaving the Active Army who are interested in an MIAD assignment can obtain more information from their post transition counselors. Additional information on the MIAD is available from the Army Knowledge Online (AKO). Go the Army Communities/Army Reserve/Direct Reporting Units and click on the MI Augmentation Detachment. You can also contact the MIAD via E-mail at MIAD2@usarc-emh2.army.mil or by telephoning 1-800-359-8483, extensions 9546/8896.

MI Corps Hall of Fame

2003 Military Intelligence Corps Hall of Fame Inductees

The 16th annual Military Intelligence Corps Hall of Fame (HOF) ceremony will be on 27 June 2003. The Corps will induct seven new members:

- ❑ Chief Warrant Officer Four (Deceased) Douglas C. Edgell.
- ❑ Colonel (Retired) Alfred H. Elliott, III.
- ❑ Colonel (Deceased) David A. McKnight.
- ❑ Command Sergeant Major (Retired) John P. O'Connor.
- ❑ Chief Warrant Officer Four (Retired) Ben E. Peets.
- ❑ Major General (Retired) John D. Thomas, Jr.
- ❑ Captain (Deceased) Humbert R. Versace.

Chief Warrant Officer Four Douglas Clyde Edgell (U.S. Army, Deceased)

Chief Warrant Officer Four Douglas Edgell was a leader, soldier, and motivator who left a legacy of professional and personal achievements. He played a leading role in developing and implementing improved Army counterintelligence (CI) tactics, techniques, and procedures (TTPs) in the changing post-Cold War environment of the late 20th century. He used his experience in CI and counterespionage to refine the role of Army CI agents in the new environment. CW4 Edgell envisioned how laptop computers, databases, and portable satellite communications could improve the Army CI mission and allow deployed CI teams to "reach back" to CI support bases in Germany or the United States for critical information. He helped refine procedures for a new type of CI analysis required to support those deployed forces and integrated all of this into new training. His vision became the standard for training, first in Germany, then throughout Army intelligence. He ensured that the evolving methods and concepts became part of Army CI doctrine.

The results of CW4 Edgell's efforts enhanced the Army CI force's capability to support deployed Army units participating in joint and coalition operations around the world and to protect them from sabotage, espionage, subversion, and terrorist threats. Ultimately, his work significantly influenced joint and sister Service CI doctrine and force modernization as well.

CW4 Doug Edgell began his distinguished Army career in 1976. He first served as a reconnaissance specialist assigned to the 11th Armored Cavalry Regiment, engaged in monitoring the inter-German border between free West Germany and Communist East Germany. Upon returning to the United States in 1979, he changed his military occupational specialty to military intelligence (MI) and began his long and exceptional career as a CI Special Agent. Assigned to the 902d Military Intelligence (MI) Group, with duty in Detroit, Michigan, then Sergeant (later Staff Sergeant) Edgell conducted numerous CI investigations supporting CI operations across Michigan, northern Ohio, and throughout the mid-western United States.

In 1983, he was selected as a CI Warrant Officer. His assignments subsequently led him from the U.S. Army Intelligence and Security Command (INSCOM) Theater Intelligence Center-Pacific—performing CI investigations and operations supporting the U.S. Army Western Command and the Joint U.S. Pacific Command (PACOM)—to a return to Germany with the 1st Armored Division (1 AD). While assigned to 1 AD, he served as the 501st MI Battalion S2, the Division CI Operations Officer, and the Signals Intelligence (SIGINT) Liaison Officer. These positions required him to develop and track enemy order of battle (OB), manage counterespionage and personnel security investigations, perform real-time terrorist and other force protection (FP) threat analysis, and conduct rear-area operations analysis and CI battlefield operational oversight. In July 1987, he became the Special Agent in Charge of the Fort McClellan, Alabama, Resident Office performing investigations, CI operations (including special-access program security support), and liaison in northern Alabama, Mississippi, and southwestern Georgia.

Chief Edgell returned to Germany in August 1990 assigned to VII (US) Corps. There he served as the Senior Planner for CI, FP, and security operations in southern Germany and later in support of VII Corps operations in Southwest Asia during Operations DESERT SHIELD and STORM. There he supervised daily CI analysis and operations security briefings for the corps commander. Following DESERT STORM in summer 1991, CW3 Edgell returned from Southwest Asia to Germany and an assignment with the 66th MI Brigade as the CI Operations Officer in the 527th MI Battalion and later the18th MI Battalion.

It was during these assignments that he began to exert extraordinary and visionary influence on the conduct of Army CI missions across the tactical-operational-strategic spectrum. He clearly saw that to be successful the Army CI force would have to adapt to the emerging challenges of post-Cold War Europe and the 21st century. These challenges ranged from peacekeeping missions in the Balkans, networked information technology for integrated CI/human intelligence (HUMINT) teams at brigade and lower levels, to revolutionary new training to prepare teams and individuals. Integrating his experience in armored cavalry border operations, strategic operational level CI support, MI battalion operations, and CI operations for a corps at war, he led a small cadre of visionaries who implemented successful changes in CI/HUMINT TTPs.

His first step was to develop the Contingency Operations (CONOPs) Course to train 18th MI Battalion soldiers to operate in the new environment. He and the battalion trained the CI agents that accompanied the U.S. Army Berlin Brigade (an elite infantry unit that had guarded Berlin during the Cold War) into Macedonia on the peacekeeping mission known as Task Force ABLE SENTRY. The methods and practices that he put in place quickly became the doctrine for theater-wide CI/HUMINT operations throughout Europe and Africa. The course became a U.S. Army, Europe (USAREUR) showcase course both endorsed and exported by the Deputy Chief of Staff for Intelligence (DCSINT), USAREUR. The XVIII Airborne Corps and other units preparing for Bosnia and Somalia later used this same training in the United States. The course ultimately became the Counterintelligence Force Protection Source Operations (CFSO) Course trained at the U.S. Army Intelligence Center and School (USAICS).

During this same period, Chief Edgell refined the operational characteristics of the Theater Rapid Response Intelligence Package (TRRIP). This 66th MI Brigade initiative provided a means for deploying CI support to an operational area early, while retaining the ability to draw on the larger CI community worldwide. The system proved highly successful in subsequent contingency deployments to Macedonia, Croatia, Rwanda, Haiti, and Bosnia and continues as a cornerstone for CI deployments to this day.

Mr. Edgell knew what the CI agents with Task Force ABLE SENTRY in Macedonia would have to accomplish while deployed and their requirement to reach back to Germany for intelligence support. He became the Chief of the Multi-Discipline Counterintelligence Cell at the USAREUR Combat Intelligence Readiness Facility in Augsburg where he taught soldiers what and how to research, analyze, and service CI support requirements.

CW4 Edgell took his European operational intelligence knowledge and experience with him to his final military assignment to the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) where he chaired the Counterintelligence Training Committee. He managed seven MI courses of instruction, provided oversight on revision and conduct of specialized antiterrorism/force protection (AT/FP) and tactical source operations, and directed the updating of existing Army CI/HUMINT doctrine and literature. He played a major role in writing the White Paper known as *Counterintelligence XXI*, which focused on the changes required of the CI community in order to effectively operate in the 21st century.

CW4 Douglas Edgell's retirement from Army active duty in June 1997 marked the beginning of a new civilian intelligence career, but not a lessening of his contribution to Army Intelligence. Working with private industry, he became a Senior Analyst and Program Manager providing functional and technical guidance to the Army's CI/HUMINT modernization effort. He assisted with standardization of CI/HUMINT forms and the development of DOD-wide tactical reporting mechanisms of new policies and guidelines for Defense CI information-system applications in the U.S. Army's All-Source Analysis System (ASAS).

Colonel Alfred H. Elliott, III (U.S. Army, Retired)

Colonel Alfred H. Elliott, III, earned a Bachelor of Arts degree in Government and Law from Lafayette College in Easton, Pennsylvania, in 1969 and a commission in the Infantry. He first served as the Training Officer in a Basic Training Battalion. In 1970, he attended helicopter flight training.

During his career, Colonel Elliott has served as a Commander, Aide-de-Camp, Operations Officer, Deputy Director of Flight Training, and Director of Combat Developments. He spent his tactical time primarily in Europe and Southeast Asia, serving in Vietnam for sixteen months as a helicopter pilot participating in frequent combat operations. At the 2d

Armored Cavalry Regiment he began his long association with Army intelligence while serving as a Border Reconnaissance Troop Commander and flying surveillance and reconnaissance missions along the inter-German border. In the intervening years, Colonel Elliott held positions of increasingly greater responsibility in the aviation community. While attending the Command and General Staff College, Colonel Elliott earned an alternate skill specialty as a SIGINT Officer. In 1982, he served with the Joint Electronic Warfare Center (JEWC). In 1993, after 11 years of successful service with the Intelligence Corps, he Branch-transferred to the MI Corps.

While assigned to the office of the DCSINT, USAREUR and Seventh Army, Colonel Elliott had a profound impact on intelligence as the Chief, Requirements Branch. He was a major force behind the successful development and restructuring of the USAREUR intelligence strategy and associated architectures for dealing with post-Cold War Europe. Colonel Elliott led the effort to identify and acquire essential, state-of-the-art intelligence systems necessary to maximize intelligence collection support throughout Europe. Among his most significant contributions in this position were—

- ❑ Fielding the Tactical Radar Correlator (a system capable of providing tactical commanders access to critical strategic-level intelligence).
- ❑ Fielding the USAREUR Imagery Exploitation System (UIES) (a system that later deployed to support Operation DESERT STORM).
- ❑ Assisting in concept and architecture development for deploying the first TROJAN Special Purpose Integrated Remote Intelligence Terminal (TROJAN SPIRIT) intelligence communications systems to the Gulf War.

Colonel (COL) Elliott culminated his European tour as the Deputy Commander, 66th MI Brigade. He ensured that despite the radical downsizing and reorganization occurring throughout the Army in the early 1990s, the 66th MI Brigade remained capable and continued to provide the outstanding intelligence support expected of its diverse units deployed throughout Germany. He repeatedly garnered recognition for providing effective solutions, which ensured mission accomplishment while minimizing turbulence.

Named the Director of Combat Developments at USAIC&FH, COL Elliott continued to build on his earlier initiatives to integrate national intelligence products into an operational architecture that allowed tactical commanders to pull the relevant information and intelligence they needed to build a common picture of the battlefield. Subsequently selected for brigade command, he served as the Garrison Commander, USAIC&FH, where he kept close and productive ties with the local civilian and military communities, was a vigilant steward of the environment, and was instrumental in Fort Huachuca's receipt of Department of the Army and Department of Energy Conservation Awards.

COL Alfred Elliott's final assignment was on the Army Staff as Chief, Intelligence and Electronic Warfare Division, Office of the Deputy Chief of Staff for Operations and Plans, Force Development, Department of the Army. His in-depth knowledge of force development and modernization processes, intelligence requirements, and his ability to balance resources resulted in a tactical intelligence modernization program under his mentorship that grew in capability. In the end, his greatest contribution may have been his ability to see the direction that Army intelligence needed to take as it headed into the 21st century and to lead us in that direction.

Colonel David A. McKnight (U.S. Army, Deceased)

Colonel David A. McKnight was a 1966 graduate of Texas Western College, today known as University of Texas at El Paso. In that same year, he joined the Army MI Branch with a detail to the Infantry. He attended the MI Officer Basic Course (OBC) and the Resident Officer Technician Course following successful graduation from the Infantry OBC. Assigned as an Infantry Officer to the Republic of Vietnam in 1967, he served as an Infantry Platoon Leader and Long-Range Reconnaissance Platoon Leader for the 1st Brigade, 101st Airborne Division. He was often credited with contributing directly to the substantial gains made by the 101st Airborne Division throughout its area of operations (AO).

COL McKnight next served with the Paris Negotiating Team seeking to end the Vietnam War. In May 1972, he returned to Southeast Asia to work as a member of the Laos Defense Attaché team. His next assignment sent him to the U.S. Military Academy at West Point, where he instructed in physical education, coached the free-fall parachute team, and taught scuba.

Receiving an early promotion to Major, he moved to the 10th Special Forces Group. He earned his Special Forces qualification, then took command of B Company, 3d Battalion, 10th Special Forces Group (A).

Reassigned to the Rapid Deployment Joint Task Force in April 1980, COL McKnight coordinated and authored the intelligence plans and documents for what became the U.S. Central Command (CENTCOM). Both Operations DESERT SHIELD and DESERT STORM validated his efforts.

Promoted to Lieutenant Colonel, he was selected for command of the 165th MI Battalion (Tactical Exploitation). Following command, he received an assignment to a sensitive Special Mission Unit as Director of Operations where he changed the unit from a reactive posture to a proactive organization, and updated and improved selection and training of personnel for their highly specialized missions. While serving as Director of Operations, he was chosen to deploy to a hostile contingency area in response to that nation's crisis in the Arabian Gulf in 1987 and 1988. He made several perilous trips into denied areas to establish effective contingency-support arrangements for potential CENTCOM operations in the area of responsibility (AOR). His accomplishments underpinned many of the successes CENTCOM achieved during subsequent operations. Colonel McKnight next participated in a Central Intelligence Agency fellowship where he served with the CIA's Office of Military Affairs.

He returned to the special operations community as DCSINT, U.S. Army Special Operations Command (SOC). From this position, he put several crucial initiatives in motion to include a tactical SIGINT collection capability, a national level method for personnel tracking, and an innovative means of collecting intelligence using special forces soldiers and equipment. During Operations DESERT SHIELD and DESERT STORM, General Steiner and General Downing chose COL McKnight to return to the CIA as U.S. Special Operations Command (USSOCOM) and Joint Special Operations Command (JSOC) Senior Liaison Officer. He provided critical and unique support to "surgical" special operations units involved in Secretary of Defense (SECDEF) operations in western Iraq. The success of these numerous incursions deep behind enemy lines to attack Iraqi capabilities in western Iraq was singularly due to his outstanding planning and coordination skills. Returning to SOC after DESERT STORM, he assumed duties as DCSINT and then Chief of Staff. Throughout his time in the special operations community, he continued to advocate initiatives for personnel tracking and recovery, beacon operations, and tactical SIGINT support and he expanded his contributions to include innovations in training and doctrine.

In March 1991, Colonel David McKnight assumed duties as J2, JSOC, and held that position until his retirement in 1994. He participated directly or indirectly in more than one hundred missions in support of SECDEF operations and directed the JSOC intelligence system through many complex joint exercises. As J2, Task Force Ranger, in Somalia, and because of his unique blend of intelligence and operational experience, he was selected to lead the first of two operational assessment teams into that troubled country. The TTPs first envisioned by him ultimately became the basis for intelligence support to surgical operations both during combat in Somalia and continuing today as a major element of special operations planning.

Command Sergeant Major John P. O'Connor (U.S. Army, Retired)

Command Sergeant Major John P. O'Connor enlisted in the Army in 1964 upon graduation from Bucknell University in Lewisburg, Pennsylvania. After school at Fort Holabird, Maryland, he became an MI Coordinator. He completed airborne qualification and moved to the 526th Intelligence Corps Detachment on the Ryukyu Islands, Japan. In 1966, he was an Intelligence Analyst with the 801st Intelligence Detachment, 6th Special Forces Group, 1st Special Forces.

In November 1967, he received his commission through Officers Candidate School. He served as the Plans Officer in the 22d Field Army Support Command. In 1968, then Lieutenant O'Connor went to Vietnam where he joined 1st Cavalry Division and served as a Rifle Platoon Leader, Reconnaissance Platoon Leader, and Executive Officer. His professional leadership and devotion to duty were rewarded after his platoon came under a well-organized attack and they were able to suppress the advancing enemy effectively. His next assignment was with E Company, 2d Battalion, 5th Cavalry, where he was again lauded for his actions during another strong enemy assault. In October 1969, Captain O'Connor assumed command of the 257th Replacement Company in Okinawa.

After a number of staff assignments in the Ryukyu Islands, he reverted to his enlisted rank of Specialist Five in 1972. Soon promoted to Staff Sergeant, he became the Senior Interrogator with the 101st MI Company, 101st Airborne Division (Air Assault). During his time with the 101st, he was the Noncommissioned Officer in Charge (NCOIC) of the Analysis and Production Section and Assistant Operations NCO, Office of the Assistant Chief of Staff, G2, and later the Intelligence NCO, 2d Squadron, 17th Cavalry. Chosen as Soldier of the Year for the Division Support Command, he was the runner-up in the 101st Division Soldier of the Year competition. During this time, he was instrumental in developing the Aggressor Assistance Team, which enjoyed notable success within the Division. He instructed at USAICS and developed training plans for several classes at the Intelligence Center. His next assignment led him to Korea in November 1976 where he served as the Intelligence Specialist for the S2 office, 1st Signal Brigade. Returning to Fort Huachuca, he became a Course Developer, Senior Faculty Advisor, and the Primary Instructor for the NCO Advanced Course.

While assigned as the Intelligence Sergeant and Tactical Surveillance NCO for the U.S. Element of the Combined Field Army, Republic of Korea, he received a promotion to Major in the U.S. Army Reserve (USAR). Returning to Fort Huachuca, he was the Senior Instructor for the Advanced Course and then the First Sergeant of A Company, 1st School Battalion, School Brigade. CSM O'Connor attended the Army Sergeants Major Academy in 1986, and remained to teach the Operations and Intelligence Course.

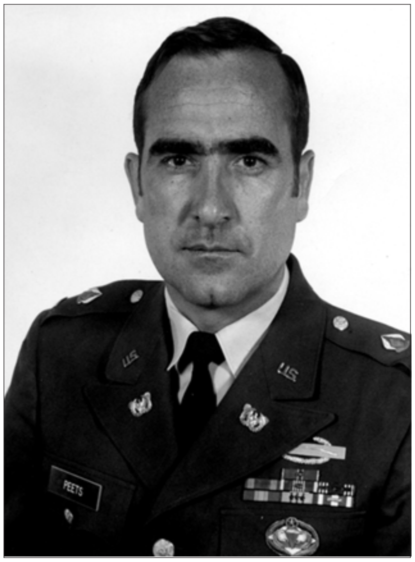
Once again, CSM John O'Connor went to Korea where he became the Command Sergeant Major of the 3d MI Battalion (Arial Exploitation [AE]). Returning to Fort Huachuca a final time in 1988, he assumed command of the Noncommissioned Officers Academy. Arguably, he made his most enduring contributions to the MI Corps while at the Academy. He revamped both the technical and philosophical policies of MI NCO training, encouraged individual thought, earned the respect of both subordinates and peers, and championed the emerging concept of small group instruction. His mentorship was evident in the many NCOs who earned advances, promotions, and recognition during his time as the Commandant. The Academy passed three intensive TRADOC accreditation inspections during his tenure. From December 1992 through his retirement in October 1994, he served as the Command Sergeant Major of the U.S. Army Garrison, Fort Huachuca.

CW4 Ben E. Peets (U.S. Army, Retired)

Chief Warrant Officer Four Ben E. Peets entered military service in January 1955. Throughout his career, he served in intelligence assignments closely aligned with airborne and special operations units. In 1966, he served as a Reconnaissance Section Leader and Brigade Intelligence Sergeant with both the 101st Airborne Division and the 1st Air Cavalry Division. During a second tour of duty in 1970 with the 101st Airborne Division in Vietnam, he served as the Chief, Special Operations Center. During this assignment, he was chosen for appointment as one of the first warrant officers in the newly created order of battle (OB) technician career field.

CW4 Peets' assignments included a tour of duty with the XVIII Airborne Corps where he served as an OB Technician, Detachment Operations Officer, CI Technician, and as the Chief of the All-Source Intelligence Center. While assigned to the 3d Armored Division from 1975 until 1978, he served as the Officer in Charge of the Division Operations and Intelligence Center. Of significance during this assignment, analysts under his direction produced and published the standardized guide to Soviet OB for the 3d Armor Division AO. Upon his return to Fort Bragg in 1978, then CW3 Peets received the task of assembling a program of instruction (POI) for a special forces operations and intelligence (O&I) course. His direct personal involvement in the development of the O&I curriculum had direct and permanent impact on how special forces personnel collect and process critical tactical and operational intelligence today.

In October 1983, CW4 Peets retired from the active Army and ac-



cepted a Department of the Army civil service intelligence position in the newly formed JSOC. During his more that 15 years with JSOC, Mr. Peets served in multiple positions in the J2, including Analyst, Senior Analyst, Branch Chief, Division Chief of two different divisions, and as the Deputy J2 for Plans, Programs and Budget for the Directorate. During this time, he repeatedly earned commendation for his efforts in educating and developing a new generation of special operations intelligence personnel.

CW4 Ben Peets played a central role in a number of JSOC operations under the direction of various national intelligence agencies and SOC. Of special note is the Integrated Survey Program (ISP) he designed and developed specifically to support the highly specialized planning and execution of complex special operations missions. He was personally responsible for its integration into a highly automated production and dissemination system. CW4 Peets continued to serve with distinction in the JSOC J2 Directorate until his retirement from civil service in April 1999.

Major General John D. Thomas, Jr. (U.S. Army, Retired)

Major General John D. Thomas, Jr., enlisted as a private in 1968 and earned his commission following his graduation as Distinguished Graduate from the Field Artillery Officer Candidate School. His initial assignments included command and staff positions in both the 7th and 2d Infantry Divisions. He then commanded an Advanced Individual Training (AIT) Company. Following his completion of the Army Basic Cryptologic and Electronic Warfare Officers Course and the Military Intelligence Officer Advanced Course, he went to Field Station Augsburg. Following service as Executive Officer, 1st Army Security Aviation Company, he commanded C Company (Guardrail), 15th MI Battalion (AE), 504th MI Brigade. Following graduation from the Armed Forces Staff College, he served in intelligence and electronic warfare staff positions at the Combined Forces Command and U.S. Forces, Korea (USFK), and on the Department of the Army Staff.

MG Thomas assumed command of the 3d MI Battalion (AE), 501st MI Brigade, at Camp Humphreys, Korea. Following graduation from the National War College, he became the Deputy Chief for Intelligence at the Special Technical Operations Division, J3, on the Joint Staff in Washington, D.C.

MG Thomas then assumed command of the 111th MI Brigade. While in command, he—

- ❑ Spearheaded the development of the Joint Unmanned Aerial Vehicle (JUAV) Testing Company.
- ❑ Championed training the Pioneer Unmanned Aerial Vehicle (UAV) as the Army's near-term answer to over-the-hill reconnaissance.
- ❑ Pressed for full integration of the lessons learned from Operations DESERT SHIELD and DESERT STORM into the Intelligence Center curriculum.
- ❑ Led the organization and training of the Brigade UAV Company that deployed to Operation DESERT STORM and provided aerial reconnaissance support to the VII (US) Corps.

He earned selection for General Officer rank and served as Deputy Commanding General and Assistant Commandant, USAIC&FH. While serving in this position, he organized an operational test for the All-Source Analysis System that resulted in the fielding of ASAS Armywide.

He next served as the Associate Deputy Director for Operations (Military Support) at the National Security Agency (NSA) and as Deputy Chief, Central Security Service. He was able to directly influence the tasking of national intelligence collection to ensure that combatant commanders around the world received timely and accurate intelligence support. His efforts paid off during successful support operations in Somalia, Iraq, Bosnia-Herzegovina, and Haiti. In August 1996, he assumed command of INSCOM where he developed new concepts for intelligence support to operational commanders and significantly enhanced the capability of the U.S. Army Land Information Warfare Activity (LIWA). In June 1998, he returned to USAIC&FH as the Commanding General.

During his career, MG John Thomas remained an inspiration to the entire MI Corps. He successfully positioned Army Intelligence for the 21st century. He provided personal mentoring and oversaw the training of literally thousands of Army intelligence soldiers. He championed changes in intelligence collection strategies that eliminated historical single-discipline "stovepipes." He spearheaded the conceptual development of the Distributed Common Ground Station-Army (DCGS-A), reshaped the future of tactical ground SIGINT collection with his vision for the Prophet system, and led the development of the Shadow UAV as the Army's organic brigade-level UAV. Most importantly, he developed Army Intelligence's transformation strategy for unifying intelligence, surveillance, and reconnaissance (ISR) activities on the battlefield and provided the framework for processor integration. His efforts led to the identification of information as an element of combat power and to the facilitation of the Army's transformation to the Objective Force. The MI Corps will clearly feel Major General Thomas' contributions for many years to come.

Captain Humbert R. Versace (U.S. Army, Deceased), United States Medal of Honor Recipient

Captain Humbert Rocque Versace graduated from the U.S. Military Academy in 1959 and received a commission in Armor Branch. He attended Ranger School and Airborne School where he earned the parachutist badge. He served with 3/40 Armor, 1st Cavalry Division, and the 3d Infantry (Old Guard).

CPT Versace volunteered for duty in Vietnam; he attended the Intelligence Course at the Military Assistance Institute at Fort Holabird, Maryland, and the Vietnamese language course. On 12 May 1962, he became an Intelligence Advisor in Long Kanh Province, III Republic of Vietnam (RVN) Corps (Xuan Loc). Subsequently reassigned to the Staff Advisory Branch, 5th Infantry Division, III (RVN) Corps (Bien Hoa), he served as the Assistant G2 Advisor. Following the completion of his initial 12-month tour, CPT Versace extended his tour for an additional six months, moving to Advisory Team 70 as Intelligence Advisor to Civil Defense and Self-Defense Forces operating in An Xuyen Province (IV Corps Tactical Zone) in the Mekong Delta region of South Vietnam. It was in this last assignment that Captain Versace was wounded and captured with two other Special Forces soldiers on 29 October 1963, while on an operation with Special Forces Team A-23 at Tan Phu on the edge of the U Minh Forest.

Upon arrival in the Viet Cong (VC) prison camp, Captain Versace assumed command as senior prisoner to represent his fellow U.S. captives. His captors immediately labeled him a troublemaker for insisting that they honor the Geneva Convention's protections for captured prisoners of war (POWs). The Viet Cong did not acknowledge any protections guaranteed to prisoners as required by the Geneva Convention, and considered the three U.S. prisoners "war criminals."

The VC soon kept CPT Versace in an isolation hut with thatch on the roof and sides, which made mid-day temperatures inside as hot as an oven. The Department of Defense (DOD) Prisoner and Missing Personnel Office stated that:

> *...Captain Versace demonstrated exceptional leadership by communicating positively to his fellow prisoners. He lifted morale when he passed messages by singing them into the popular songs of the day. When he used his Vietnamese language skills to protest improper treatment to the guards, Captain Versace was again put into leg irons and gagged.*

He took advantage of his first opportunity to escape, dragging himself on his hands and knees out of the camp through dense swamp and forbidding vegetation to freedom. The guards quickly discovered him outside the camp and recaptured him. After recapture, Versace was returned to leg irons and his wounds left untreated. They put him on a starvation diet of rice and salt. During this period, VC guards told other U.S. prisoners that despite beatings, Captain Versace refused to give in.

At the end, their captors often moved him away from his fellow prisoners. According to Brigadier General Nicholson, who participated in the numerous operations launched to free Versace, his fellow prisoners, others, and villagers reported that CPT Versace not only resisted the VC attempts to get him to admit war crimes and aggression but also verbally and convincingly countered their assertions in a loud voice so that those around him could hear his resistance. Their captors ultimately executed him 26 September 1965.

Captain Versace was posthumously awarded the nation's highest award for military valor, the U.S. Medal of Honor, on 8 July 2002. A fellow POW, an Alexandria-based group of friends, classmates from the U.S. Military Academy, the Army's Special Forces Command, and a devoted researcher struggled for 30 years to secure this honor for CPT Versace. According to retired Lieutenant General Howard G. Crowell, Jr., who bunked with him in Vietnam, "*He was so eager to accomplish his mission of gathering intelligence that it was bound to get him into trouble sooner or later."* Unlike the Air Force, Navy, and Marines, the Army had never before awarded the Medal of Honor to a POW from Vietnam for heroism during captivity. "Rocky" Versace won the Medal for every day of his 23 months in captivity.

(Continued on page 71)

112th Training Notes

112th MI Brigade (Provisional) Training Notes

by George A. VanOtten, Ph.D.

by George A. VanOtten, Ph.D.

The 112th Military Intelligence (MI) Brigade (Provisional) is working a plethora of training activities, innovations, and initiatives. These include the highly intensive training missions of the 304th and 306th MI Battalions.

The 306th MI Battalion is responsible for training the Striker Brigade Combat Teams (SBCTs). To date, the 306th has completed two iterations of SBCT training and will begin the third iteration in the summer of 2003. The 306th is also actively engaged in developing a five-week course designed to prepare military intelligence professionals to combat terrorism effectively. (See the article in page 52.) The first group of students began this course of study in January 2003. The Functional Course Division of the 306th MI Battalion is responsible for the coordination, development, and implementation of this course. Numerous other organizations and agencies including (but not limited to) the University of Arizona, the Defense Intelligence Agency the 304th MI Battalion, and the 111th MI Brigade are providing valuable assistance. In addition, the 306th will continue to accomplish its regular training mission, which includes teaching a wide range of specialized courses by the Functional Course Division.

The 304th MI Battalion is responsible for MI Officer and Warrant Officer training. The 304th also teaches some specialized courses including the Staff Weather Officer Course (SWO) designed to prepare U.S. Air Force weather officers to operate in a typical Army field environment. Currently, the 304th MI Battalion is intensely involved in working with the U.S. Army Training and Doctrine Command (TRADOC) to develop the MI portions of the new Officer Education System (OES). While this endeavor remains a work in progress, it is clear that the OES will bring major changes in the training and education of MI officers.

As part of its commitment to finding the most effective and innovative ways to train and educate the force, the leadership of the 304th MI Battalion has established an Intelligence Combat Training Center (ICTC). The ICTC is a digital tactical operations center (DTOC) that allows MI professionals to develop and test their analytical, digital, communications, leadership, and decisionmaking skills through exercises designed to reflect the contemporary operational environment (COE). Contractors are now modifying the basic Caspian Sea Scenario for use in the ICTC.

George VanOtten is currently the Dean, 112th MI Brigade (Provisional) (Advanced Training and Education) at the U.S. Army Intelligence Center and Fort Huachuca in Arizona. He has a Master of Science degree in Education and Doctor of Philosophy degree. Readers may contact Dr. Van Otten via E-mail at george.vanotten@hua.army.mil and by telephone at (520) 538-7303 or DSN 879-7303.

Hall of Fame

(Continued from page 70)

While not commissioned into Military Intelligence, Captain Humbert Versace served much of his all too short Army career and, specifically, his final tour of duty in the Republic of Vietnam performing the duties of an intelligence officer. His total commitment to Army values and the attributes of the MI Corps continue to be an example of heroism and professional leadership for another generation of MI professionals to both honor and emulate him.

MI Corps Hall of Fame Nominations

The time is fast approaching to begin the selection process for the 2004 MI Corps Hall of Fame (HOF) inductees. We want to again recognize enlisted soldiers, warrant officers, commissioned officers, and civilian professionals who have made a significant contribution to the MI Corps. The 2004 HOF Nomination Board will meet this fall to consider new nominations; it is not too early to start preparing a nomination package today. You can obtain a sample nomination packet and instructions by sending a request in writing to Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-MI (23), Fort Huachuca, AZ 85613-7080 or by calling (520) 533-1173 or DSN 821-1173. You may send E-mail requests directly to OCMI@hua.army.mil.

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, TTPs, 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 it, quotations from senior leaders describing how good it 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 **jonell.elkins@us.army.mil** and **liz.mcgovern@us.army.mil** or mail (with a soft copy on disk) to Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-FDT-M, 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, and ASCII; we need the graphics in Adobe, tif, jpg, 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 (see page 61).
- ❑ 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 in the article text.
- ❑ 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. (Please indicate whether we can print your telephone number and your E-mail address with the biography.)

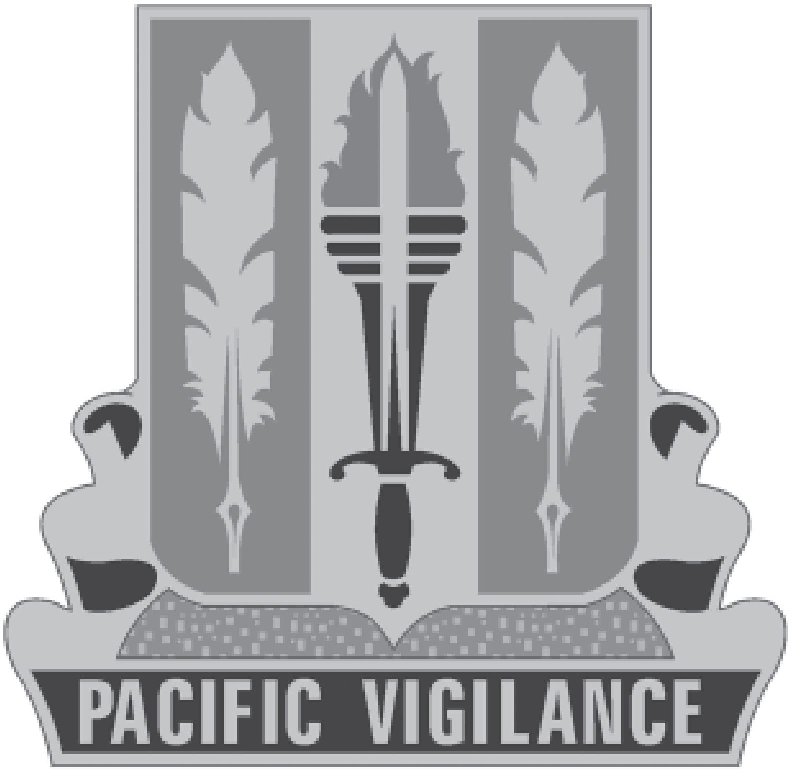
We cannot guarantee we will publish all submitted articles but will send you a message acknowledging its receipt. We may notify you again when we get ready to publish it. Please inform us of any changes in contact information as it can take a year or more before we publish some articles.

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

Military Intelligence Professional Bulletin
Upcoming Themes and Deadlines
for Article Submission

Issue	Theme	Deadline
Jul-Sep 03	Information Operations	5 Apr 03
All	Global War on Terrorism	
	Signals Intelligence	
	Imagery Intelligence	
	Intelligence Operations in Iraq	

205th Military Intelligence Battalion



Oriental blue and silver gray are the colors traditionally associated with Military Intelligence units. Blue conveys devotion and loyalty, red is indicative of courage and zeal, while white portrays integrity. Gold reflects excellence, achievement, and high ideals. Black reflects covert capabilities. The quills symbolize the unit's analytical functions; the torch signifies guidance, leadership, and knowledge; and the sword is symbolic of military preparedness. The lightning flash indicates both speed and accuracy and alludes to the Battalion's heritage and association with the Signal Corps. It is red to indicate the Meritorious Unit Commendation received by the unit during World War II. The palm fronds stand for victory while the Oriental dragon personifies vigilance and preparedness. They suggest the Pacific Theater and reflect the unit's motto.

The unit first activated as the 2d Signal Service Company on 1 January 1939 at Fort Monmouth, New Jersey. The company integrated all intercept personnel of the Army's Signal Intelligence Service (SIS) into one unit. Company detachments were at several stations in the continental United States (CONUS), Panama, Hawaii, and the Philippine Islands. The company conducted the mission of obtaining the signals intelligence (SIGINT) required by the SIS.

In March 1940, as the tempo of defense activity accelerated, the company headquarters moved to Washington, D.C., bringing it nearer to SIS headquarters. Eight months later, with greater emphasis placed on the activity of the SIS, the Signal Service Company redesignated as the 2d Signal Service Battalion.

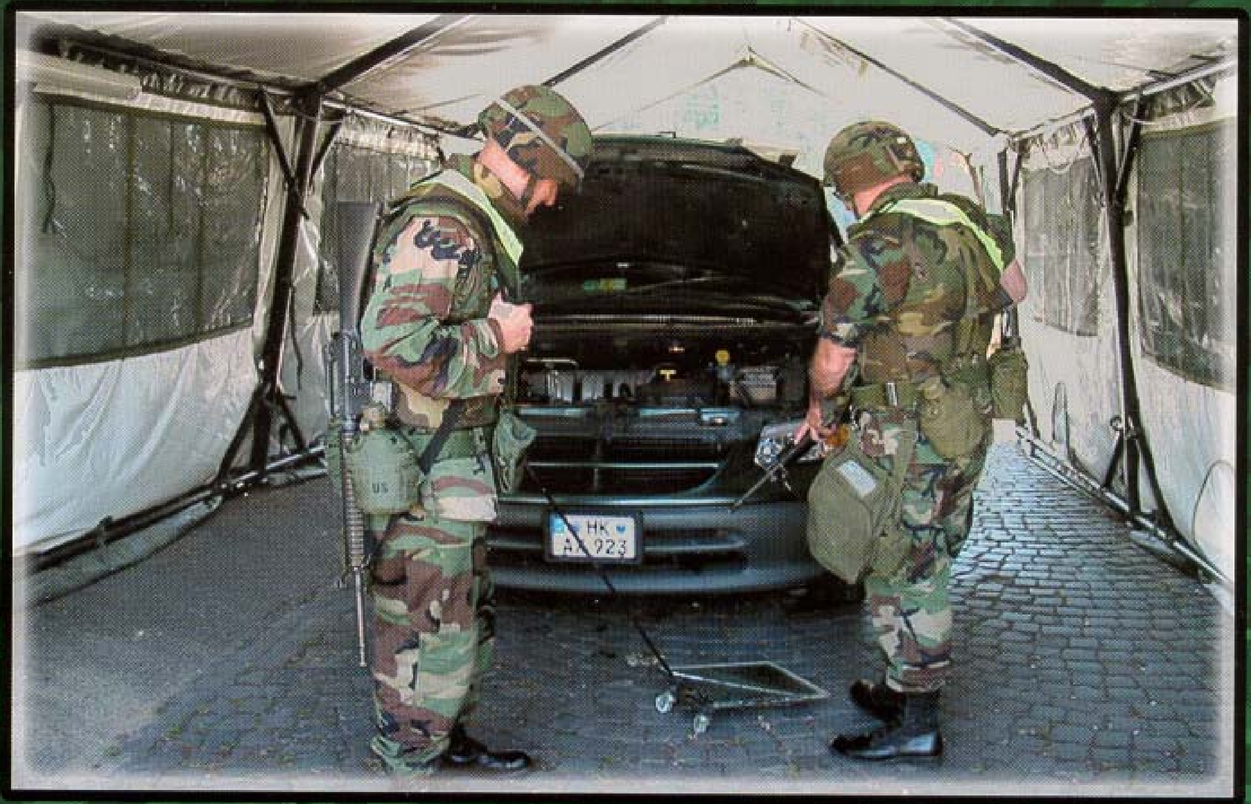
The United States' entry into World War II produced an increased number of stations. By the end of WWII, the 2d Signal Service Battalion comprised more than five thousand personnel assigned at both Arlington Hall Station (headquarters of the Signal Security Agency, SIS's successor organization) and monitoring stations worldwide. The commander of the Signal Security Agency also served as the battalion commander.

Resulting from the formation of the Army Security Agency (ASA) 20 April 1946, Headquarters Company, 2d Signal Service Battalion redesigned as Headquarters and Headquarters Company, Arlington Hall Station. Detachments of the battalion continued to operate field stations in CONUS and overseas until May 1950, when the Army disbanded the Battalion.

The Battalion reconstituted, reorganized, and redesignated as the 205th Military Intelligence Battalion effective 15 October 1992. The Battalion headquarters is at Fort Shafter, Hawaii, and subordinate elements are at Fort Richardson, Alaska; Kwajalein Atoll, Republic of the Marshall Islands; Fort Lewis, Washington; Phoenix, Arizona; and at three locations on the island of Oahu. In October 2001, the Army designated the 205th MI Battalion as a multi-component unit. 205th MI Battalion deployed teams to East Timor in support of Operation STABILISE in 1998 and 1999. In October 2001, the 205th MI Battalion deployed soldiers to combat operations in support of Operation ENDURING FREEDOM in Uzbekistan and Afghanistan, while simultaneously supporting Operations NOBLE EAGLE and ENDURING FREEDOM - Philippines.

PACIFIC VIGILANCE … EYES OF THE WARRIOR!

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



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

PIN 080604-000