MIPB

Military Intelligence Professional Bulletin

July-September
2007
PB 34-07-3

FROM THE EDITOR

This issue's focus is on GEOINT with a varied range of topics. There are several articles from the National Geospatial-Intelligence Agency (NGA), briefly describing such products as the Commercial Joint Mapping Toolkit (CJMTK) and Geospatial Intelligence for Operations support and the Battlefield, or GIB. The CJMTK leverages commercial-off-the-shelf technologies to provide the warfighter with a standardized geospatial visualization tool. The GIB gives users the ability to manipulate "layers" of data to create a customized and fused view of their surroundings. Another NGA article describes some of the training support provided by the Army's NGA Support Teams, in this case FalconView™ training.

Colonel Crabtree, from TRADOC TPIO-Terrain Data describes geospatial engineering and the emerging partnership between geospatial engineers and imagery analysts that will provide the most complete common operational picture for the warfighter.

We have two training related articles, describing the revamping of the MOSs 96D10 (Imagery Analyst) and the MOS 35M (HUMINT Collector) Courses taught here at Fort Huachuca.

From another arena, Vince Cattera and Patrick Ahrens discuss the mission of the Army Broadcast Intelligence Office (ABIO). The ABIO manages the Integrated Broadcast Service (IBS) which provides time-critical and actionable intelligence data to the tactical force.

Be sure to check out the Army G2 IT Note to the Field on our FOUO website at http://www.universityofmiltaryintelligence.us/mipb. It is packed with information on available imagery and geospatial exploitation tools and POCs for acquisition and training.

We have resumed printing! If your unit or agency would like to receive MIPB at no cost, please send an email to sterilla.smith@conus.army.mil including a physical address and quantity desired or call me at 520.538.0956/DSN 879.0956. We are no longer accepting personal subscriptions.

Sterilla A. Smith

Sterilla A. Smith
Editor

MILITARY INTELLIGENCE

PB 34-07-3 Volume 33 Number 3 July - September 2007

Commanding General
Major General John M. Custer III

Deputy Commanding General, Reserve Component
Brigadier General Edward A. Leacock

Deputy Commandant for Futures
Mr. Jerry V. Proctor

Deputy Commander for Training
Colonel James G. Rose

Director, Directorate of Doctrine
Colonel Mark R. Wallace

Chief, ISR Operations Analysis Division
Mr. Chet Brown

MIPB Staff:

Editor
Sterilla A. Smith

Design Director
Sharon K. Nieto

Associate Design Director/NCOIC
SFC Philip M. MacCluskey

Design and Layout
SSG Patrick N. Franklin

Cover Design
SFC Philip M. MacCluskey

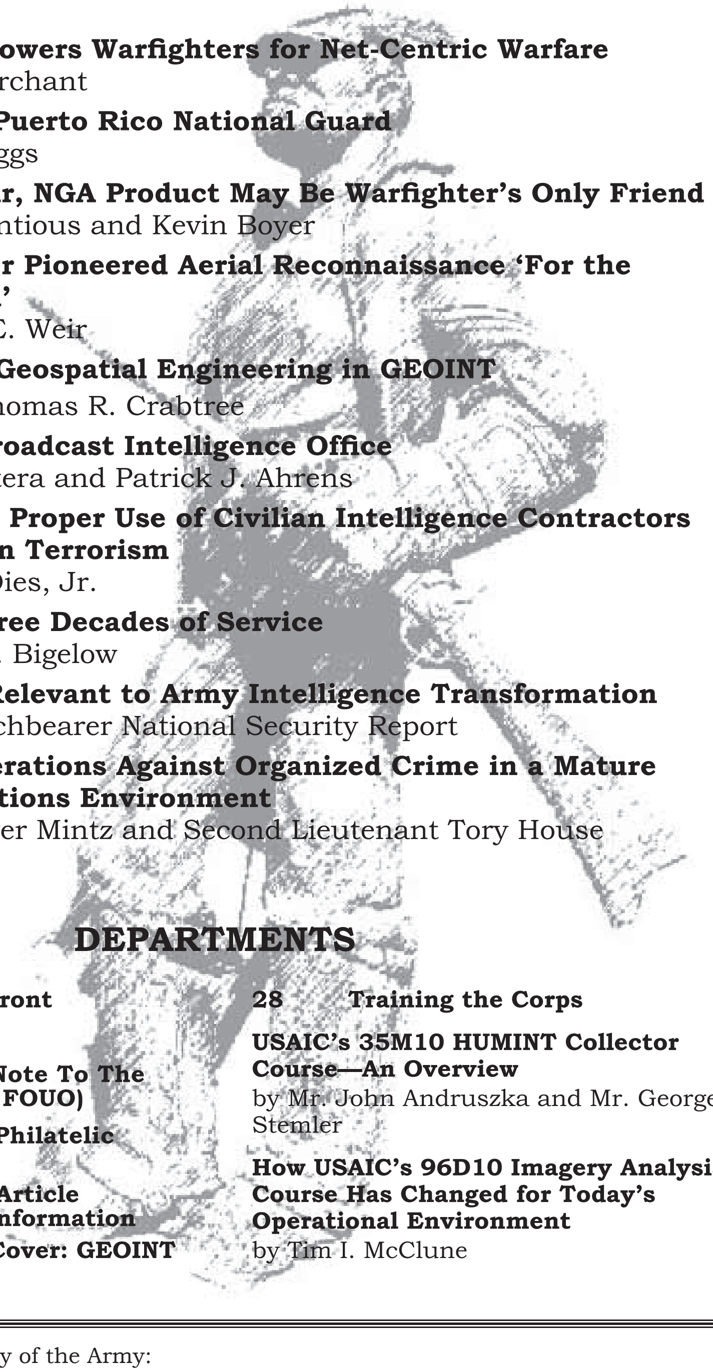
Inside Back Cover:
SFC Philip M. MacCluskey

Issue Photographs:
Courtesy of the U.S. Army

Purpose: The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) publishes the **Military Intelligence Professional Bulletin** (**MIPB**) quarterly under the provisions of **AR 25-30**. **MIPB** presents information designed to keep intelligence professionals informed of current and emerging developments within the field and provides an open forum in which ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, etc., can be exchanged and discussed for purposes of professional development.

Disclaimer: Views expressed are those of the authors and not those of the Department of Defense or its elements. The contents do not necessarily reflect official U.S. Army positions and do not change or supersede information in any other U.S. Army publications.

FEATURES



DEPARTMENTS

By order of the Secretary of the Army:
Official:

Joyce E. Morrow

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0717301

GEORGE W. CASEY JR.
General, United States Army
Chief of Staff

Always Out Front

by Major General John M. Custer III
Commanding General
U.S. Army Intelligence Center and Fort Huachuca

In recent issues of MIPB you may have noticed an increasing number of articles on Geospatial Intelligence (GEOINT). This reflects the U.S. Army Intelligence Center's (USAIC) recognition that our mission is constantly evolving to improve our support to the warfighter. In February 2006, GEOINT was designated as an Army Intelligence discipline and is currently undergoing a full functional review through a Cradle-to-Grave (C2G) analysis. The C2G is assessing GEOINT and Imagery Intelligence (IMINT) throughout the domains of Doctrine, Organization, Training, Materiel, Leader Development, Personnel, and Facilities (DOTMLPF) to:

- Identify problem areas.
- Develop solutions.
- Identify decisions.
- Facilitate integrated solutions.

Our C2G effort is being done in coordination with a wide range of GEOINT players to include the National Geospatial-Intelligence Agency (NGA), the U.S. Army Intelligence and Security Command, the U.S. Army Engineer School (USAES), the U.S. Army Training and Doctrine Command (TRADOC), and various tactical users. The results of our C2G assessment and pending actions include—

Doctrine. USAIC is writing emerging GEOINT doctrine that is fully coordinated with USAES, the other Armed Services, and NGA. GEOINT doctrine will further describe what it is, who does it, how it is done, and how it will support the operational environment. GEOINT doctrine will be incorporated in the following manuals:

- **FM 2-22.11/3-34.630, Geospatial Intelligence (GEOINT)**.
- **FM 2-22.5, Imagery Intelligence**.
- **FM 2-01.3/MRCP-2-3A, Intelligence Preparation of the Battlefield (IPB)**.
- **FMI 2-01.301, Specific Tactics, Techniques, Procedures, and Applications of IPB.**
- **FM 2-33.4, Intelligence Analysis**.
- **FM 2-0, Intelligence**.
- **FM 3-24, Counterinsurgency**.

Organization. USAIC (in full coordination with USAES) designed and proposed GEOINT structures at the brigade through Army Service Component levels to facilitate information sharing and GEOINT production. If approved, the proposals will result in changes to Tables of Organization and Equipment (TOEs) and subsequently, how we do business.

Training. Here at USAIC, we are enhancing our MOSs 96D/35G (Imagery Analyst) and 96H/35H (Common Ground Station Operator) training to meet evolving mission requirements as documented during our lessons learned collection effort and Critical Task Site Selection Board process. Based on lessons learned from the field we are adding Advanced Geospatial Imagery (AGI), Full Motion Video (FMV), Imagery Exploitation Support System (IESS) functions, and Moving Target Indicator (MTI) familiarization to our 96D/35G training. We have added MTI forensics and FMV familiarization training for MOS

(Continued on page 4)

CSM Forum

by Command Sergeant Major Franklin A. Saunders
Command Sergeant Major
U.S. Army Intelligence Center and Fort Huachuca

MI MOS Update AUGUST 2007

MOS Mergers at the E-8 Level

The Office of the Chief, Military Intelligence (OCMI) staffed an action with the Department of the Army (DA) that will consolidate/cap the following military occupational specialties (MOSs):

35F (96B) Intelligence Analyst
35G (96D) Imagery Analyst
35H (96H) Common Ground Station Operator

at E-8 in MOS 35X (96Z)

35L (97B) Counterintelligence (CI) Agent
35M (97E) Human Intelligence (HUMINT) Collector

at E-8 in MOS 35Y (97Z)

Consolidation of these MOSs at E-8 vice E-9 will improve grade structure and provide more equitable promotions. The consolidated E-8 positions have been loaded into the enlisted distribution and assignment system (EDAS) allowing eligible E-7s in MOS 35F (96B), 35G (96D), and 35H (96H) to be considered for promotion to E-8 in MOS 35X (96Z) and eligible E-7s in MOS 35L (97B) and 35M (97E) to be considered for promotion to E-8 in MOS 35Y during the next E-8 board. This change in MOS structure will be addressed by OCMI in its guidance to the promotion board.

HUMINT NCO Special Recruiting Program

Currently, we have 14 Soldiers attending our initial class that began on 14 May 2007. Thirty six Soldiers were selected to attend the next class which began 20 August 2007. An additional class will be added to this program and is currently scheduled for February 2008. We are reopening the window for submission of applications for Soldiers who are interested in attending this class. The deadline for submission of these packets to OCMI is 15 September 2007. Interested applicants should go to the HQDA G2 Sergeant Major's website for more information on this class at http://www.dami.army.pentagon.mil/sgm/index.asp.

MOS 98C BNCOC

Starting in September 2007, the training and access to the National Security Agency's (NSA) databases during BNCOC will require ALL 98C students to complete the ANNEX P process and obtain a Personal Key Identifier (PKI). In addition, all students must have an up-to-date (not older than 5 years) polygraph. If the polygraph cannot be accomplished in time, the Soldier must download, complete, and sign a Pre-Polygraph CSP Consent Form as a waiver for access to the NSA databases. Please make sure that if you have NCOs attending this course that they are aware of and comply with these requirements. For additional information please contact SFC Daryl McNeil, 98C Senior Instructor at daryl.mcneil@us.army.mil or (520) 533-6198/(DSN) 821-6198.

(Continued on page 5)

(Continued from page 2)

96H/35H. Upon acquiring additional resources, we will expand 96D/35G training to ensure we more thoroughly train these new skills.

Our 96D/35G and 96H/35H Skill Level 10 through 40 soldiers, warrant officers and officers are exposed to division level GEOINT operations during their final course exercises at our Joint Intelligence-Combat Training Center (JI-CTC) conducted in a collaborative intelligence environment with students from Human Intelligence, Counterintelligence, Measurement and Signature Intelligence, Signals Intelligence, and All-source disciplines using a dynamic, real-world scenario. Skills trained and reinforced in the JI-CTC GEOINT training are:

- FMV exploitation.
- Unmanned Aerial System (UAS) flight operations and mission planning.
- Joint Surveillance Target Acquisition Radar System (J-STARS) MTI exploitation.
- Cross-cueing of assets with emphasis on UAS and MTI.
- Report writing hyperlinked to Imagery Derived Product (IDP), in concert with the Army Distributed Common Ground Station (DCGS-A), video clips of action from UAS and/or MTI, advanced mapping products, etc.
- National and Remote Sensing (Commercial) exploitation.
- Section Leader duty responsibilities.
- Fast-paced, first phase Tactical Identification and Ground Order-of-Battle analysis.
- Briefing skills.
- Communications systems and Common Operational Picture (COP) development.
- Field Artillery Intelligence Officer (FAIO) interaction
- Battle Damage Assessment (BDA).
- Brigade Combat Team commander support operations.
- AGI and DCGS-A GEOINT toolsets and applications.

JI-CTC GEOINT training today includes sister Services and deploying NGA personnel. In coordination with the USAES, we will soon expand our training to include selected Engineer Geospatial Analysts.

Materiel. We are closely tracking the development of emerging GEOINT capabilities for integration into our current and future processing and collection capabilities. With our transition to DCGS-A, our TRADOC Capabilities Manager Sensor Processing (TCM-SP) is integrating Engineer and Imagery Analyst tool sets. The Engineers Digital Topographic Support System (DTSS) will be integrated into DCGS-A operations beginning in 2008. Part of our materiel tracking includes ensuring that all future fielded systems have an embedded means to train Intelligence Soldiers with realistic simulations or systems replication tools.

Leadership. There are multiple leader skills one needs to understand to fully exploit GEOINT and all its components–Imagery, IMINT and Geospatial Information and Services (GI&S). We are analyzing these skills, reviewing what and where we currently train, and looking towards expanding and updating our training.

Personnel. Along with possible organizational changes we are looking at what MOSs we will need for the future. The first changes are in our MOSs 96H/35H and 96D/35G. With the transition of CGS from a stand alone station to its inclusion into DSGS-A, we need a blending of skill sets for those soldiers performing their mission on a DCGS-A system. In addition, our lessons learned collection tells us that commanders need more Imagery Analysts to keep up with the increased reliance on FMV. Adaptive commanders and Soldiers are already using MOS 96H/35H Soldiers to perform Imagery Analysis. In addition to cross training 96D/35Gs and 96H/35Hs, we have proposed merging these MOSs by FY 2011 and provide reclassification training for 96H/35Hs to become 96D/35Gs. Reclassification training is currently planned to last ten weeks.

Other personnel changes include a detailed examination of our Area of Concentration (AOC) 35C, Imagery Intelligence Officer. We are determining if GEOINT assignments will increase the requirement for AOC 35C, whether we need to expand the skill sets of our 35C officers beyond just imagery management, or whether the AOC 35C should be a skill identifier (SI) and taught to only those projected to go to an IMINT assignment.

Facilities. While Army wide GEOINT does not require new facilities, we are examining whether GEOINT training facilities are adequate. We are working the implications of GEOINT daily, and push decisions and issues to the forefront so they can be acted upon. We will continue our C2G effort until we get GEOINT to a place where it permeates our Intelligence DOTMLPF responsibilities.

What does this new discipline GEOINT mean to the warfighter? It means that our analysts will continue to produce the products they produce today, but will also be able to provide more detailed, accurate, timely, and relevant visualization products to the war fighter at all echelons. It also means that our leaders and analysts will have more adaptive skills and tools to allow them to do even more than they do today, to further increase their contribution to victory.

Always Out Front!

(Continued from page 3)

CSM Forum

MOS 98GA

There are 38 Soldiers within our ranks that still hold the MOS 98GA. Please make sure that these Soldiers are working with their career counselor in exploring their reclassification options before the Army chooses an MOS for them.

MOS 98C/Y (35N/S) Transition Training

Continue to send your 98C/Y Soldiers to transition training. Information on the following classes can be found in ATTRS at https://www.atrrs.army.mil/atrrscc/.

- ✦ 232-98C1/2/3/4 (98C) (T) 98C to 98C Transition 4 Weeks (Fort Huachuca, Arizona), 1,314 98C Soldiers still show in EDAS as needing Transition Training as of July 2007.
- ✦ 233-98Y1/2/3/4 (98K) (T) 98K to 98Y Transition 7 Weeks (Fort Huachuca, Arizona), 294 98Y Soldiers still show in EDAS as needing Transition Training.
- ✦ 232-98C1/2/3/4 (98J) (T) 98J to 98C Transition 7 Weeks (Goodfellow AFB, Texas), 152 98C Soldiers still show in EDAS as needing Transition Training.
- ✦ 233-98Y1/2/3/4 (98J) (T) 98J to 98Y Transition 16 Weeks 2 Days (Corry Station, Florida), 168 98Y Soldiers still show in EDAS as needing Transition Training.

The previous Commanding General (CG), U.S. Army Intelligence Center and Fort Huachuca (USAIC and FH), MG Fast approved the U.S. Army Intelligence and Security Command's Alternative Transition Training courses listed below. Upon completion of this alternate training, the unit S3/G3 must forward a memorandum to OCMI stating that Soldier has completed the required courses. The memorandum must include Soldier's name, SSN, MOS, and date that training was completed and can be faxed to OCMI at (520) 533-1186, DSN 821-1186 or emailed to SFC Teddy Woods at teddy.woods@us.army.mil.

- ✦ MOS 98Cs (former 98Cs who need OPELINT skills) can attend FUSE 1100 and SIGE3110DV to receive credit for transition training.
- ✦ MOS 98Ys (Former 98Ks only) can attend MATH1030, and SIGE2810 to receive credit for transition training.

STAR MOS List (As of July 2007)

After 31 months on the STAR MOS list at E-6, MOS 96D has been removed. This is good news, however attention still needs to be given to this issue especially with MOSs 96B, 97B, and 97E.

E-5 MOS	# Needed	# of Eligible Soldiers that could be boarded	Primary Zone	Secondary Zone	Months on List
09L	30	22	0	22	9
96D	17	57	36	21	24

In addition 98G is a STAR MOS at Skill Level (SL) 2 in the following languages: Indonesian, Pashtu, Hebrew, Portuguese, and Vietnamese.

E-6 MOS	# Needed	# of Eligible Soldiers that could be boarded	Primary Zone	Secondary Zone	Months on List
09L	22	0	0	0	9
33W	2	117	30	87	3
96B	290	589	139	450	40
97B	85	162	30	132	22
97E	332	324	72	252	37
98C	11	371	47	324	12

98G STAR at SL 3 in Arabic, French, Hebrew, German, Korean, Indonesian, Persian-Farsi, Portuguese, Pashtu, Russian, Tagalog, Thai, and Urdu.

MI MOS Data Updated on COOL Website

The Credentialing Opportunities On-Line (COOL) website has been updated to reflect criteria for certification programs that qualify for specified MOS promotion points. For more information go to the COOL website and review the fact sheet at https://www.cool.army.mil/pubs/promoPointsFactSheet.pdf. Additional information can be found at the HRC Technical Certification Matrixes link at https://www.hrc.army.mil/site/active/select/techCert.htm and the search link for each MOS at https://www.cool.army.mil/search.htm.

MOS 09L

A Force Design Update (FDU) that will stand up two companies with 149 09L Soldiers per company has been approved by the Vice Chief of Staff Army. This FDU creates force structure for this MOS through the rank of E-8.

MOS 35G (96D)

A proposal for MOS (35G) 96D to assume all duties, functions, positions and personnel from MOS (35H) 96H is included in the fiscal year (FY) 2007 Military Occupational Classification and Structure (MOCS) submission (for implementation in FY 2011). The previous CG, USAIC and FH, approved the creation of an additional skill identifier (ASI) for use with MOS 35G to identify Common Ground Station operators when MOS 35G assumes the functions of MOS 35H. Former 35H Soldiers will be awarded this ASI upon reclassification to MOS 96H.

MOS 35H (96H)

The previous CG, USAIC and FH, also approved a 10 week reclassification course for 96Hs to become 96Ds as a result of an earlier decision approving the recommendation to recode and reclassify 96H Soldiers and positions to MOS 96D and subsequently delete 96H. The creation of an ASI for use with MOS 35G (96D) to identify CGS operators has also been approved.

MOS 35K (FY 2008) and 15W (FY 2009) (96U)

The FY 2007 MOCS contains a proposal that MOS 96U Soldiers must complete an Army Class III medical physical prior to arrival at training base. Additionally, they must annually maintain this Class III medical physical. The proposal also states that Soldiers in this MOS are not required to complete or pass the Type II decompression sickness/chamber training requirement.

MOS 35L (97B)

We need to ensure every effort is taken to send qualified 35L (97B) Soldiers in the rank of E-5 to the promotion board at their earliest eligibility. Promoting qualified E-5s to E-6s will help the overall MOS health by improving our strengths at E-6 and decreasing our on-hand strengths at E-5, allowing for the promotion of remaining 460 SL10 Soldiers.

MOS 35M (97E)

Effective 1 October 2012, a TOP SECRET (TS) clearance with Sensitive Compartmented Information (SCI) access eligibility is required to hold this MOS. Effective 1 October 2008, all Soldiers accessing into MOS will be submitted for TS clearance and SCI access eligibility.

A five-year language suspension for 97E Soldiers in the U.S. Army Reserves (USAR) has been approved by HQDA in a memorandum dated 19 May 2007. This suspension remains in effect until 1 April 2012. The suspension is requested to mitigate 97E/35M shortages in the USAR.

As a result of a joint decision made by the previous CG, USAIC and FH; CG, INSCOM, and DCS, G2 during the 31 May 2007 General Officer Steering Committee, language will return as a 35M MOSQ requirement at all skill levels in FY 2010 in the Active Component. Soldiers accessed into the Active Army during the language suspension period will not be required to hold a foreign language in order to meet MOSQ or promotion eligibility standards. The language suspension period for the Active Army is 5 May 2006 through 30 September 2008. OCMI has produced and submitted the Out of Cycle (OOC) MOCS package detailing this MOSQ revision and it is currently being staffed at TRADOC.

This MOS has a significant shortage of NCOs due to the rapid increase in requirements (E-6 44% fill and E-7 77% fill). We need the help of leaders at all levels to encourage the retention of these Soldiers. The current selected reenlistment bonus is 4A/4B/4.5C with a max cap of $30K. We also need your support in reclassifying quality NCOs into this MOS.

As demonstrated in the STAR promotion stats above, we need to ensure every effort is taken to send ***qualified*** 35M (97E) Soldiers to the promotion board at their earliest eligibility. This will help the MOS health.

MOS 35N (98C), 35P (98G), and 35S (98Y)

INSCOM requested adding a requirement for a CI Scope Polygraph for all Signals Intelligence MOSs. This proposal was approved by the previous CG, USAIC and FH, and is currently being staffed with HQDA.

"Soldiers are Our Credentials"

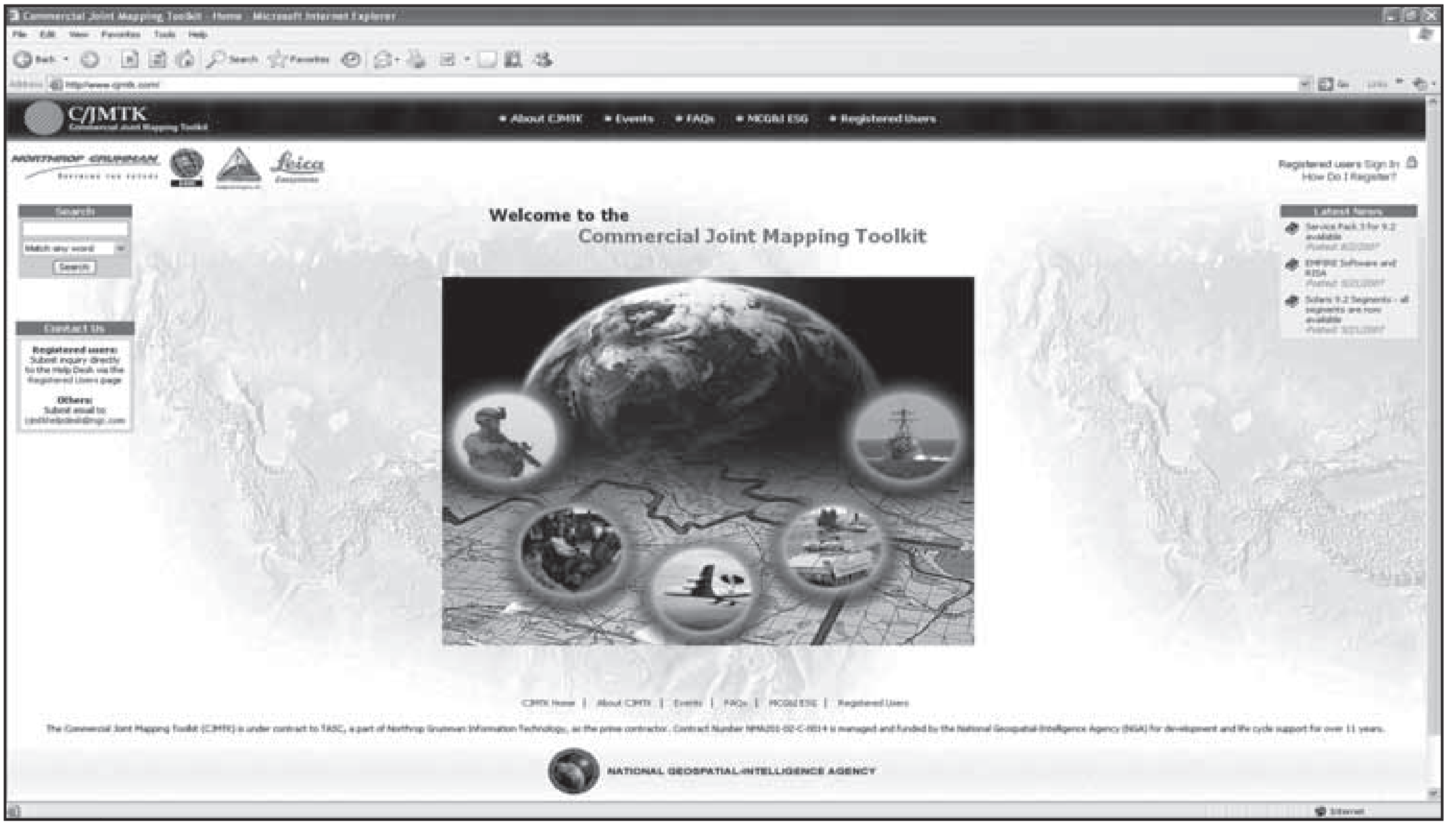
Toolkit Empowers Warfighters for Net-Centric Warfare

By Susan Marchant

This paper was first formally published in the National Geospatial-Intelligence Agency's Pathfinder magazine (May June 2007).

NGA is leading the way in geospatial visualization and analysis tools for net-centric warfare, leveraging the latest and greatest in commercial-off-the-shelf technologies. Our Commercial Joint Mapping Toolkit (CJMTK) empowers warfighters with situational awareness.

"CJMTK is a critical enabler to our Battle Command migration to a service-oriented architecture," says Col. Harold Greene, Project Manager for Battle Command, a unit of the Army Program Executive Office for Command, Control and Communications Tactical (PEO C3T). "Today, we are hamstrung in showing a common picture by multiple map engines and displays with unique interfaces."


Commercial Joint Mapping Toolkit - Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address http://www.cjmtk.com/
C/JMTK
Commercial Joint Mapping Toolkit
About CJMTK
Events
FAQs
MCG&I ESG
Registered Users
NORTHROP GRUMMAN
Leica
Registered users Sign In
How Do I Register?
Search
Match any word
Search
Contact Us
Latest News
Welcome to the
Commercial Joint Mapping Toolkit
CJMTK Home | About CJMTK | Events | FAQs | MCG&I ESG | Registered Users
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
Internet

Registered users: Submit inquiry directly to the Help Desk via the Registered Users page

Others: Submit email to cjmtkhelpdesk@ngc.com

Service Pack 3 for 9.2 available

EMPIRE Software and RIDA

Solaris 9.2 Segments - all segments are now available

The Commercial Joint Mapping Toolkit (CJMTK) is under contract to TASC, a part of Northrop Grumman Information Technology, as the prime contractor. Contract Number NMA201-02-C-0014 is managed and funded by the National Geospatial-Intelligence Agency (NGA) for development and life cycle support for over 11 years.

Driving to a Common Viewer

The Army "is driving to a common viewer with a known interface for all of our functional services," Greene said. "CJMTK provides that to us today. We've already seen great improvement in interoperability for those systems we've migrated to CJMTK."

NGA was providing a Joint Mapping Toolkit (JMTK) to the Command, Control and Intelligence (C2I) community through the Defense Information Systems Agency (DISA) Common Operating Environment when Congress mandated the toolkit's commercialization. Three years later—in 2002—NGA acquired the CJMTK following a successful source-selection competition.

What is a "Toolkit"?

The CJMTK is not a stand-alone application. It is a collection of software components that the C2I developers embed into their mission applications to support the use of standardized geospatial visualization and analysis tools tailored to their specific missions. By using a suite of ArcGIS™ tools, the C2I community obtains the advantage of interoperability without the costs of licensing and maintenance. Other advantages of the commercial toolkit include the availability of worldwide training, increases in functionality through incremental enhancements, standardization and the ability to capitalize on the latest technical benefits and economies of scale.

CJMTK is available through three major licensing options:

- Option 1, for the C2I community, provides free access, centrally funded by NGA, through the DISA Common Operating Environment and Net-Centric Enterprise Services.
- Option 2, for the extended user community, is available to users who do not qualify as members of the C2I community but want to be interoperable with the CJMTK community at their own expense.
- Option 3, for foreign governments, provides access through a U.S. government sponsor by purchasing seats through a Foreign Military Sales office.

This toolkit and its license agreement translate into a bundle of functionality that has far-reaching possibilities for the military services as they move into the realm of joint net-centric warfare and service-oriented architecture.

Payoffs

The C2I community has already capitalized on the advantages of the CJMTK, fielding over 235 mission-approved applications. For example, the Coast Guard's Search and Rescue Optimal Planning System is built on CJMTK technology. The system provides geographic displays of optimal search areas for missing mariners or vessels using data such as last known position and potential drift intervals.

An early adopter of CJMTK, the Army's Maneuver Control System, continues to harness CJMTK's power of visualizing and sharing geospatial intelligence (GEOINT) by integrating commercial technology into the tactical environment. Planners use the system to understand the battlefield and plan actions to achieve the commander's objectives. Both rely on the system to deliver accurate information about friendly and enemy capabilities and locations, weather, terrain, obstacles and other GEOINT.

The Air Force Portable Flight Planning System and Joint Mission Planning System are integrating CJMTK to provide the capabilities of an advanced geographic information system to the C2I mission-planning community. These systems have the ability to consume a wide variety of information from Web mapping services and through direct access to geographic databases. Both systems, for example, use CJMTK to integrate weather information from Web mapping services into the mission-planning environment.

A collaborative effort of DISA and the Global Command and Control System is the Joint Web Common Operational Picture (COP). This system uses CJMTK to provide a simple, intuitive user interface that enables soldiers to view critical information without extensive training. By distributing data-access and map-production capabilities to existing C2I systems, Joint WebCOP reduces the processing performed on its server. The distributed C2I systems feed information back to the Joint WebCOP server in Extensible Markup Language (XML) or as a simple map image. Any platform with network connection and a Web browser may view the COP.

Strange but True

Although NGA funds the CJMTK program, the Agency is not qualified as a user due to the fact that CJMTK is for the exclusive use of the C2I community. However, NGA has other licenses and avenues for obtaining the same functionality.

As Functional Manager for the National System for Geospatial Intelligence, NGA enables warfighters to plan, execute, report and visualize the COP through CJMTK. With over 145,000 users, or "run-time seats," CJMTK is on the rise. More information about CJMTK is available at www.CJMTK.com.

Susan Marchant works in NGA's Acquisition Directorate's CJMTK Program Office.

NGA Trains Puerto Rico National Guard

By Joseph Riggs

This paper was first formally published in the National Geospatial-Intelligence Agency's Pathfinder magazine (May June 2007).

"We have some Puerto Rico Army National Guard soldiers that need FalconView™ training," Staff Sgt. Katie Phelps, an all-source intelligence technician with the Southwest Army Reserve Intelligence Support Center, told members of the Army NGA Support Team at Fort Hood, Texas. FalconView™ is a portable computer mapping system that pilots use in flight planning.

The Puerto Rico guard members received specific data sets over the Sinai Peninsula for their upcoming one-year service as peacekeepers with the Multinational Force and Observers (MFO). The MFO's peacekeeping force supervises implementation of the security provisions of the Peace Treaty between the governments of Egypt and Israel in the Sinai Desert, Straits of Tiran and Gulf of Aqaba.

Fifty copies of a special reference graphic provided by an Army unit returning from the MFO were also printed. Coordination with the local Fort Hood command was a key element in making the training a success. The Technical Division of the Central Technical Support Facility (CTSF-TD) at Fort Hood provided classroom space and technical expertise on the functionality of the Army Battlefield Command System. John Seibert of the CTSF-TD continued his promotion of NGA products and services as co-instructor.

Two-Year Effort

For two years, the 75th Infantry Division (Training Support) has engaged NGA's Office of Military Support and the National Geospatial Intelligence College for FalconView™ training. Soldiers are trained on the basics of the program, using the NGA course "Geospatial Information and Services for the Warrior" or a shorter, locally produced course.

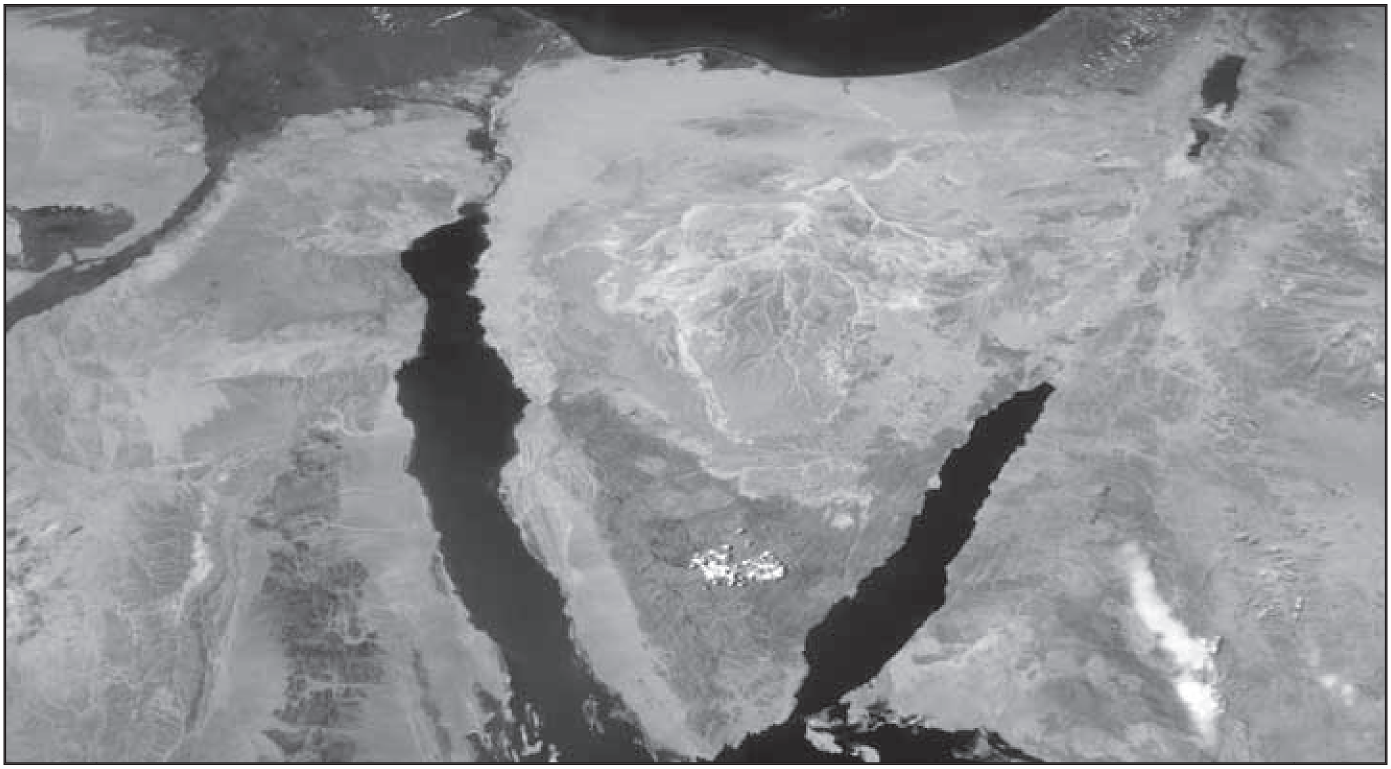


Image courtesy of the Image Science & Analysis Laboratory, NASA Johnson Space Center.

The Puerto Rico guard members received specific data sets over the Sinai Peninsula for upcoming service as peacekeepers with the Multinational Force and Observers (MFO). The MFO monitors access to the Gulf of Aqaba, on the peninsula's east side (right) through the Strait of Tiran.

The college sends a mobile training team for a four-day course that teaches the soldiers the basics of geospatial intelligence (GEOINT) products, map ordering and FalconView™. This is the preferred method for training infantry soldiers on FalconView™. If the unit does not have time for four days of training, NGA has analysts in place at strategic locations to assist units in tailoring training to their specific needs. The collaboration between the analyst and the college includes all course materials and train-the-trainer courses.

The soldiers gain an information edge for their mission analysis by using FalconView™ as a mission planning tool. The analyst trainer is able to adjust the course of study to enhance the students' ability to see how GEOINT is used to prosecute military objectives based on their specific battle-space visualization requirements.

Course materials, including GEOINT data and contact information, are tailored to the specific mission requirements of the students. Analyst trainers also use student questions to guide the course of study to fit the mission requirements. In response, the analyst generates standard and non-standard GEOINT products, such as special-reference graphics. By integrating specific datasets, student needs, and visualization tools like FalconView™, students achieve a reliable understanding of their battle space.

"The training was quite effective and the take-home materials presented are excellent for further training," wrote Warrant Officer Carolyn Compton, an all-source analyst technician, who recently provided feedback.

Joseph Riggs is a geospatial intelligence analyst on the Army NGA Support Team, serving with III Corps at the Central Technical Support Facility, Fort Hood, Texas.

Unit Profiles

Tell us about your unit. Please send us a write-up with the following items and information:

- High resolution color photographs or high resolution soft copy (preferred) of the unit crest.
- History of the unit to include campaigns and decorations.
- Current unit subordination, status and mission (unclassified).
- Operations your unit has supported in the last 15 to 20 years.
- Recent special accomplishments or activities that make your unit unique.
- Images of specialized equipment (unclassified).
- POC name, email address and phone numbers for this project.
- Full unit mailing address.
- Other information you would like included not listed above.

In order to allow our graphics designer time to create your unit crest, please send any photographs at the earliest possible time to:

ATTN ATZS-CDI-DM
Military Intelligence Professional Bulletin (MIPB)
Box 2001
Bldg. 51005
Fort Huachuca, AZ 85613-7002

Please send the soft copy crest and the unit write-up to sterilla.smith@conus.army.mil.

In Fields Afar, NGA Product May Be Warfighters' Only Friend

By Sabine Pontious and Kevin Boyer

This paper was first formally published in the National Geospatial-Intelligence Agency's Pathfinder magazine (May June 2007).

Picture this: a small Army unit plans an operation in the embattled Tall 'Afar area of Iraq, the site of historic clashes between coalition forces and insurgents. These young Soldiers are alone, cut off from their comrades and from modern comforts and technology—but they are armed with a laptop loaded with data about the countryside around them. They are using an NGA product called Geospatial Intelligence for Operations Support and the Battlefield, or GIB, a handful of DVDs containing an array of imagery and geospatial products.

The Soldiers are grateful for GIB's simplicity: A geospatial information system (GIS) bundled with the product allows them to manipulate the various "layers" of data to create their own customized, fused view without requiring any GIS expertise. They simply need to know how to navigate in a Web browser environment. In fact, within one hour of receiving GIB from an NGA technical representative, the Soldiers have taken it on patrol and are using it to better visualize and understand their surroundings. This is a true story.

Wealth of Data, Ease of Use

GIB provides an amazing variety of data. For example, Controlled Image Base® is unclassified digital imagery ideal for providing locational awareness in emergencies. Handheld photographs and movies include 360-degree immersive photos (similar to virtual real-estate tours) and video with embedded coordinates. Imagery obtained through light detection and ranging (LIDAR), a technology similar to radar, is used in line-of-sight and urban warfare planning. The data includes a catalog of standard NGA products, including Compressed Arc Digitized Raster Graphics, Vector Map, Digital Terrain Elevation Data and Digital Aeronautical Flight Information Files, as well as precise targeting data.

The sheer volume of accessible data is staggering. Using "MrSid" compression technology, NGA is able to load 20 DVDs' worth of data onto one DVD. But GIB's greatest attribute is its ease of use: With point-and-click navigation through interactive displays, even novice users can quickly become experts at GEOINT. Users are able to save the custom views they create and insert them into other applications, including briefings. A mere few years ago, it would have been unthinkable to offer such high-end GIS capabilities in such a compact, user-friendly package.

Photo courtesy of U.S. Marine Corps.

The ability to access and analyze imagery and geospatial information in the field is available through an NGA product called Geospatial Intelligence for Operations Support and the Battlefield, or GIB.

Meeting the Challenge

What is the origin of GIB? In 2004, then NGA Technical Executive (TX) Roberta Lenzcowski approached a few of the Agency's geosciences experts and challenged them to devise a geospatial data and imagery package to send forward to warfighters. She stipulated that the package be self-contained, presented in a universal format (with no constraining system requirements) and simple to use, as well as *free* to users. At the time, NGA was able to send out similar packages on an ad hoc basis, but demand was limited, because users had to be experienced with GIS applications and already possess the software.

Photo courtesy of the Department of Defense.

A new NGA product gives warfighters situational awareness on their laptops with a handful of DVDs containing imagery and geospatial information and an easy-to-use geographic information system to analyze it.

The staff quickly met the TX's requirements. Within about a year, the original prototype had become a viable product. Now, the Defense Logistics Agency, distributor of NGA products, offers 70 NGA GIB titles with three or four DVDs each, covering individual countries or regions. Recently, during just one month, a team of four analysts compiled six multi-DVD GIBs over countries in the Horn of Africa.

A Widening Circle of Users

Although GIBs were initially developed for warfighters, they are now being used in an ever widening circle of homeland security applications—of course, conforming to strict congressional oversight of domestic imagery. In early March, GIB data was collected for Twentynine Palms, Calif., and delivered to the Marine Corps Air Combat Center there. The Marines are using it to train troops for urban combat and route reconnaissance. NGA provided a New York State GIB to the Army National Guard in Albany late last year, prompting a request for additional homeland security imagery. Even the Las Vegas Metropolitan Police Department became fans: The Intelligence and National Security Manager in the Homeland Security Bureau declared, "The flexibility of this tool is phenomenal."

NGA's goal with GIB, as with all of our products, is to provide our government and civil partners with the easiest access to the most useful GEOINT information. End of story.

Note: The Geospatial Intelligence for Operations Support and the Battlefield (GIB) program is an example of a collaborative effort across several NGA offices. It is very similar to NGA's current support to Geospatial-Intelligence Contingency Packages, formerly in hardcopy called Noncombatant Evacuation Operations Packages, or NEOPacks. As NGA migrates toward a data-centric environment, the GIB and GCP programs will converge to provide a single service to the National System for Geospatial Intelligence community.

Sabine Pontious is a Booz Allen Hamilton contractor supporting communications for the Source Operations and Management Directorate. She has also performed outreach and communications for the Analysis and Production Directorate and Office of Corporate Relations.

Kevin Boyer is an image scientist in the Source Operations and Management Directorate, specializing in custom data sets for geographic information systems. He started government service in 1983 and has also worked as a cartographer and geospatial analyst.

Photographer Pioneered Aerial Reconnaissance

‘For the Lives of Men’

By Dr. Gary E. Weir

This paper was first formally published in the National Geospatial-Intelligence Agency’s Pathfinder magazine (May June 2007).

“I [finally] have an opportunity to get off a letter to Paris.... [T]he railroads are being used by the military—I only know that war is inevitable now,” the American photographer Edward Steichen wrote to his friend Alfred Stieglitz in New York in one of his letters now stored in the Steichen Archive of the Beinecke Library at Yale University.

It was 1914—the year the European Great Powers initiated a war that changed the world forever—and that momentarily stranded Steichen with his family in the French village of Voulangis.

That summer Steichen sent his loved ones to relatives in Great Britain and departed himself for New York City via Marseilles on board the steamer SS *Sant’Anna*. The location of his French home permitted him to see some of the early fighting, to sense the change of mood in France, and to witness the effect of mobilization. He certainly had no illusions about the horror unfolding before his eyes.

When the United States entered the war in 1917, Steichen received a commission from the Army and shipped out with the American Expeditionary Force (AEF) to France as a specialist in aerial reconnaissance. Unlike many of his fellows in the art world, Steichen, a naturalized citizen from Luxembourg, felt a strong compulsion in both world wars to serve his adopted country close to the front. He also felt that his extraordinary skills with a camera would both aid the American cause and vividly demonstrate the waste and absurdity of war.

From Pigeons to Airplanes

Armies had long since realized the advantages of photographic aerial observation. In 1903 the Germans developed a 70-gram homing pigeon camera that took 38-millimeter negatives automatically every 30 seconds. When the United States entered the Great War in 1917**,** the Army followed suit with a pigeon system that took pictures of the enemy lines.

The First World War also provided the opportunity to combine airplane technology with the still-image camera. This step gave the armed forces the ability to move, see and record the Earth in a more systematic manner. The reliability, regularity and responsiveness of the airplane permitted conversion of the data gathered into reliable and timely intelligence.

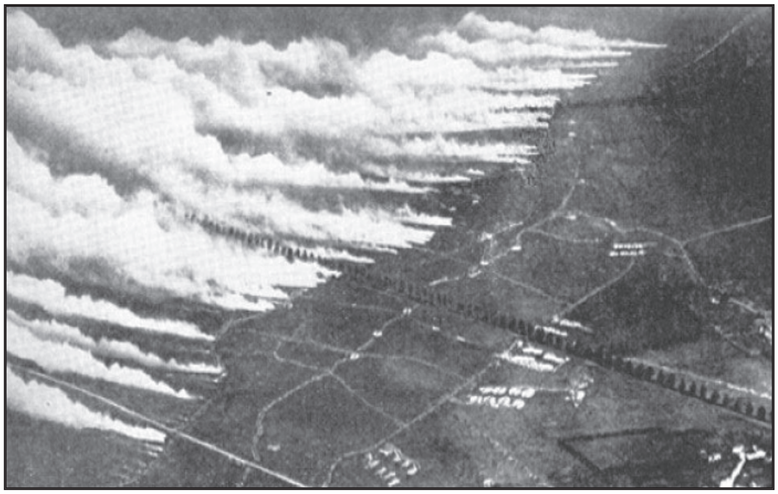


Photo courtesy of the U.S. Army Center for Military History.

Aerial reconnaissance captures a gas attack on the Western Front. An accomplished artist striving to make photography an art form before World War I, Edward Steichen led the wartime effort to transform aircraft photography into reliable and timely intelligence.

Under Steichen's direction the AEF in France successfully made the transition to aircraft photography. An accomplished artist in oils who struggled just before the war to raise photography to an art form, he now advised the Army on the best way to use the large, aircraft-mounted cameras. In short order he significantly improved the results presented to Army senior leadership, as he regularly moved between AEF headquarters and the front lines. Of course, security regulations and access to classified methods and materials permitted him to tell his friends via his letters home only a small part of what he did for the warfighter.

Greeting Stieglitz in one of his letters, Steichen remarked, "Well, here I am in the famous 'somewhere in France'—hard at it . . . and once again for photography—only this time . . . photography and plus. I suppose that means the lives of men. I wish I could tell you about it but that is naturally taboo…."

Imagery Reconnaissance Operations

Steichen eventually commanded a reconnaissance unit on the Western Front consisting of 55 officers and 1,111 enlisted soldiers. The unit daily provided Gen. Billy Mitchell's air staff with imagery intelligence, recounts Catherine Tuggle in "Edward Steichen: War, History and Humanity," in the History of Photography, vol. 17, number 4 (Winter 1993). Before America's two years of war concluded, Steichen had implemented image gathering and overnight processing procedures that could daily place, on demand, as many as 4,000 black-and-white prints of the Western Front before the AEF leadership, Tuggle writes.

Photo courtesy of the U.S. Army Center for Military History.

An aerial photo of Vaux, in northeastern France, shows damage after its capture by the U.S. Army's Second Division July 1, 1918.

Aerial photographs not only revealed troop movements and enhanced cartographic services but also offered more reliable battle-damage assessments based upon images captured before and after bombardment from the air or by artillery. Steichen and his staff helped military leaders standardize many other techniques, including the use of multiple images to produce three-dimensional effects, enhancing detection further.

This aerial intelligence pioneer always viewed his part in the Great War as simply part of life, always keeping it in perspective. He clearly realized the war's excitement, its value to his personal development and its terrible absurdity.

"It's a great game—life—when it goes at such a pace and when the price [of life] counts as little as it does here," he wrote Stieglitz. "And whether it's the thump thump thump of marching troops or a delicious *Sole frite* [fried fish] with a bottle of Barsac—what's the difference—or freezing up in the air [gathering imagery] or feeling like a corpse in a cold, damp *has been a bed*—it is full and rich with meaning—even though [it is] the result of human imbecility."

After the war concluded in 1919, Steichen returned to New York City and worked for Condé Nast publications, virtually defining American fashion and portrait photography while gaining a reputation as one of the world's great imagery artists.

Dr. Gary E. Weir recently assumed duties as the NGA Historian. A former member of the history faculty at the U.S. Naval Academy, he spent the last decade as head of the Contemporary History Branch of the U.S. Naval Historical Center, a component of the Office of the Chief of Naval Operations.

The Role of Geospatial Engineering in GEOINT

by Colonel Thomas R. Crabtree

In today's rapidly-changing environment of geospatial technology and services within a net-centric environment, the warfighter can access numerous geospatial products across a sea of platforms and formats. The extensive inventory of imagery and "map-like" products available to users in this environment can give the impression that technology has made obsolete the traditional disciplines of mapping, charting, and geodesy. But to the contrary, the age of GEOINT is validating and expanding the need for geospatial engineering to produce high-quality digital terrain products as the foundation upon which GEOINT is achieved.

One of the dangers in the digital age is that products can be digitally created, combined, and modified with a resulting end-product that is difficult to trace as to origin. How can I know that the digital map I'm looking at is accurate, and to what degree is it accurate? I see a target on a video feed. I know (from experience) that the building I see on video is located at the intersection of two known streets. I can locate the same intersection on a map product and pull a 10 digit grid coordinate. But is this grid accurate to 1 meter (m), 10m, or 200m? The answer has to be traced to the origin of the geospatial product. This problem grows when I really want to target the second story window using a three dimensional (3D) image. Today, any user with the right software can build a 3D model and save it on a server for others to use. But it takes a geospatial engineer or National Geospatial-Intelligence Agency (NGA) geospatial analyst to create products with known accuracy and manage this data in such a way that supports analysis and targeting. How are geospatial product standards enforced in today's net-centric and ever changing TOC environment? It depends, and this is one of the growing challenges facing geospatial engineers in today's GEOINT environment

What is Geospatial Engineering?

Given that GEOINT consists of Imagery, Imagery Intelligence, and geospatial information, then where does geospatial engineering come in? Geospatial engineering is the discipline practiced by MOSs 21U, Topographic Analyst and 215D, Terrain Analysis Technician, that takes raw imagery and geospatial information and turns it into maps and terrain products useful to warfighters in a military context. Under GEOINT, the NGA name for this discipline is "geospatial analysis", but engineers prefer "geospatial engineering" because it's clearer as to who performs this role in the Army. This discipline is also referred to as Geospatial Information and Services (GI&S). Here's a definition of geospatial engineering from the soon-to-be-published **FM 3-34, Engineer Operations**:

*"Geospatial engineering is the **art** and **science** of applying geospatial information, to enable understanding of the physical environment for military operations."*

The ***art*** is to the ability to understand the mission, enemy, terrain and weather, troops and support available, time available, and civilian considerations (METT-TC) and the geospatial information available, in order to explain the military significance of the terrain to the commander and staff, and create geospatial products for decision making. (This art is essential to Steps 1 and 2 of the Intelligence Preparation of the Battlefield process.)

The ***science*** is the ability to exploit geospatial information, producing spatially accurate products for measurement, mapping, visualization, modeling, and all types of analysis on the terrain. (The science really precedes the art—it's the foundation for further exploitation.)

Producing a Common Operational Picture

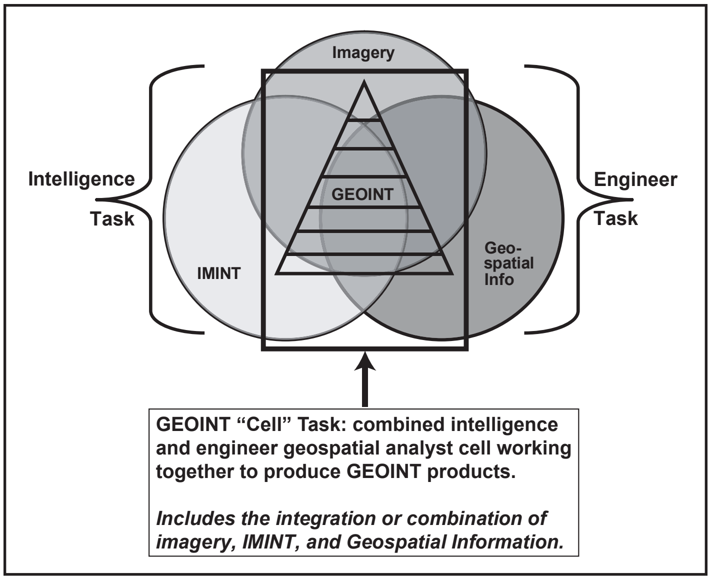
One of the key roles of geospatial engineers for the future is to manage the geospatial foundation of the common operational picture (COP) for battle command. The scope of battle command in this context is inclusive of operations, intelligence, modeling and simulations, and training, since all these functions depend on sharing the same geospatial data used on operational command and control (C2) platforms. Without deliberate management (collecting, processing, updating, conflating, deconflicting, and disseminating), there will be no unified COP. This point is hugely significant, because today we have many "operational pictures" but not a "unified COP" due to the plethora of platforms and incompatible formats which prevent systems interoperability. Deliberate management of the COP, along with adoption and integration of geospatial data standards across battle command systems and staffs, will solve this for the future. And who's responsible for this management?—geospatial engineers!

Now, what does this have to do with GEOINT? Traditionally, the COP is in the G3/S3 domain, but the future platform for managing the geospatial foundation of the COP is the Distributed Common Ground System–Army (DCGS-A), a GEOINT platform. We've always used the phrase "intel drives operations", and this illustrates how intelligence and operations are increasingly linked as we move to the future. It's the geospatial information foundation that allows the merging of GEOINT with operations, with all events being tied to their spatial location, and able to be displayed on the COP or analyzed using geospatial information shared across the warfighting domains. This concept describes the synergy of GEOINT. It is also highly dependent upon the ability to achieve a true COP, and not attainable without the science of geospatial engineering.

GEOINT Cells and the Way Ahead

The concept of GEOINT cells is emerging through collaboration among NGA, the Joint community, and the Army Intelligence and Engineer communities. GEOINT cells are formed when Imagery Analysts and Geospatial Engineers work together at a given echelon. Their purpose is to manage and update GEOINT data for their units' area of interest, and to create mission-specific GEOINT products to support planning and operations. Based on echelon and unit size, GEOINT cells may be permanent or temporary. Generally, GEOINT cells should operate continuously at division level and above.

In emerging doctrine at the Joint task force (JTF) level, the GEOINT cell process is called the JWIG (Joint Warfighter Interoperable Geospatial Intelligence) process. As such, it would supervise all spatially referenced functions, data, and activities within the JTF. Additionally, the GEOINT cell must establish relationships across the JTF to enable the Joint warfighter to define requirements; discover and obtain GEOINT; put it into usable form; and then use, share, and maintain GEOINT with mission partners. **Joint Publication 2-03, Geospatial Intelligence Support to Joint Operations,** 22 March 2007, describes the steps of the Geospatial Intelligence Preparation of the Environment process, and gives GEOINT cell responsibilities for each phase of contingency planning. Both National System for Geospatial Intelligence publications and Joint doctrine recognize that GEOINT data and processes provide the foundation for all fusion, analysis, and visualization activities, especially in the development of the COP.



GEOINT "Cell" Task: combined intelligence and engineer geospatial analyst cell working together to produce GEOINT products.

Includes the integration or combination of imagery, IMINT, and Geospatial Information.

Note: This diagram is from the U.S. Army Intelligence Center and Fort Huachuca's presentation to the Army Geospatial and Imagery Conference on 7 May 2007. It was co-developed by Colonel Crabtree and Mr. Charles Hayward, Deputy Director, Requirements Determination Directorate, USAIC.

The emerging Joint doctrine forces us to further define how GEOINT cells will operate at each echelon within the Army. A conceptual diagram depicting the relationship of Army engineers and intelligence Soldiers in GEOINT cells is shown above. Since GEOINT cells are currently only described in concept, continued collaboration between Military Intelligence (MI) and Engineers is required to refine this concept; develop tactics, techniques, and procedures and doctrine; revise Tables of Organization and Equipment to document cells as organizational elements, and then obtain resources to fully achieve the capabilities envisioned.

Conclusion

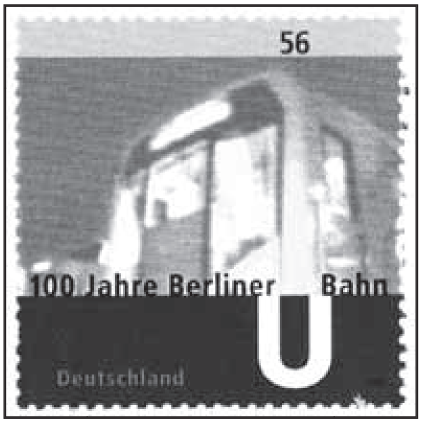
Geospatial engineers perform a critical role in producing the high quality digital terrain foundation products on which the COP and GEOINT depend. This geospatial information allows GEOINT to merge with operations. Understanding accuracy, data types, correct usage of data, and data exploitation to enhance mission readiness and execution are all functions performed by the geospatial engineer. Additionally, DCGS-A is the future platform that engineers will use to manage the COP; it's not solely an intelligence platform. Engineers and MI must continue to work together to realize the full benefits of GEOINT for the warfighter.

Colonel Thomas R. Crabtree is currently the Director of the TRADOC Program Integration Office (TPIO)—Terrain Data, at the Maneuver Support Center, Fort Leonard Wood, Missouri. He is also chair of TRADOC's Geospatial Integrated Capabilities Development Team (ICDT), responsible for geospatial solutions that will enable battle command interoperability. COL Crabtree is an Engineer officer with experience from platoon through battalion command, and staff assignments from company through HQDA level. He previously served as the chief environmental analyst on the Army's basing study for BRAC 2005, with oversight of geospatial analysis for the BRAC team. COL Crabtree is a 1982 graduate of USMA and holds an MS in Computer Science from the University of California, San Diego.

INTELLIGENCE PHILATELIC VIGNETTES

"Train" of Political Thought

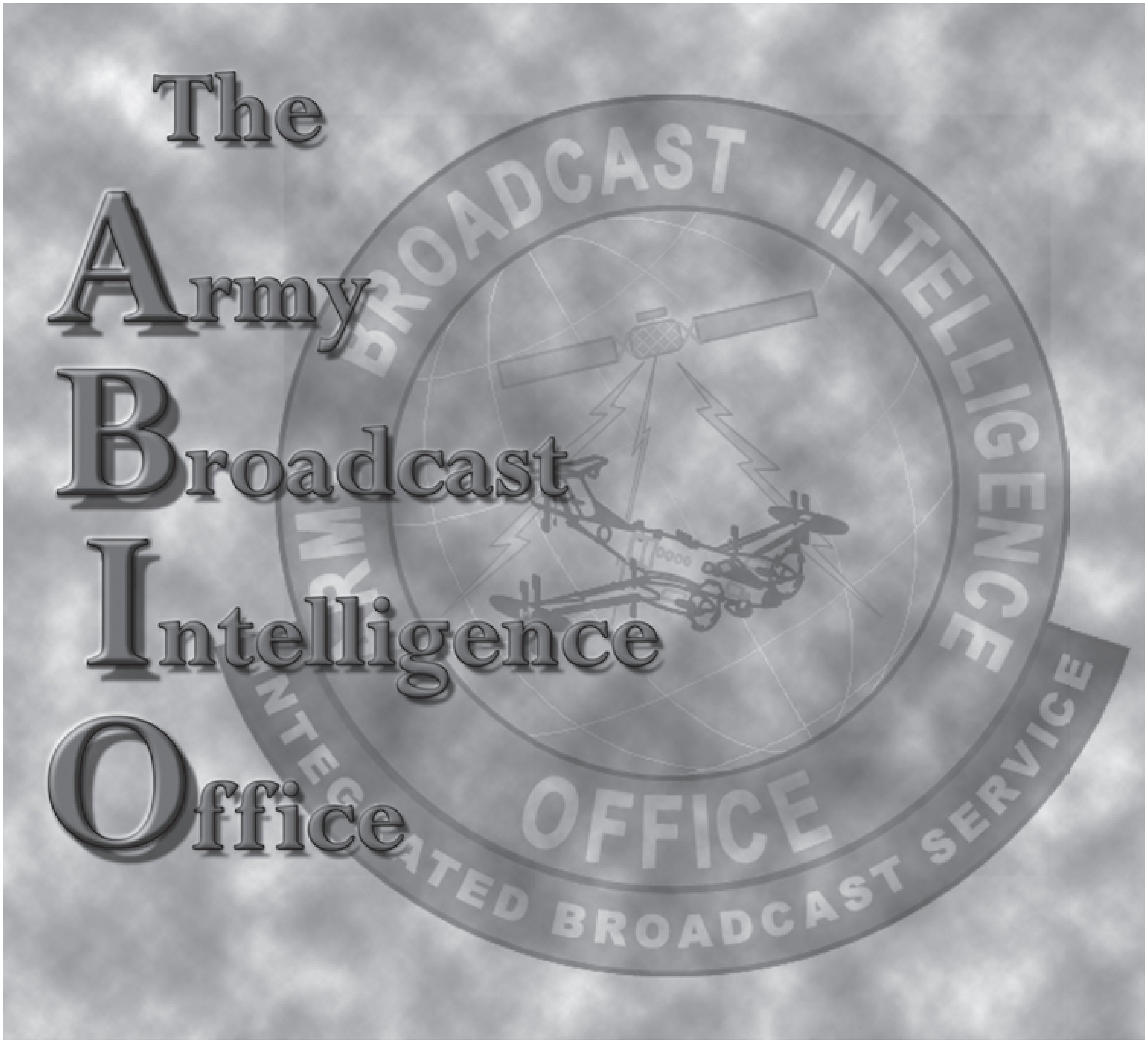
by Mark Sommer



The subway system in Berlin, Germany, called the U-Bahn, celebrated its centennial recently. First begun in 1902, much of the system was above ground in the early years, but today it reaches all parts of the city mostly underground. During the Cold War, Berlin was a divided city creating a problem for the subway system, which ran under the now defunct Wall into East Berlin and then curved back into the Western sector. The East German government found it impractical to try to stop the trains, but to keep its citizens from escaping to the West, it sealed the stations which were called "Ghost Stations." All were opened after the 1991 reunification of Germany.

Subway systems in major cities have distinctive signs to mark entrances. The signs for the Berlin U-Bahn have a large "U" on dark blue (perhaps invoking the political feelings of its residents during the Cold War?) One can only guess how many "dead drops," "wet affairs," etc. took place in these stations. The stamp was issued on 7 February 2002.

Mark Sommer holds a BA in Political Science from Yeshiva University and an MA in International Relations from Fairleigh Dickinson University. He teaches at Stevens' Institute of Technology in the Humanities Department. His philatelic memberships include The American Philatelic Society (www.stamps.org); Military Postal History Society (www.militaryPHS.org); Forces Postal History Society (UK), and The Psywar society (www.psywarsoc.org).


The
Army
Broadcast
Intelligence
Office
ARMY BROADCAST INTELLIGENCE OFFICE
INTEGRATED BROADCAST SERVICE

First printed in the 2nd quarter 2007 MICA Vanguard.

by Vince Cattera and Patrick J. Ahrens

Introduction

The Army Broadcast Intelligence Office (ABIO) was chartered by the Department of the Army (DA) G3 to act as the Army's centralized manager for the Integrated Broadcast Service (IBS). The ABIO mission is to ensure that the IBS delivers the Army's requirements for information and intelligence in support of Army operations in the War on Terror. One of the ways this is accomplished is by developing Army Information Exchange Requirements (IERs) that establish reporting criteria for time-critical and actionable "survival" information and intelligence to support Army mission planning and execution of operations, to include support to both Operations Iraqi Freedom and Enduring Freedom. The ABIO works in coordination with Army Service Component Commands (ASCCs), TRADOC Centers of Excellence (COEs), the U.S. Army Intelligence and Security Command (INSCOM), DA staff, and National intelligence agencies to identify shortfalls in reporting that affect Army operations in prosecuting the War on Terror and takes action to correct those shortfalls. As an example, the ABIO was instrumental in getting unattended ground sensor

(UGS) and improvised explosive device (IED) alert messages on the broadcast which provided actionable intelligence to the affected units within 5 to 10 seconds of injection.

ABIO also coordinated with the Distributed Ground System-Army (DCGS-A) TCM and program managers to ensure their Tactical Data Processors (TDPs) were able to receive and process IBS data. The ABIO identified that the DCGS-A TDP was not compatible with IBS and had to be modified. If ABIO had not identified this shortfall, then new versions of DCGS-A would not have been able to receive or disseminate data over the IBS. This effort directly supported the GWOT since DCGS-A is the primary TDP used by the Army to receive the IBS.

The ABIO works to match new counter-terror capabilities with the global dissemination capabilities of the IBS. Recent successes include a collective ABIO and INSCOM initiative to disseminate data from forward deployed collectors in the Middle East and to disseminate that data via IBS. On another front, the ABIO is currently working with the IBS Support Office at the National Security Agency to improve IBS dissemination of known or suspected IEDs within CENTCOM areas of operations (AOs). Note that the IBS program does not develop new information and intelligence collection platforms; rather, IBS provides both a regional and global dissemination system to ensure that current or newly developed collection platforms can forward their information and intelligence to those who need it most—the Soldier.

What is the IBS?

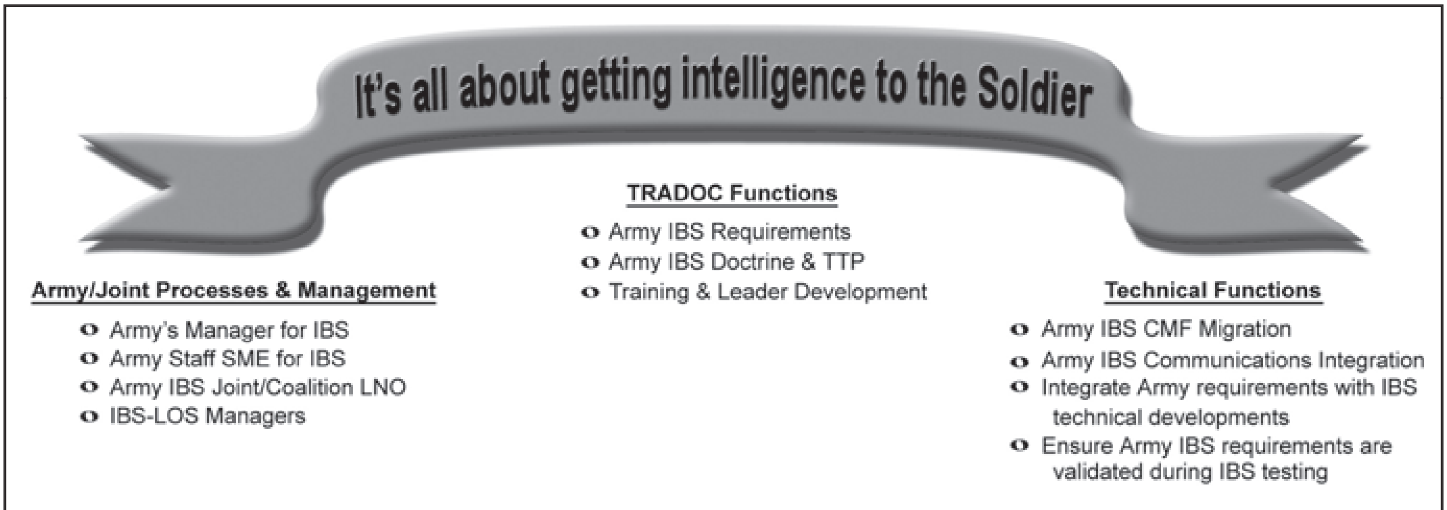
The IBS provides time-critical and actionable "survival" information and intelligence data broadcast via the Global Information Grid (GIG) to tactical forces. As part of its primary mission the IBS provides a global early warning capability that spans the full spectrum of conflict from ballistic missile launch detection to imminent terrorist strikes against U.S. Army units, organizations and installations. The IBS provides a critical dissemination path. This IBS dissemination is not limited to terrorist threat data, but also includes a Blue Force tracking capability for Army special units operating in hostile territory throughout the world and weapons status reporting of missiles in flight that strike known or suspected terrorist havens and training camps. Examples of time critical and actionable survival information and intelligence include threat detection, threat warning, and situational awareness. In other words, the information sent is so time-sensitive it needs to be broadcast to forces within the broadcast footprint and will allow commanders to take immediate actions to defeat or counter the threat and/or causes the commanders to order a protective posture.

IBS provides both multi-source intelligence and combat information that contribute to situational awareness, survivability, and targeting. It provides commanders the ability to access a multi-source, integrated network of threat data that is automatically "pushed" to forces deployed worldwide. Commanders may also query the IBS network in order to "pull" specific data. The characteristics of survival information are[1] :

- ✦ Information that requires the recipient to take immediate action to avoid danger or hostile action.
- ✦ Information that is essential to enable the recipient to take immediate action to destroy, nullify, or defeat a hostile entity, weapon, or force.

The ABIO is working with the IBS community to establish a standardized broadcast data message format and a single family of radios (transmit and/or receive) that are interoperable with all of the Services and with designated "five eyes" Allies. The ABIO is the Army's agent for coordinating and providing Army input to the IBS Common Message Format (CMF), which includes routinely updating and adding Army input to the IBS Data Elements Dictionary. ABIO work on the CMF ensures that IBS data includes Army driven data elements in formats comprehensible to soldiers. Without this work, IBS data relevant to the GWOT would go unrecognized.

Dissemination of IBS reports throughout the GIG is via two pathways—low bandwidth ultra high frequency (UHF) broadcasts and wideband networks (SIPRnet, JWICS, etc.). Time-sensitive "survival" information and intelligence that is broadcast via IBS travel on low bandwidth radio frequency (RF) links supported by a combination of SATCOM and air breathing platforms. UHF broadcasts are intended for soldiers who do not have access to wide band networks and support early entry operations and other AOs that lack a mature wide-band communications infrastructure. This is particularly relevant in GWOT operations that require quick entry and exit into areas hostile to U.S. military presence. The UHF IBS broadcast is uniquely capable of supporting Special Operations Forces (SOF) (transmit and receive) deployed in these high threat AOs. Additionally, all IBS reports, both time sensitive and non-time sensitive, travel via wideband networks (SIPRnet, Global Broadcast Service (GBS)) to ensure widest dissemination. Wideband dissemination of IBS reports allows for a high volume of non-time critical data to be shared for improved situational awareness and is absolutely essential for the extensive intelligence analysis required to identify, find, and target terrorist networks.



It's all about getting intelligence to the Soldier

TRADOC Functions

- Army IBS Requirements
- Army IBS Doctrine & TTP
- Training & Leader Development

Army/Joint Processes & Management

- Army's Manager for IBS
- Army Staff SME for IBS
- Army IBS Joint/Coalition LNO
- IBS-LOS Managers

Technical Functions

- Army IBS CMF Migration
- Army IBS Communications Integration
- Integrate Army requirements with IBS technical developments
- Ensure Army IBS requirements are validated during IBS testing

ABIO Performs in 3 Functional Areas to Develop Army Capabilities and Protect Army Equities

The ABIO works continuously to integrate and leverage the IBS broadcast to the Army's fullest advantage. Since terrorists can strike any time, anywhere, the Army wants IBS dissemination of counter-terrorist and force protection data available to shooters, mobile units, fixed installations, Intelligence Analysts and any Army element that will benefit from the availability of that data. Although IBS dissemination is extensive in today's deployed force, the ABIO is working on approved Army requirements to deliver time-critical information and intelligence via low bandwidth UHF IBS broadcasts down to vehicle and aircraft level in a future combat system (FCS) equipped force. Expanded IBS data dissemination includes early warning of threat terrorist activities to Army organizations, installations, and units dispersed throughout the globe. Where feasible, capabilities intended for the future force are implemented now to support current operations. Army brigades, to include conventional and FCS Brigade Combat Teams (BCTs) and SOF, will be, or are currently capable of receiving IBS reports via both UHF low bandwidth broadcasts and wideband networks. This dual capability will support early entry operations and AOs that lack wideband infrastructure while allowing for high volume IBS dissemination of both non-time and time critical information and intelligence via wideband networks in mature AOs.

The information and intelligence collection systems that produce the IBS broadcast data are referred to as "IBS Producers." IBS producers include National-level collection capabilities and service collection platforms, to include Army sensors. Most of the IBS producers and dollar investments have been provided by non-Army resources. The Army's intent is to continue to leverage these investments and the extensive resources to provide survival information and intelligence, terrorist threat warning, and targeting data to Army tactical forces at an economical cost. The ABIO is the Army's key agent for leveraging Joint and National level IBS investments to Army advantage.

The collection platforms that inject information and intelligence into IBS broadcasts were initially designed to provide technical intelligence in support of high intensity warfare. As the Army and the ABIO identifies further IBS requirements via TRADOC's Joint Capabilities Integration and Development System

(JCIDS) process, the Army will introduce additional IBS producers to include more informational and multi-intelligence systems, platforms, and soldiers who can provide survival information and intelligence across the ***full*** spectrum of conflict. But this does not mean that the ABIO or the Army waits years to implement IBS dissemination of new capabilities for a future force. As done with IED and UGS reporting, new collection capabilities that contribute to the GWOT are immediately integrated into the IBS broadcast. The ABIO continuously works with Joint and Army agencies to identify new capabilities for IBS data broadcasts.

Current and planned Army IBS producers include PATRIOT, Joint Tactical Ground Station (JTAGS), Guardrail Common Sensor (GRCS), Aerial Common Sensor (ACS), Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS) and other Army combat information and intelligence sensors as well as BCTs. The current IBS ground terminal is the Joint Tactical Terminal (JTT) (AN/USC-62), which will be in service at least until 2013. In the future, the Joint Tactical Radio System (JTRS) will be the Army's IBS radio-receiver. TDPs in use by the Army will be capable of manipulating IBS data (in IBS CMF) at IBS entry points designated by the Army. Current and future IBS capable TDPs include the Common Ground Station (CGS), the DCGS-A, and TIPOFF-NT (used by PATRIOT). The FCS will use an embedded DCGS-A appliqué to receive and present IBS data. All IBS producers (Air Missile and Defense (AMD), FIRES, Aviation, Intelligence, etc.) will employ JTTs and associated TDPs. The ABIO tracks and works with these cross-programmatic IBS elements to ensure that the Army retains relevant use of IBS broadcasts in GWOT operations during the migration to IBS FOC in 2013.

IBS White Paper currently being written to define INBS support to Army operations.

ABIO engaging with AMD, Aviation, Batle Command, and FCS to ensure support to operations.

ABIO working to inject Army-centric data and sources (such as Unattended Ground Sensors) onto the broadcast.

Conclusion

The IBS is a living and ever-changing system of systems. The IBS, like the Army, must be ever adaptable to respond to dynamic threats across the full spectrum of conflict. It must be poised to exploit new and cost effective technologies and intelligence collection capabilities that allow our soldiers to win and survive. Whenever feasible and cost effective, the ABIO works to integrate new collection capabilities with IBS dissemination to support current War on Terror operations. The ABIO, co-located with the Intelligence Center at Fort Huachuca, is the Army's centralized manager for development and change management of the IBS. The ABIO works in coordination with ASCCs, TRADOC COEs, INSCOM, DA staff, National intelligence agencies, the Acquisition Community, and the IBS Executive Agent to identify new intelligence collection capabilities that produce actionable combat information and intelligence on tactical timelines. The ABIO also assesses costs, risks, benefits, and trade-offs at the introduction of new Army IBS users and producers to ensure that a transforming IBS capability is maintained at an economical cost.

Endnote

[1] Characteristics of survival information extracted from IBS Joint Operational Requirements Document (JORD) dated 05 March 2007 and FCS ORD dated 13 July 2004.

Vince Cattera retired from the U.S. Army in 1995 as a Chief Warrant Officer. He served with the 1st Infantry (Vietnam); 2nd and 7th Infantry Divisions; 1st Cavalry Division; European Defense Analysis Center; and USCENTCOM. While at USCENTCOM, he served as the Senior Iraq/Iran Ground Forces Analyst within the Intelligence Directorate (J2) where he had direct input into National level Iraqi and Iranian military studies (National Intelligence Estimates), intelligence briefings, and exercises. He currently works in support of the ABIO.

Patrick Ahrens is a retired U.S. Army colonel. He served with the 1st Armored Division; 29th MI Battalion; Combat Maneuver Training Center; 3rd Armored Cavalry Regiment; the British Ministry of Defence and DA G2. He currently works in support of the ABIO.

Guide to the Proper Use of Civilian Intelligence Contractors in the War on Terrorism

by Harry P. Dies, Jr.

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

Introduction

You are newly arrived in Iraq, Afghanistan, or at some other new front in the War on Terrorism, and you have just met your civilian contractor Intelligence Analysts, Counterintelligence (CI) and Human Intelligence (HUMINT) teams. What type of intelligence support can these civilian intelligence contractors provide you? Who do they really work for? What type of taskings can you give them? These and other questions concerning civilian intelligence contractors are swirling through your mind, and you have a limited amount of time to devote to it due to your current operations tempo.

After my military retirement, with 23 years of active duty service in the U.S. Army, I spent one year as a civilian contractor in an intelligence advisory role in Iraq. I offer this brief guide on how to properly use civilian intelligence contractors and leverage the support they offer to win the battle against insurgents and terrorists.

This article will provide a brief overview of the relatively new phenomenon of civilian intelligence contractors performing intelligence jobs/functions normally performed by Soldiers and Department of Defense (DOD) civilian employees (i.e., intelligence analysts, interrogators, and CI and HUMINT personnel.) The overview includes: background on the use of civilian contractors; intelligence functions contractors can perform; command, control, and oversight of contractors; comparison of Soldiers to contractors; and practical advice on contractor use to assist the military in accomplishing the mission.

Contractors performing intelligence functions are very different than the traditional technical support contractors Military Intelligence (MI) has used to advise on and/or maintain MI technical systems such as the All-Source Analysis System and other electronic and computer-based intelligence systems. The technical support contractors have been around for sometime, while contractors performing actual intelligence functions are relatively new to supporting MI. Civilian contractors, as part of your intelligence team may be around for awhile, so it behooves MI leaders at all levels to understand the "can's and cannot's" with respect to their use.

Background

The U.S. military's use of civilian contractors is nothing new. George Washington's Continental Army employed civilian contractors during the American Revolutionary War.[1] Booz Allen Hamilton, a leading U.S. private contracting company, provided contract support to the U.S. Army in World War I.[2] Civilian contractors supported the military during World War II and during all other conflicts to the present date. Army **Field Manual (FM) 3-100.21 (100-21),** ***Contractors on the Battlefield*** states that "the increasingly hi-tech nature of our equipment and rapid deployment requirements have significantly increased the need to properly integrate contractor support into all military operations. Recent reductions in military structure, coupled with high mission requirements and the unlikely prospect of full mobilization, mean that to reach a minimum of required levels of support, deployed military forces will often have to be significantly augmented with contractor support."[3] What is new with civilian contract support to the U.S. military is the large quantity of the support. The number of civilian contractors supporting the U.S. military in Iraq is unprecedented. There are more private companies providing civilian contractors to the U.S. Armed Forces in Iraq than any other war in history.[4]

With the end of the Cold War, the U.S. began reducing its military forces to "35 percent from its Cold War high."[5] And of course MI was required to take its share of reductions. By the mid-1990s new regional conflicts began popping-up, and correspondingly U.S. military deployments increased dramatically. The new popular adage (or complaint) in the military became the phrase "doing more with less." One commander of mine took this logic further when he said "we will soon be asked to do everything with nothing."

As mentioned above, traditional civilian contract support to MI usually consisted of technical advisors and maintainers of the many MI computer-based systems used in intelligence collection, analysis, and dissemination. All through the Cold War, the U.S. military employed high-technology intelligence collection systems that became the premier means of intelligence gathering. In the past, contractor focus was training Soldiers on operating and maintaining these intelligence systems. What is relatively new are the "intelligence gathering" contractors—CI personnel and interrogators as an example.

At the end of the Gulf War, President Bush proclaimed the pursuit of a "new world order" and the Army responded by "building down." This build-down effort resulted in reductions across the board for the U.S. Army to include MI. The reduction led to shortages of personnel particularly in the CI and HUMINT fields. The reduction in CI and HUMINT personnel became critical as the threat shifted from the massive, conventional Soviet Army to the more loosely defined and non-traditional threat that conflicts such as those in Somalia, Haiti, and Bosnia brought to the forefront. After the Al Qaeda terrorist attacks of September 11, the U.S. military was ordered to deploy to Afghanistan and subsequently to Iraq. Note, the military was still at its "build-down" manning levels and now directed to fight the long talked about two-war scenario. The military found itself with serious shortages of Soldiers with intelligence military occupational specialties. An example of MI personnel shortages is cited in Chris Mackey's book, *The Interrogators.* Mackey states, "When the war in Afghanistan started, the Army had just 510 interrogators, including 108 of us who spoke Arabic—a tiny number for a nation about to embark on a massive effort to dismantle Al Qaeda, set up a string of new bases around the Persian Gulf, and within a year and a half, invade Iraq."[6] How to make up for the lack of interrogators, CI and HUMINT personnel, and intelligence analysts? The answer was outsourcing—providing an intelligence services contract to the private sector to reduce the deficit of key intelligence personnel. The U.S. Army has subsequently outsourced for civilian intelligence contractors in the Balkans, Afghanistan, and Iraq.

Intelligence Functions

There are a variety of intelligence functions that contractors are now performing for the military. Many of these functions are non-traditional roles for civilian contractors, with the exception of linguists. These include intelligence analysts, CI and HUMINT personnel, locally-employed personnel screeners, and interrogators. The issue for military leaders is understanding what intelligence support contractors can legally do and functions that contractors cannot do. The Army's Contracting Officer Representative, or COR, is responsible for managing the overall contract that makes these contractors available to the user units. The COR will interface on a regular basis with the parent private company that the contractors work for. What you need to do right off the bat is request a copy of the Statement of Work (SOW) from the COR through your chain of command. The SOW outlines in detail what the military and private contractor's responsibilities are in fulfilling the contract. The SOW will also describe the exact duty descriptions of the contractors. This is very important because you must always remember that these *augmenting* intelligence personnel are not Soldiers, they are civilians. There are certain functions they can perform for you in supporting your mission and certain functions that are prohibited by law and/or military regulations.

As an example, civilian CI contractors are limited in what duties they can perform. In June 2004, the Deputy Chief of Staff, G2 published a memorandum entitled *Contractor Support to Army Counterintelligence.*[7] The memorandum states that, "Contractors supporting CI activities have a limited role due to legalities and Army liabilities, and because the direction and control of CI is considered an "inherently governmental function." The memorandum also states, "Contractor subject matter experts will not carry badge and credentials (B&Cs) or Representative Credentials, nor will they be referred to as Special Agents." The memorandum prohibits CI contractors from conducting CI investigations and states that allowable support to CI investigations includes only case analysis, accredited forensics examinations and analysis, and translator/interpreter duties.

So you might be thinking at this point what's the use of having the contractors if the Army is going to place restrictions on the support they can provide to you? As we all know, people are the most valuable resource we have and are essential in getting the mission accomplished. From the previous example, your contractors can perform tasks "inside the wire" which allows your Soldier teams to perform their mission outside the wire. Again, it is very important to understand the capabilities of your contractors. You can best do this by requesting a copy of the SOW, reading it and directing any questions or concerns to the COR. Also, have your supporting contractor personnel provide you an overview on what support they can provide you.

Command, Control, and Oversight

Your civilian contractors are obviously not Soldiers. Contractors come from varied backgrounds; some may be retired military, prior service veterans, and some from law enforcement backgrounds. You cannot "treat" contractors as you do your Soldiers. As an example, **AR 715-9, Contractors Accompanying the Force**, states "in an area of operations where an international agreement authorizes the presence of U.S. forces (stationing agreement) or regulates their status (SOFA), the status of contractors and their employees, under local law, must also be established by international agreement."[8] Duties of contractors are established solely by the terms of their contract—they are not subject to Army regulations or the Uniform Code of Military Justice (UCMJ) (except during a declared war). Authority over contractors is exercised through the contracting officer.[9] Law of war treaties, such as the Hague and Geneva conventions, attempt to establish and clarify the status of contractors when supporting military operations. These treaties entitle contractors to be treated as prisoners of war.[10]

Contractor status however, is not your responsibility. AR 715-9 states the Contracting Officer's Representative "… acts as the government's representative for day-to-day management and/or receipt of contracted battlefield support services."[11] The regulation also states that, "… the commercial firm(s) providing the battlefield support services will perform the necessary supervisory and management functions of their employees. Contractor employees are not under the direct supervision of military personnel in the chain of command. The contracting officer (KO), or their designated liaison contracting officer's representative (COR), is responsible for monitoring and implementing contractor performance requirements; however, contractor employees will be expected to adhere to all guidance and obey all instructions and general orders issued by the Theater Commander. In the event instructions or orders of the Theater Commander are violated, the Theater Commander may limit access to facilities and/or revoke any special status a contractor employee has as an individual accompanying the force to include directing the Contracting Officer to demand that the contractor replace the individual."[12] AR 715-9 also states, "contracted support service personnel will not command, supervise, administer, or control DOD Civilian personnel."[13] It must be clearly understood that commanders do not have direct control over contractor employees (**contractor employees are not government employees**); only contractors directly manage and supervise their employees.[14]

So, what does all this mean to you? Well, first, the COR is the military point of contact that is responsible for the overall supervision and day-to-day monitoring of the contract. The private company, who the contractors work for and are paid their salaries by, is responsible for providing supervision and managers to provide this supervision in carrying out the contract. Note, AR 715-9 states, "contract employees are not under the direct supervision of military personnel in the chain of command."[15] Does this mean that your civilian contractors do not have to perform the tasks that you direct? The answer is yes and no. Remember, they are civilians and not Soldiers, so if the military or their company supervisor/manager says "write that report," they can refuse and quit at anytime. In the private sector there is the concept of "hire and fire" at will, meaning the company can as easily fire their employees as they can hire them. Of course, illegal firings can be taken to court by the terminated employee for reasons of discrimination and other wrongful acts. But my point is the employee also has the right to quit at anytime, normally giving at least two weeks notice. The military provides the task(s) to be performed to the contractor supervisors/managers and they in turn direct the contractors to perform the tasks per the SOW. Per AR 715-9, if individual contractor employees violate any military command policies or orders, the base commander can "limit access to facilities" of the contractors or request that the COR direct the contractor's employer to replace him.[16]

Another important aspect to be aware of is that contractors cannot supervise Soldiers or DOD civilians. Civilian contractors are *augmenting* the force to accomplish the mission. Contractors advise and assist the military, while the military decides and controls.

Oversight is an important issue since there is the hazard to lose control over what contractors are doing in support of your mission. An example of this is the Abu Ghraib incident. The Army employed civilian contractor interrogators and interpreters at the Abu Ghraib prison in Iraq. The reports of prisoner abuse at Abu Ghraib led to Major General Antonio Taguba's AR 15-6 investigation and subsequent report in 2004. John Singer, in the periodical *Foreign Relations*, states that, "Abu Ghraib contractors were involved in 36 percent of proven incidents and identified six civilian employees as individually culpable."[17] It is obvious that both Soldiers and civilians can make poor judgments and stray off course if not provided proper leadership and guidance.

"Can't Compare Soldiers to Contractors"

Former Secretary of the Army, Mr. Francis Harvey has stated that comparisons between Soldiers and contractors are "pointless."[18] Mr. Harvey was quoted in an article in the *Stars and Stripes* in 2005 concerning the pay gap between Soldiers and private sector contractors. His comments arose from growing complaints of Soldiers in Afghanistan and Iraq that they were "working side by side with contractors who earn double or even triple the military's base pay."[19] Mr. Harvey argued that people should not expect to get rich by joining the military, but rather take the satisfaction of protecting the nation and that after a 20-year career military personnel could also go into the private sector and pursue financial goals as well. I reluctantly write about this issue because it has the potential to create divisiveness in your team. Remember, it is supposed to be the Total Army concept with an attitude of "one team, one fight." Civilian contractors augment the force and thus, in my view, should be considered part of the overall team effort. Many contractors are military retirees or have some amount of prior military service. Young Soldiers should not believe that contractors come off the street with no prior military experience, training, or qualifications. Army leaders at all levels should stress that contractors are part of the team.

Practical Advice

I offer some practical advice for military leaders utilizing civilian intelligence contractors and also some advice for civilian contractors supporting the military.

To the military leader:

- ✦ View and use your civilian contractor support as a force multiplier.
- ✦ Understand the contract Statement of Work and what contractors can and cannot do.
- ✦ Use the contractor company provided supervisors and managers to direct and task contractors.
- ✦ Remember that contractors are not Soldiers.
- ✦ The COR is the authority on your questions and the responsible officer for contract support.
- ✦ The military, through contractor supervisors and managers, control supporting contractors.

To the civilian contractor:

- ✦ Understand and follow the guidance provided to you (company SOPs, SOW, and ARs and policies).
- ✦ Conduct legal operations and support to the military; protect classified material.
- ✦ Always remember that the military is the customer; support the customer.
- ✦ In combat areas, expect austere working and living conditions.
- ✦ Get along not only with your military customer, but also with your fellow contractors (keep the personality conflicts to a minimum).
- ✦ Remember that you advise and support.

Conclusion

With the downsizing of the U.S. military at the end of the Cold War and the unexpected beginning of the War on Terror, senior government leaders have pursued outsourcing as a mechanism to augment our Armed Forces. The use of civilian contractors to augment MI activities will likely continue until the War on Terror is won or the present military force is greatly expanded. MI leaders must understand what capabilities civilian contractors bring to the fight and then integrate this personnel resource into the team to accomplish the mission.

Endnotes

1. **FM 3-100.21, Contractors on the Battlefield**, 3 January 2003, Preface.

2. Booz Allen Hamilton Historical Timeline Brochure, January 2005, 3.

3. FM 3-100.21 (100-21), 4.

4. Bill Sizemore and Joanne Kimberlin, "Blackwater: Inside America's Private Army: On the Front Lines," *Norfolk Virginian-Pilot*, July 25, 2006, 1.

5. Peter W. Singer, "Understanding the Private Military Sector," *Foreign Affairs,* March April 2005, 5.

6. Chris Mackey, *The Interrogators, America's Task Force 500 and Secret War Against Al Qaeda* (New York, NY: Little, Brown and Company, 2004), xxvi.

7. Department of the Army (DA) Memorandum, ATTN: DAMI-CD, Subject: Contractor Support to Army Counterintelligence (CI), 10 June 2004.

8. AR 715-9, Contractors Accompanying the Force, (Washington, DC: 29 October 1999), 13.

9. FM 3-100.21, 1-2.

10. Ibid., 4-13.

11. AR 715-9, 9.

12. Ibid., 14.

13. Ibid., 15.

14. FM 3-100.21, 4-1.

15. AR 715-9, 14.

16. Ibid., 14.

17. Singer, 5.

18. Stars and Stripes Mideast Edition, *"Army Secretary: Can't Compare Soldiers with Contractors,"* November 9, 2005, 6.

19. Ibid.

Major Harry P. Dies, Jr., U.S. Army, Retired, served as G2X CI/HUMINT Advisor (civilian contractor) to the 101st Airborne Division (Air Assault), Task Force Band of Brothers, in Iraq from 2005 to 2006. During his military career he served in South Korea and Germany, and deployed to Kuwait during Operation Desert Fox. He holds a BS from Austin Peay State University in Tennessee and has an MA from Webster University in Missouri. Readers may contact the author via email at harry.dies@us.army.mil.

TRAINING THE CORPS

USAIC's 35M10 HUMINT Collector Course—An Overview

by Mr. John Andruszka and Mr. George Stemler

Introduction

The 309th Military Intelligence (MI) Battalion has the responsibility for training the U.S. Army's 35M10, Human Intelligence (HUMINT) Collector Course, the Army's largest HUMINT military occupational specialty (MOS) producing course. The 309th trained over 1,150 new HUMINT Collectors during Fiscal Year (FY) 2006, which was a 345% increase above the FY 2002 (260) student training load. The annual student training load for FY 2007 and beyond, is projected to be in excess of 1,400 Soldiers.

Effective 1 October 2007, the old MOS 97E10 (Interrogator) will become MOS 35M10 (HUMINT Collector) as part of the Army's MOS realignment effort. During the 1990s, the role of the interrogator rapidly expanded as the need for HUMINT collection grew in response to ongoing operations in the Balkans and Southwest Asia. In these HUMINT centric environments, interrogators were used in source contact operations, force protection screenings, and friendly force debriefings. In 2000, the title of MOS 97E10 was officially changed to HUMINT Collector, which reflected the 97E's expanded HUMINT role.

Since 11 September 2001, the 35M10 Program of Instruction (POI) has undergone several course improvements to ensure it remains current and relevant with world events and Army mission requirements. In October 2006, the 97E10 course was lengthened from 16 weeks 3 days to 18 weeks 3 days to accommodate 19 new critical tasks, and command guidance from **FM 2-22.3**, **Human Intelligence Collector Operations**, 6 September 2006.

The War on Terror, the Army's modular force conversion, and the Army's intelligence transformation are fueling a tremendous operational requirement for HUMINT Collectors (See Figure 1). To meet the growing demand for HUMINT professionals, the Army increased the 35M10 student training load every year since FY 2002 (October 2001). Despite the increased work load, the 35M10 graduation rate increased to a historical high and feedback from field commanders has been overwhelmingly posi-

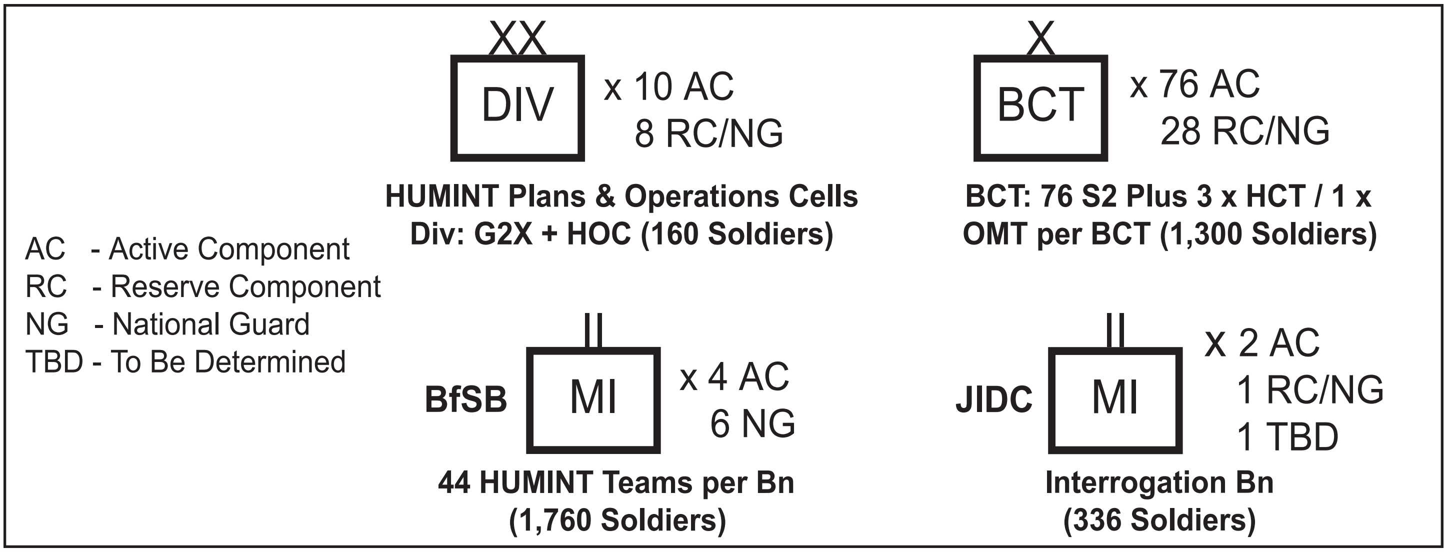


Figure 1. Projected HUMINT Capacity. Source: DA, Deputy CofS, G2, MI Transformation, 30 May 2007. Updated September 2007.

tive. Figures 2 and 3 compare the graduation rates and student loads between FY 2002 and FY 2006.

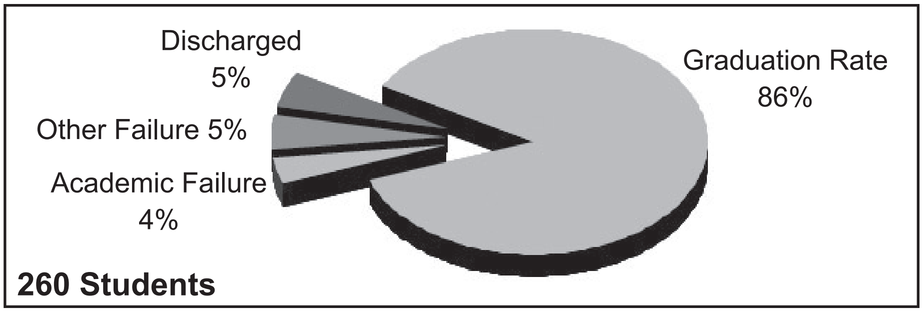


Figure 2. FY02 Student Training Load.

Educational Approach to 35M10 Training

Constructivism is extensively employed throughout the 35M10 curriculum. Constructivism is based upon the premise that learning is an active process and students will incorporate their current and past knowledge into their newly learned concepts to solve numerous curriculum based problem sets (which increase in complexity as the course progresses.) The learning environment within the 35M10 course ensures that students are active participants and are provided numerous opportunities for collaboration and team work with other students. Because the course is designed to create a hands-on experiential environment, each Soldier is able to explore and learn new concepts and ideas relevant to the goal of graduating and becoming a productive and efficient HUMINT Collector.

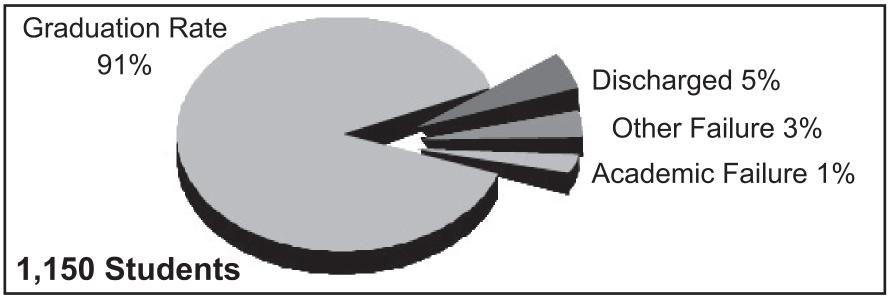


Figure 3. FY06 Student Training Load.

There are 51 critical tasks trained and evaluated during the 35M10 course. The course incorporates the six levels of intellectual behavior important in learning as identified by Benjamin Bloom. Collectively, the six levels (within the cognitive domain) are known as Bloom's Taxonomy, and range from the lowest level (simple recall of facts) to the most complex cognitive level (evaluation). The 35M10 course utilizes Bloom's Taxonomy to measure each Soldier's level of competency for each of the critical tasks trained, using criterion referenced hands-on performance or performance based testing. Figure 4 depicts the distribution of training within Bloom's taxonomy as applied to the critical tasks evaluated during the course.

35M10 Course Scope

Soldiers graduating from the 35M10 Course are fully prepared to rapidly assimilate into their permanent units as a HUMINT Collector. Course instruction reflects lessons learned from the ongoing theater operations in Iraq and Afghanistan, human source contact operations, detention camp opera-

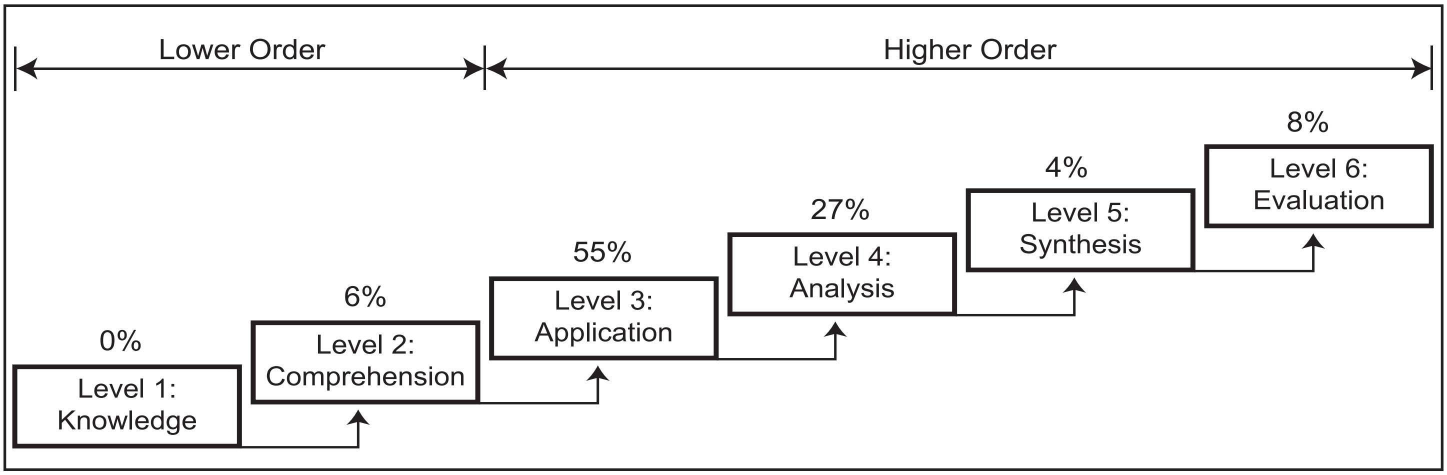


Figure 4. Bloom's Taxonomy.

tions, general area of interest (AI) target knowledge, and cultural aspects of the AI. Throughout the course, students learn to fully incorporate Military Justice and Intelligence Law into HUMINT collection services and operations. They practice interrogation techniques and procedures to include planning and preparation; questioning techniques; screening; assessment; approaches; research, and the application of analytic skills to curriculum problem sets. Students write numerous HUMINT related reports; identify information gaps; perform predictive analysis, and prepare link diagrams, time event charts, and activity and association matrices. Students learn to coordinate mission requirements with interrogators, interpreters, and translators to meet mission or unit requirements and are familiarized with Distributed Common Ground Station–Army (DCGS-A) system as part of their HUMINT automation training.

35M10 Course Organization

The HUMINT Collector Course is organized into four academic modules. Each module builds progressively upon the skills and knowledge acquired in previous modules. The four modules are linked by a common operational scenario allowing for progressive situational awareness and realistic cause-and-effect during student practical exercises and performance evaluations. The fourth module is the course's capstone field training exercise (FTX). All fifty-one 35M10 critical tasks (previously evaluated) are reinforced during the FTX. Throughout the exercise, students are placed into demanding situations which challenge their comprehension and application of the critical tasks in conditions designed to simulate operations in Iraq and Afghanistan. Figure 5 depicts the percentage of the course devoted to each training module.

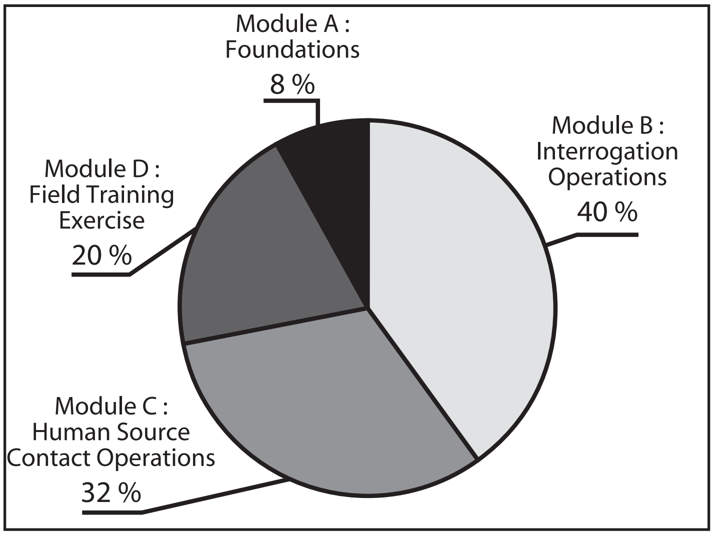


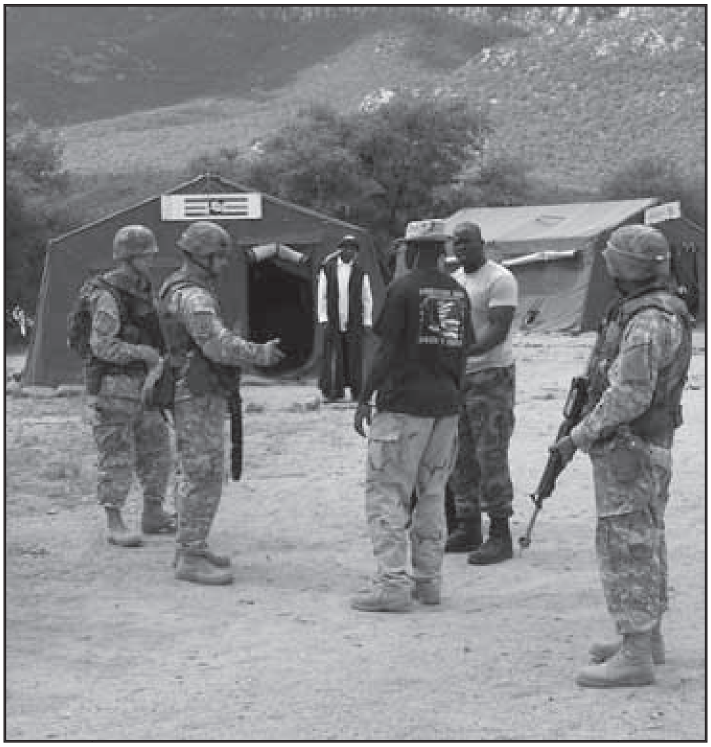
Figure 5. Percentage of course by Training Module.

Module A—HUMINT Foundations.

During the 10 day (68.5 academic hours) HUMINT Foundations module, students are trained and evaluated in map reading, Intelligence Oversight, Law of Land Warfare, Information Security, and protecting classified material. These academic areas are continuously reinforced throughout the course. All legal training is conducted by Judge Advocate General lawyers with experience in HUMINT collection operations. In addition, students are introduced to information and skills such as the Biometric Automated Tool System, Analytical Tools, the FalconView™ mapping application, cultural awareness, and the intelligence process. During Module A, students are organized into HUMINT Collection Teams (HCTs) and begin receiving operations orders; intelligence summaries; contemporary operating environment order of battle factors, and collection requirements based upon the course's Iraq scenario.

Module B—Interrogation Operations.

During the 44 day (332 academic hours) Interrogation Operations module, students carry out



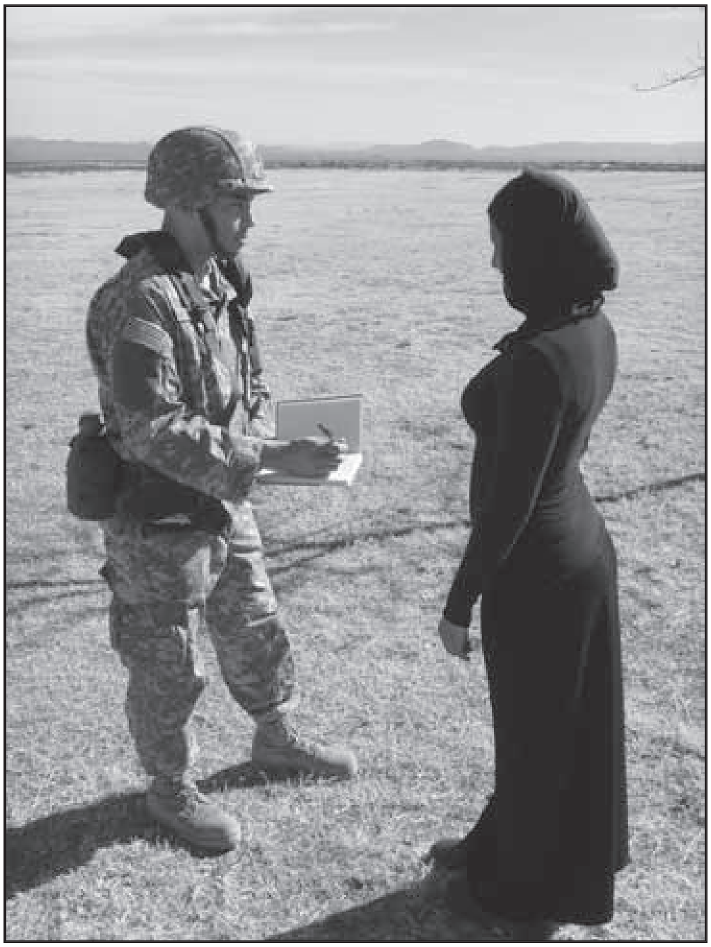
Students encounter "hostile villagers."

duties as if assigned as an interrogator in a Joint Interrogation and Debriefing Center (JIDC). Students conduct coordination with Military Police elements, screen detainees for potential answers to intelligence collection requirements, and prepare screening reports using the knowledgeability brief (KB) format found in FM 2-22.3. Students complete all five phases of HUMINT collection, to include: planning and preparation, approach, questioning, termination, and reporting. Every student is required to produce an interrogation plan consisting of a questioning sequence designed to obtain the information unique to their detainee and scenario driven collection requirements. Using trained role players (one-on-one) as detainees, students conduct nine evaluated interrogation practical exercises. Each detainee's role is culturally correct and designed to evaluate the student's orchestration of approved approach strategies, questioning skills, and awareness of deceit and deception. Students are required to report any suspected law of war violations as well as any information that may be of counterintelligence (CI) interest. Every interrogation exercise is digitally recorded and used for after action reviews (AARs) and retraining. In addition to the interrogation exercises, students learn to exploit captured enemy documents (DOCEX) and debrief friendly forces. Students learn to report intelligence information by writing numerous SPOT reports and Intelligence Information Reports (IIRs). Throughout the scenario-driven Interrogation Operations module, students conduct HUMINT analysis while using analytical tools such as activities matrices, association matrices, link diagrams, and time event charts.

Module C—Human Source Contact (HCT) Operations

During the 29 day (261.5 academic hours) Human Source Contact (HCT) Operations module, students continue to operate in their designated HCT created during Module A. Each student in the HCT must plan and conduct HUMINT operations and collect intelligence from one time sources, continuous contacts and formal contacts. Throughout the module, students are required to conduct operational reconnaissance, use communications plans and take other actions to ensure the physical and operational security of their HUMINT operation. The physical and operational security requirements are made relevant to the student by conducting the module's practical exercise outside of the normal academic area. Building upon skills learned in Module B, students are challenged with a variety of culturally correct role players during 15 different hands-on practical exercises. Each student must assess multiple potential sources and spot at least one source for use during the module while maintaining a source dossier. Students are evaluated on their ability to conduct a liaison meeting, a one time source meeting, a recruitment meeting, and a formal contact meeting.

Student technical report writing skills, evaluated in previous modules, are again evaluated for relevancy and doctrinal correctness. Reports include Operational Reconnaissance, Contact, Communications Plans, Source Lead Development, Operational Reviews, and Biographical Source Data. Students continue to update their analytical tools, first created in Module B, in support of the scenario's ongoing Human Source Contact Operations (HSCO). Each student HCT provides information briefings to their operational management team (OMT) and



A student interviews a role player "local villager".

Students interview the local "police chief".

to the other student HCTs as they gain an understanding of the scenario's threat organization, modus operandi, and intentions. The scenario's realistic operational conditions also provide students the opportunity to correctly use and account for Intelligence Contingency Funds (ICF). Use of an interpreter is taught, practiced, and evaluated; and, if available, MOS 09L, Interpreter/Translator Soldiers (assigned to Fort Huachuca) are incorporated into Module C graded exercises.

Module D—Field Training Exercise.

During the 10 day (164 academic hours) FTX, students continue to operate with their HCT against the course's scenario based threat(s). All 51 of the 35M10 critical tasks, trained, and evaluated in the three previous modules, are reinforced as the students operate a brigade interrogation facility. During the FTX, students conduct screenings and interrogations on the objective, HSCO in mock Iraqi villages (populated by trained and scripted "Iraqi" role players), and screen personnel at traffic control points (TCP). During the FTX, each student must perform several challenging interrogations, screen large groups of potential sources, and collect information from one time sources and continuous contacts while maintaining operational security in the FTX's "Iraqi" villages. Students must work as teams to collectively plan and conduct HUMINT collection missions outside of the FTX's forward operating base. All HCTs are required to brief their OMTs and the CI/HUMINT Operations Manager (2X) daily. Immediately following each task and mission an instructor-led "hot wash" or AAR is conducted. The AAR helps to ensure students receive immediate feedback concerning their mission performance. Detailed AARs are also conducted at the end of each duty day. During the FTX, students are certified as fully qualified on the TRADOC Warrior Tasks and Battle Drills, which are in addition to their MOS critical tasks. Students leave the 35M10 FTX field site tactically and technically proficient in their MOS and ready to graduate the 35M10 HUMINT Collector Course.

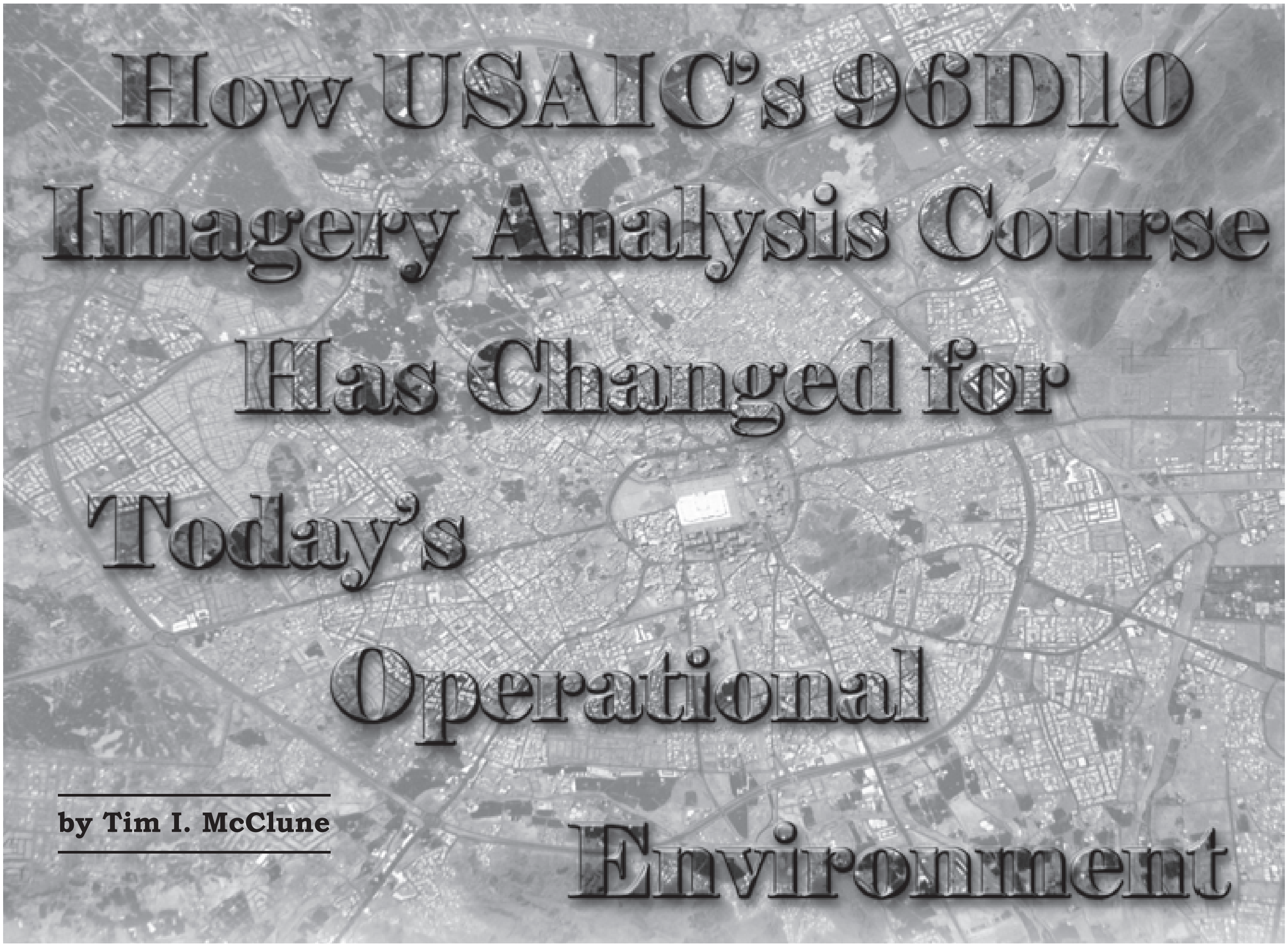
Conclusion

As the Army moves to create modular tactical intelligence force packages capable of rapidly responding to global hotspots, it is imperative the modern HUMINT Soldier is prepared for the rigors of an immediate deployment upon graduation from advanced individual training (AIT). The 309th MI Battalion is fully committed to its AIT training mission, and Soldiers graduating from the 35M10 course are receiving the best initial HUMINT training resources allow. For the foreseeable future, the 309th will do its part to ensure highly trained and disciplined HUMINT Soldiers are prepared to make a positive impact towards fighting the War on Terror.

Mr. George Stemler is the 309th MI Battalion's Senior Civilian Training Specialist. Mr. Stemler has worked as a civilian Training Specialist since retiring from the U. S. Army in 1999 after 20 years of military service. He holds an MS from the University of Phoenix in Computer Information Systems and a BS from Wayland Baptist University in Education with a minor in Business Management. Mr. Stemler can be contacted at 520-533-2262, or by email at George.I.Stemler@us.army.mil

Mr. John Andruszka is a DA Training Specialist in the 35M10 course. Mr. Andruszka has worked as a Training Specialist since retiring from the U.S. Army in 2004 after 20 years of military service. He holds a BS from Wayland Baptist University in Education with emphasis in Intelligence Operations and Computer Information Systems and an AAS from Cochise College in Intelligence Operations with an emphasis on Interrogations. Mr. Andruszka can be contacted at 520-533-4368, or by email at John.Andruszka@us.army.mil.

How USAIC's 96D10 Imagery Analysis Course Has Changed for Today's Operational Environment



by Tim I. McClune

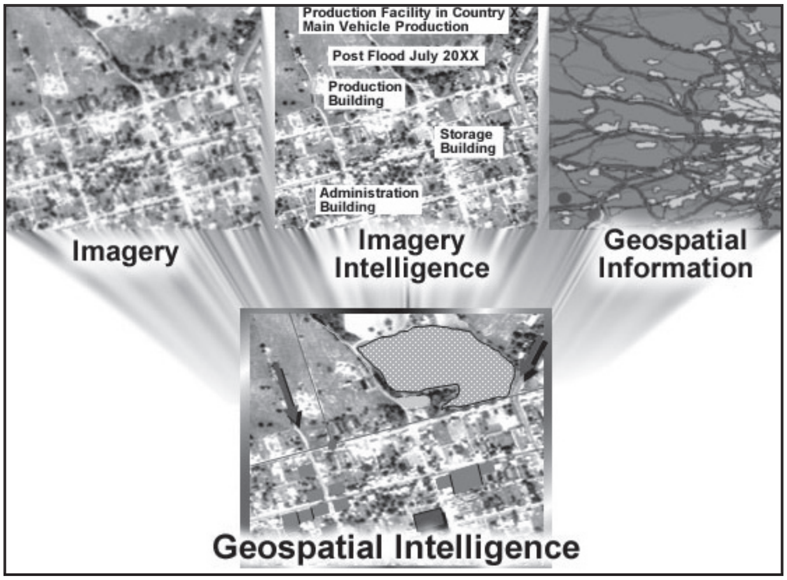
Introduction

When I became an Imagery Analyst in 1984 we were still fighting a Cold War and our training centered on large static targets. The reconnaissance and surveillance assets of the of the Vietnam era were still being taught even up to the Gulf War in 1991. Students were expected to learn the majority of their job after they graduated. After the Gulf War things started changing. Our world became very different as technology was quickly evolving. The Berlin Wall was finally torn down, effectively ending the Cold War. The Army is now concerned with fighting small limited wars and counterinsurgency operations (COIN) along with peacekeeping missions in areas such as in Bosnia.

The imagery environment has evolved to meet the new operational environment in several ways. Advances in computer technology now allow us to process digital data and data files can be searched, sorted, and stored for future reference. Images that used to be wet processed on a film base and stored on long rolls are now stored digitally where one image can easily be referenced to another. Digital data can be merged or layered onto the image to create enhanced intelligence products. The second change was the Internet. The World Wide Web allows us to easily share information. We can transmit data and intelligence anywhere in the world, often in near real time. Warfighters can access imagery and information even in a combat zone.

The third event that changed everything was 9/11. Terrorism is not new; in the past we saw it happen in other countries in the news. But the events of September 11, 2001 made all Americans aware that it was our problem too. The terrorist attacks made us realize that we are now fighting a shadowy adversary that doesn't necessarily have fixed bases, a defined order of battle, or even a uniform. Instead of identifying equipment and static targets we are looking for individuals. Critical thinking, collaboration and knowledge sharing are keys to rooting out terrorists. Instead of carpet bombing large targets we now need to strike a single building or vehicle with surgical precision in order to limit collateral damage. Our primary weapon is the dismounted soldier who must kick in doors and engage the enemy at arm's length.

The last change was the use of geospatial information by imagery analysts. Not too long ago the topographic analyst provided geospatial information to intelligence analysts as part of the Intelligence Preparation of the Battlefield (IPB) process. Today geospatial information is critical in identifying patterns of activity to cue forces to find and kill terrorists. Because this is an intelligence function, the time has come for imagery analysts to become proficient in some geospatial tasks. The imagery analyst blends imagery, geospatial information, and imagery intelligence into one intelligence product. A product created in this way is referred to as geospatial intelligence or GEOINT. Because of this the imagery analyst is now *commonly* called a GEOINT analyst, although this is not an official designation.



Changes to the 96D10 Imagery Analysis Course

The Imagery Analysis Course taught at Fort Huachuca was designed around Cold War doctrine and conventional warfare. 9/11 made some imagery critical tasks obsolete and started a round of critical thinking about what skills an imagery analyst would need to have acquired upon course completion. A country at war needs Soldiers who can successfully perform their mission as soon as they get to their first assignment; many are finding themselves in a combat zone within weeks after advanced individual training. Prior to 9/11 it was assumed that a Soldier would learn many basic and intermediate skills at their unit during the first year or so. Today, a soldier assigned to a brigade combat team (BCT) will have no time to develop skills, and due to the limited number of imagery analysts in the unit, the new Soldier may very well be the senior imagery analyst in the unit.

Therefore, the course had to prepare Soldiers to perform tactical missions using advanced technology to meet the needs of a modern Army fighting on a digital battlefield. They must be able to provide imagery and geospatial intelligence against terrorists and insurgents in a timely manner. This is certainly the most difficult mission for an imagery analyst due to the nature of unconventional warfare. The lack of static targets and military equipment limits the usefulness of conventional imagery. Imagery of transitory targets and unconventional facilities must be merged with other data and geospatially referenced to make useful intelligence.

To prepare our Soldiers for today's mission we had to first assume they would deploy immediately into a combat zone. The basics must still be taught such as map reading, imagery analysis techniques, and vehicle identification. But today the student is also introduced to digital geospatial information at the very beginning of the course. During the Map Reading instruction, students are quickly introduced to Compressed Arc Digital Raster Graphics (CADRG) and Digital Terrain Elevation Data (DTED). We start with FalconView™ as the first visualization tool the students see; it is easy to learn and is useful for geospatial visualization. The students learn the basics of GEOINT and the four main types of data (raster, vector, matrix, and textual.) Later in the course they will explore this data in depth using more advanced tools.

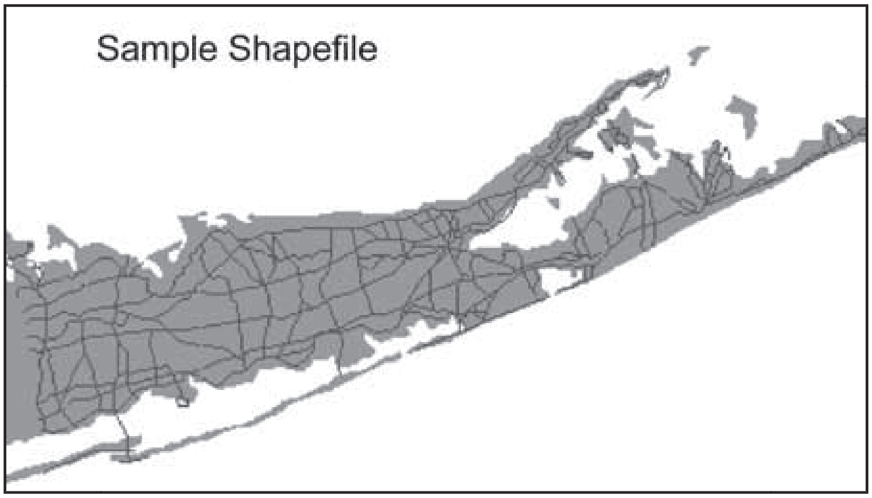
The precursor to Battle Damage Assessment (BDA) is Targeting. Students learn to use digital point positioning data base (DPPDB) and provide mensurated points using the targeting software, Digital Precision Strike Suite (DPSS). The main tool we use is Precision Strike Suite for Special Operations Forces (PSS-SOF).

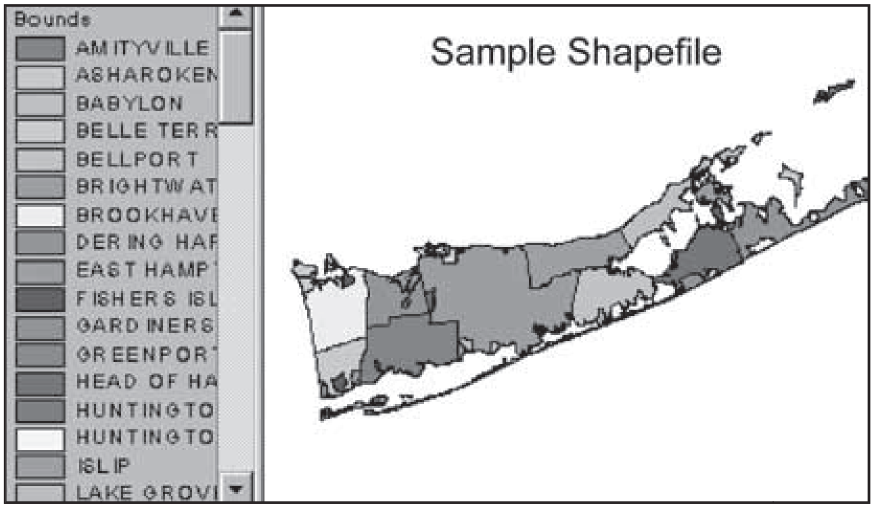
Reports used to be a paper-based exercise where students literally hand wrote imagery reports. Now students enter reports in the common report writing software, Imagery Exploitation Support System (IESS).

Students learn about imagery databases and how to research targets. They download National and commercial imagery, CADRG, and DTED as if they were in the field and satisfying a requirement. The emphasis is making sure the student knows data is available and how to get it. After researching a target, the students create imagery derived products and prepare professional military briefings. Instructors usually critique the students but often guests such as visiting officers and warrant officers attend the brief and provide valuable feedback to the students.

Students get excellent training in advanced geospatial intelligence (AGI) or Imagery Derived MASINT. They actually produce two color multiview (2CMV) products in class along with other products and then brief their own products. Not only can the students recommend the best imagery derived MASINT product to satisfy a requirement, but they also know how they are produced and how to interpret the product.

With the inclusion of GEOINT, the imagery analyst's mission has evolved largely due to the types of data that can be processed geospatially in addition to images. Detailed analysis can be performed on imagery in conjunction with collected database information in order to detect patterns of activity that give away terrorist and insurgent movement. We live in a visually oriented world. Our students grew up with computers and video games; therefore, they learn to work with geospatial data very quickly. In the field, the customers the GEOINT analysts support also want to be able to visualize data. Database information is often best portrayed geospatially and merged as layers over an imagery base. To build layers of geospatial data the students are learning to work with ESRI's ArcGIS. They create raster databases and import Shapefiles as layers. They also create their own Shapefiles and learn the importance of attributes associated with each feature. Finally, the students export their data as a product that satisfies the needs of the requestor. Geospatial data can be exported as Shapefiles, spreadsheets and databases as well as special products such as PowerPoint presentations and interactive maps. This is all done in class using raster data such as CADRG or imagery as a spatial reference.





Training at the JI-CTC

The last phase of the course is the situational training exercise (STX) conducted at the Joint Intelligence-Combat Training Center (JICTC). Here the students, in a division ACE GEOINT Cell, operate in various positions where technical competence, leadership, briefing skills, and critical thinking skills can be honed and assessed while performing GEOINT tasks in a stressful environment. The main focus in the exercise is the unmanned aerial system (UAS) simulator using Multi-User Simulator Environment (MUSE) software.

Several tools are available that the students will also see when they get to the field. Students use FalconView™, RemoteView, and ArcGIS as visualization and exploitation tools. We are currently evaluating Socet-GXP as an exploitation tool. PSS-SOF is used for targeting and when a mensurated point is required. The students communicate through mIRC, a chat tool, and Voice over Internet Protocol (VOIP) which is used for secure voice communication. Every effort is made to incorporate the Distributed Common Ground Station-Army (DCGS-A) tools whenever possible.

Training in the STX is focused on using imagery, geospatial data, and intelligence to keep the warfighter informed of the current situation and to help predict what the enemy is going to do next. Students manage UAS operations in COIN missions as well as a conventional warfare situation. 2CMV AGI products are created in response to intelligence requirements and are included in the daily brief. Recent additions to the STX include using commercial and National imagery as well as full motion video to satisfy information requests generated from other exercises within the JI-CTC. Students manage a requirements database and attempt to answer each request with a suitable GEOINT product. Through this they learn the basics of time and asset management. During the exercise targeting scenarios are introduced as time sensitive requirements for mensurated points. The result of the targeting is witnessed by a UAS on station and the student can report BDA.

A Joint Service Work Station (JSWS) simulator is used to provide cross cueing for UAS operations. Our students are instructed in the basics of moving target indicator (MTI) analysis prior to the STX. The UAS mission manager communicates with the mission planner through mIRC chat tool and VOIP. The NCOIC communicates with the cadre using the same means to receive missions and intelligence reports. Tactical reports (TACREPS) are passed over VOIP and also posted to PathFinder.

Each day ends with the Battle Update Brief. Students prepare a professional military brief for the commander complete with PowerPoint slides, GEOINT products, and AGI. The students are preparing for the brief all day and are eager to report the successes of the day, yet are anxious about facing the commander to report mission failures. Not every scenario has a happy ending. The ultimate outcome depends upon student interaction, reactions to situations, and communication. Feedback is critical to learning so each day ends with an after action review where each situation is discussed and lessons are learned so mistakes will not be repeated. Each morning begins with a new mission and another chance to excel.

Conclusion

The key to GEOINT training today is to continue to train the basics and then focus on today's counterinsurgent/counterterrorist situation, by having the students prepare professional GEOINT products that satisfy a particular intelligence need. The students learn to work as individuals and as a team to ensure success using DCGS-A tools whenever possible. Students graduate the 96D10 course knowing full well they are likely to be in a combat zone on their first assignment. We cannot assume they will have a year or more to learn the skills necessary to perform their mission. We provide them with the skills, knowledge, and experience to work in a production center, division ACE or a BCT as part of a GEOINT team.

The Soldier and civilian cadre here at Fort Huachuca are dedicated to producing the finest Imagery Analysts. Feedback from the field is critical to improving the quality of our training. Many of our scenarios are based on real situations. As operations continue in areas such as Iraq, we will continue to update training based on lessons learned. The Soldiers graduating this course will not only be on the cutting edge of GEOINT technology, but will hopefully lead the field by introducing their peers and supervisors to new and better ways to analyze geospatial data.

Mr. Tim McClune enlisted in the Army in 1984 and graduated from the Imagery Analyst Course at Fort Huachuca, Arizona. His imagery analysis assignments include CM&D, III Corps, Fort Hood, TX; 452nd MI Detachment, 172d Light Infantry Brigade, Fort Richardson, Alaska; V Corps ACE, IMINT Requirements, Heidelberg, Germany, and Third U.S. Army, IMINT Requirements, Fort McPherson, Georgia. He was deployed in support of the V Corps DISE; Operation Joint Endeavor; and TSAR AB, Hungary 1996 Coalition Task Force. He instructed imagery analysis at the 5-104 MI Battalion (USAR) and was a training developer for the National Geospatial-Intelligence Agency. As a civilian, Mr. McClune has served as an instructor and training developer for USAIC. Currently, he is responsible for developing the 96D10 STX and incorporating GEOINT training into the course.

UNITED STATES ARMY
INTELLIGENCE AND SECURITY COMMAND
INSCOM
30 YEARS★1977-2007
The US Army's Operational Intelligence Force

Three Decades of Service

By Michael E. Bigelow, INSCOM History Office

This article was first printed in the Winter and Spring 2007 INSCOM Journal.

Introduction

This year marks the U.S. Army Intelligence and Security Command's (INSCOM) thirtieth year. Over these three decades of service, INSCOM has provided intelligence support to the Army that helped win the Cold War as well as successfully fight regional conflicts. INSCOM's personnel supported the myriad of peacekeeping, treaty verification, stability, and humanitarian operations. More important, they continue this service with support to the current War on Terror.

The command's establishment in 1977 was a radical departure from previous Army intelligence organizations. Since then, INSCOM has effectively transformed itself as needed to remain relevant to the Army. During the 1980s, INSCOM sought to make its units more deployable. Then, with the end of the Cold War, it had to assume new missions as its resources were diminishing. The resulting change involved not only the command's restructuring, but also a change in mindset. Instead of a well-ordered tier of tactical, operational, and strategic intelligence assets, intelligence assets had to be tied together with a seamless connectivity, and INSCOM became the linkage between national assets and the deployed warfighter. The current War on Terror made this connectivity even more imperative, and INSCOM has added rigor and consistency in bringing the national intelligence capabilities to bear on the tactical commander's problems. In short, INSCOM has continued to reshape itself and assess its methods with the goal of providing ever better intelligence support.

Establishing the Command (1977-1981)

In the mid-1970s, the Army undertook a major restructuring of its intelligence components. Since World War II, these various components had developed in isolation, often according to their own priorities and agendas. With significant budget cuts looming, General Frederick C. Weyand, the Army Chief of Staff, believed it was an opportune time to re-examine Army Intelligence. In 1974, he commissioned the Intelligence Organization and Stationing Study (IOSS) to evaluate the intelligence structure that had evolved haphazardly. A panel of senior officers headed by Major General James J. Ursano undertook the study. Released in mid-1975, the IOSS study recommended that the Army break up existing intelligence organizations and reassemble them into a new configuration. These recommendations led to the most sweeping reorganization of Army intelligence in a generation.

Major General William I. Rolya

At the center of this transformation was the break-up of the U.S. Army Security Agency (ASA), the Army's large Signals Intelligence (SIGINT) organization. The Army stripped ASA of its training center and research and development activities, and assigned them to the U.S. Army Training and Doctrine Command (TRADOC). Furthermore, ASA's tactical SIGINT units were resubordinated to the tactical units they supported. Finally, the remaining nucleus of ASA was merged with U.S. Army Intelligence Agency (USAINTA) at Fort Meade, Maryland and various small production elements to form a new major Army command. On 1 January 1977, ASA was redesignated the U.S. Intelligence and Security Command (INSCOM) with Major General William I. Rolya as the first commanding general.

Headquartered at Arlington Hall Station in Virginia, INSCOM was considerably smaller than ASA, but it still controlled a vast array of diverse assets. Initially, this included four overseas military intelligence (MI) groups, a variety of functional units, and eight fixed field stations. Initially, USAINTA operated as a separate command under INSCOM, but the two headquarters merged on 1 October 1977, thus completing the integration of high-level intelligence organizations for the Army. In broad terms, this new organization was to perform multidiscipline intelligence, security, and electronic warfare functions at the echelons above corps.

To provide intelligence support to the Army's overseas theaters, INSCOM relied on its deployed MI groups. These groups were multidiscipline elements, formed by integrating former ASA assets into existing intelligence units. Originally, INSCOM had three such units: the 66th MI Group in Germany, the 470th MI Group in Panama, and the 500th MI Group in Japan. In early 1978, the 501st MI Group was established in Korea. INSCOM tailored the four groups to meet theater-specific requirements, and each of them varied in size, mission, and composition. The 470th MI Group that supported a two-battalion infantry brigade in Panama was relatively small; at the same time, the 66th MI Brigade, which supported the two-corps USAREUR, was large. To support the U.S. Eighth Army, the 501st MI Group included INSCOM's only aerial exploitation battalion. Meanwhile, the 500th MI Group in Japan was primarily a human intelligence (HUMINT) outfit. Regardless of size and composition, however, the theater commanders retained operational control of these groups.

In addition to the theater support groups, INSCOM received control of various single-discipline elements. An expanded 902d MI Group handled both a counter-intelligence and signal security support mission throughout the continental U.S. The CONUS MI Group provided Army cryptologic personnel to the National Security Agency. The Operational Group engaged in HUMINT collection operations, while the Special Operations Detachment handled the most sensitive CI operations.

INSCOM also controlled a number of former ASA fixed installations. Six of these sites were located overseas: two in Germany, two in Japan, one in Turkey and one in Korea. Two sites were in the continental U.S. Known as "field stations," they varied in size, but all operated sophisticated communications equipment. Throughout the early years of INSCOM, these sites remained extremely important collection assets.

Over the first few years, INSCOM steadily expanded and acquired new missions. From the several production assets, INSCOM established a unified production element, the Intelligence and Threat Analysis Center (ITAC) on 1 January 1978. Later, it assumed control over the U.S. Army Russian Institute in Germany. In late 1980, the Army set up a new field station—the first since the Vietnam War—at Kunia, Hawaii, and assigned it to INSCOM. Field Station Kunia became a joint service organization under INSCOM's administration.

By bringing together the full spectrum of intelligence disciplines, INSCOM provided the Army with a single instrument to conduct and coordinate intelligence operations at the level above corps and to provide finished intelligence tailored to the Army's needs. The new command established a framework for the various elements of the Army's intelligence system to cross-cue one another, resulting in a collective effort so the whole is greater than the sum of the parts. It also provided a central organization for the administration of personnel and logistics in support of national agencies and theater commanders. By the time he turned over command in 1981, MG Rolya had ensured that INSCOM was the centerpiece of the Army's intelligence organization.

513th MI Brigade on Parade at Fort Monmouth, New Jersey during reflagging ceremony in 1986.

Winning the Cold War (1981-1989)

Responding to growing threats abroad, the U.S. reinvigorated its military during the 1980s. A strengthened Army was able to field new, sophisticated weapon systems and to develop new warfighting doctrines. The Army's intelligence system also benefited during this time of plenty, and INSCOM provided an invaluable base onto which the Army could build an expanded intelligence program.

When Major General Albert N. Stubblebine assumed command of INSCOM, he promptly announced his commitment to preparing it for war. One of the most tangible steps towards this goal was the establishment of the 513th MI Group at Fort Monmouth, New Jersey in 1982. INSCOM activated the group to support possible operations of the newly organized U.S. Central Command, which had been set up to defend American interests in the Middle East. The new organization included a tactical signals intelligence battalion, a counterintelligence (CI) battalion, and a technical intelligence battalion. In case of war in Europe, the 513th would deploy in Germany to join the 66th MI Group in its support of USAREUR.

The 513th's activation signified INSCOM's commitment to provide deployable support to the Army. In 1986, the 513th as well as the four overseas multidiscipline intelligence groups were redesignated as brigades. This transition was more than a superficial name change. Now the units were organized for possible warfighting rather than simply having structures geared to peacetime collection requirements. Still, the diversity of intelligence requirements in the various theaters meant the brigades retained specialized and varied organizations.

Meanwhile, INSCOM also organized troops manning some of its SIGINT organizations into numbered MI brigades and battalions. This initiative was designed to enhance and develop *esprit de corps* among

INSCOM Headquarters, Fort Belvoir, Virginia.

INSCOM Soldiers and provide units with appropriate designations that would be more familiar to the Army as a whole.

Since the end of the Vietnam War, the Army had emphasized its role in the defense of Western Europe against the Soviet threat. Reflecting this orientation, INSCOM allocated considerable resources to Europe. With a peak strength of 2,500 personnel, the 66th MI Brigade was the command's principal unit in theater and engaged in a broad range of CI, HUMINT, and specialized electronic warfare operations. INSCOM also continued to operate two field stations in Germany—Field Station Augsburg (now the 701st MI Brigade) in Bavaria, and Field Station Berlin, 105 miles behind the Iron Curtain—to collect against the Soviets and their Warsaw Pact allies. Finally, INSCOM personnel manned Field Station Sinop on Turkey's Black Sea coast.

Although Europe remained the primary focus for the Army, INSCOM also maintained an active presence in the Pacific throughout the 1980s. In Hawaii, its troops manned a theater intelligence center on Fort Shafter. Moreover, Soldiers under the newly organized 703rd MI Brigade manned the Kunia field station, near Schofield Barracks, Hawaii. The station's sophisticated communication systems allowed INSCOM to close down older facilities in the Far East. In Korea, INSCOM's large 501st MI Brigade continued to monitor the Demilitarized Zone in its support of the U.S. Eighth Army. In Japan, the smaller 500th MI Brigade supported U.S. Army, Japan as well as satisfying theater and national intelligence requirements.

In the Western Hemisphere, INSCOM continued to maintain its presence in Panama. In 1982, the command established a new field station and subordinated it to the 470th MI Brigade. Initially, the brigade concentrated its efforts on gathering intelligence on the unstable political environments in Panama, Nicaragua and El Salvador. Later, it would broaden its scope to support counterdrug operations in South America. To assist the 470th, INSCOM activated an experimental unit to utilize new aerial collection systems and other sensors against leftist insurgents in Central America. This unit later evolved into the MI Battalion, Low Intensity, using the Aerial Reconnaissance Low (ARL) System.

In the U.S., INSCOM's CONUS MI Group became the 704th MI Brigade. In addition to its mission to support NSA, the 704th assumed management of the Army's new TROJAN program that provided Army units in CONUS with access to live signals environment for training. The 902d MI Group remained INSCOM's principal CI organization, but it underwent reorganization. In 1985, the group's subordinate elements were restructured along a functional, rather than geographic, basis. In the process, the group moved away from a concept of providing general security support toward one focusing on priority objectives, such as polygraph examinations, technical services countermeasures and counterespionage operations in the continental U.S.

In a time of increased emphasis on CI, INSCOM scored two significant triumphs. In 1988, INSCOM CI agents in Europe tracked down Clyde Conrad, a retired Army noncommissioned officer who was a key figure in an espionage ring who betrayed NATO war plans to the Hungarian intelligence service. Later, INSCOM's Foreign CI Activity (formerly the Special Operations Detachment) arrested Army Warrant Officer James Hall, who sold American secrets to the Soviets.

During this period, INSCOM lost its intelligence production function. In 1984, the Army removed ITAC from INSCOM as the basis for the newly formed Army Intelligence Agency. With the departure of ITAC, INSCOM was able to concentrate on its principal mission: managing the Army's strategic and theater-level intelligence resources.

Ever since INSCOM's organization in 1977, its headquarters staff elements had operated at both Fort Meade and Arlington Hall Station. Nine years later, INSCOM was finally able to consolidate all headquarters elements at Arlington Hall. Unfortunately, this location lacked sufficient office space and could not adequately support INSCOM's growing communications and automation networks. Consequently, the Army decided to build a new headquarters on Fort Belvoir. During the summer of 1989, the INSCOM staff moved into the new building, named after Maj. Gen. Dennis Nolan, the G2 of the American Expeditionary Forces in World War I.

Regional Conflicts and Drawdown (1989-2001)

No sooner had the staff settled into the Nolan Building, the Cold War ended with the sudden fall of the Berlin Wall in late 1989. This fortuitous outcome, however, only presented INSCOM with a new set of challenges. Largely structured and deployed with the Cold War's priorities in mind, INSCOM began to search for a new role in the transformed world. Yet, just as the Cold War ended, INSCOM found itself in the middle of a new conflict.

At the end of 1989, Panamanian strongman Manuel Noriega posed a threat to U.S. interests and provoked an American military intervention, Operation Just Cause. As American task forces fought Noriega's security forces, INSCOM's 470th MI Brigade deployed its assets to support the operation. Intimately familiar with both the terrain and the disposition of Panama's armed forces, teams from the 470th provided spot reports throughout Panama City. Using their sources, 470th Soldiers obtained critical information on troop movements and locations of weapons caches. After the fighting, they helped identify and apprehend a number of Noriega's top aides. For its role in the operation, the 470th was awarded a battle streamer.

Less than a year later and halfway across the world, another crisis developed when Iraqi troops crossed into Kuwait. American ground, naval, and air forces quickly deployed in Saudi Arabia to prevent further Iraqi expansion. Once the situation stabilized, elements of INSCOM's 513th MI Brigade began to arrive on the Arabian Peninsula with a full array of assets. In addition, Major General Stanley H. Hyman, INSCOM's commanding general, and his successor, Major General Charles Scanlon, used the resources of their command to compensate for any deficiencies in the intelligence effort to support the CENTCOM's Army component (ARCENT). Companies and teams from the 66th MI Brigade as well as reservists from the U.S. deployed to support the 513th. By Christmas 1990, the brigade had deployed over a thousand Soldiers.

Quickly, intelligence professionals from INSCOM proved their worth. Before Operation Desert Storm, the offensive against the Iraqi forces, a terrain team assured Army planners that the desert area around Kuwait was trafficable by Army tanks and armored vehicles. INSCOM technicians reconfigured the TROJAN system, formerly a training system, for use as a secure intelligence communication link that could transmit real-time information down to the division level. INSCOM also provided force protection teams at the ports, and technical intelligence teams to train U.S. forces on Soviet equipment used by the Iraqis.

During the U.S.-led offensive, INSCOM elements played key roles in several of CENTCOM's joint intelligence centers, and the 513th's echelon-above-corps operations center was expanded to a full operations battalion and placed in support of ARCENT's G2. As Allied forces quickly smashed the Iraqi military, INSCOM CI personnel were among the first to enter the liberated Kuwait City where they policed up documents and provided essential force protection. When the fighting came a halt, INSCOM human and technical intelligence specialists were busy screening and examining 50,000 Iraqi prisoners, thousands of documents, and numerous pieces of Soviet-made equipment.

The challenges of Just Cause and Desert Storm placed large demands on the Army's intelligence community. INSCOM played no small part in meeting these demands. Fortunately, INSCOM's major players had been correctly postured. For Just Cause, the 470th had been in place for more than a decade when the crisis broke. For Desert Storm, the 513th had a long-standing contingency mission to support ARCENT. In both cases, INSCOM had been able to draw on resources built up for the Cold War.

Once Desert Storm successfully ended, however, the drawdown of those Cold War resources began in earnest. For INSCOM, the most noticeable cutbacks occurred in Europe where it closed three major field stations—Berlin, Augsburg, and Sinop—and downsized the 66th MI Brigade to a provisional group. In addition, the joint European Command took control of the Army Russian Institute from INSCOM. Reductions were not, however, limited to Europe. In 1997, the Army inactivated the 470th MI Brigade reduced the 500th MI Brigade in Japan to group status. Earlier, INSCOM had transferred most of its HUMINT assets to the Defense Intelligence Agency.

In the midst of these reductions, however, it quickly became apparent that the post-Cold War world would hold unforeseen and perhaps unforeseeable danger. Throughout the 1990s, INSCOM was called to support peacekeeping, stability, counter-drug, and humanitarian operations in the Caribbean, Africa, the Middle East, and the Balkans. As the 20th century drew to a close, new menaces arose in the form of terrorism and cyber warfare. The reduction of resources and redefinition of missions meant that INSCOM faced its greatest reorganization since its establishment.

To respond more effectively to the regional crises of varying sizes, INSCOM reorganized its assets. Upon the inactivation of the Army Intelligence Agency, INSCOM regained the Army's intelligence production agencies and merged them together in the National Ground Intelligence Center (NGIC). The center's capabilities were improved when it moved into its new headquarters in Charlottesville, Virginia. INSCOM also became the executive agent for two mission sites with cutting-edge technologies in Bad Aibling, Germany and Menwith Hill, United Kingdom. At Fort Gordon, Georgia, INSCOM set up a Regional Security Operations Center (RSOC) comprising personnel of the newly organized 702d MI Group (later redesignated the 116th MI Group). The 513th MI Brigade, the command's rapid response unit, moved to Fort Gordon in 1994 and colocated with the RSOC, allowing the theater brigade personnel to take part in national missions. Finally, INSCOM established the Land Information Warfare Activity (LIWA), a completely new type of intelligence element. LIWA received the mission of defending the Army's automated communications and data systems from intrusion and of developing Army capabilities for offensive and defensive operations in cyberspace.

Information Dominance Center at INSCOM Headquarters.

The efficiencies gained by these reorganizations were crucial in allowing INSCOM to effectively coordinate the movement of intelligence specialists from its units worldwide and deploy them where needed. Moreover, instead of simply operating at echelons above corps, INSCOM began to provide a seamless connectivity between national level agencies and tactical units in the field. Improvements in automation and dedicated intelligence communications gave INSCOM unprecedented connectivity with its subordinate units when deployed. The forward-deployed intelligence assets reached back and exploited databases and other intelligence located in the U.S., Europe or other secure areas. As INSCOM reduced its physical presence around the globe, it found itself working more closely with the overall intelligence community and with the Army's own tactical intelligence assets.

The Global War on Terrorism (2001-2007)

The attacks of September 11, 2001 demonstrated in no uncertain terms that the U.S. faced a new kind of threat: a complex network of international terrorists, who transcended national borders and military areas of responsibility. This new War on Terror demanded a truly global intelligence effort. Consequently, INSCOM, with its ability to draw on Soldiers and information around the world, necessarily played a major role in this new conflict.

As the U.S. invaded Iraq, the 513th MI Brigade once again found itself at the center of INSCOM's support to the warfighter. The 513th successfully executed split-based operations. When the 513th's main body deployed in Camp Doha, Kuwait, elements of its headquarters and subordinate battalions remained at Fort Gordon. Once deployed, the brigade's assets established a ground-based collection baseline to provide indications and warnings, reinforced CI operations to provide critical force protection, and manned joint intelligence centers to provide fused intelligence for the commanders. In the end, the 513th MI Brigade's deployed strength exceeded 2,200 Soldiers and civilians.

Behind the 513th, INSCOM marshaled all of its resources for the campaign. The other theater intelligence groups tracked terrorist activities in their areas, established new mission priorities to better support the Iraqi missions, and provided individual Soldiers and teams for Afghanistan and Kuwait. Both NGIC and the 116th MI Group adopted "Doha Time" to analyze intelligence and communicate with the theater in a single battle rhythm. Both units sent massive amounts of intelligence through dedicated secure intelligence channels. All this was tied together with a robust TROJAN network that provided more than 60 times the bandwidth available for Desert Storm.

Moreover, Major General Keith B. Alexander, the INSCOM commanding general, accelerated ongoing efforts for restructuring the command into an operational headquarters. He sought to improve synergy and integration among the INSCOM units to better support the forward deployed units. At INSCOM headquarters, the Information Dominance Center (IDC) became one of the primary instruments for this synchronization. The IDC fused signals intelligence focused on terrorist activity with open-source intelligence, measurements and signatures intelligence, and imagery of known terrorists and their associates. The IDC made INSCOM the Army's critical information conduit to leverage the national, theater, and tactical reporting and create actionable intelligence that could be funneled to the commanders and national law enforcement agencies in near real-time.

Although the major combat phase has ended, INSCOM continues to commit its unique worldwide multi-discipline capabilities to prosecute what promises to be a long intelligence war against a global threat.

Conclusion

"As we move into the future," MG Rolya noted in 1979, "we should consider that our perspectives will again change and the "perfect" system we conceive today will be the imperfect system we operate with tomorrow." He went on to advise, "Constant objective reassessment is the key." As we reflect on INSCOM's thirtieth year, we would do well to take note of the first INSCOM commanding general's words, since the INSCOM story continues to unfold. Although rooted in the past, INSCOM continues to refine, retool, and revise the ways it meets the Army's need for intelligence support.

Key Issues
Relevant to Army Intelligence Transformation

The following are portions of the AUSA's Torchbearer National Security Report "Key Issues Relevant to Army Intelligence Transformation" (Arlington, Va.: Association of the United States Army, July 2007), reproduced by permission of the publisher; available online at http://www.ausa.org/webpub/DeptILW.nsf/byid/JRAY-75LT2E/$File/TB-Intel.pdf?OpenElement.

Preface

Since 2001, combat operations in Afghanistan and Iraq have clearly demonstrated the critical need for increased military intelligence (MI) capabilities within the Army's brigade combat teams (BCTs) and maneuver battalions (BNs). Commanders at the tactical level must understand, decide, act, and react in near real time to capitalize on fleeting opportunities, achieve intended effects and mitigate risk. Successful use of information can be accomplished only through aggressive teaming between operations and intelligence, a shared common operating picture of the battlefield, and effective employment of organic and supporting MI assets. The Army has incorporated this hard-won field experience into its ongoing modular conversion, which shifts the warfighting nexus from division- to brigade-level operations and equips Soldiers for the asymmetric fight.

Army modular forces place a high premium on the ability of BCT intelligence (S2) elements to collect, rapidly exploit, and fuse all sources of information into actionable intelligence in response to rapidly changing circumstances and commanders' operational needs. This has driven significant MI growth at the BCT and battalion levels, establishment of reinforcing MI units within new battlefield surveillance brigades (BfSB), major expansion of Army human intelligence (HUMINT) forces, rebalancing of MI skills across active and reserve components, and new intelligence readiness programs linked to Army Force Generation (ARFORGEN) readiness cycles. Intelligence requirements have concurrently driven development and accelerated fielding of advanced, all-source, "flat" network fusion analysis capabilities achieved through Distributed Common Ground System-Army (DCGS-A) workstations and network access down to battalion level. DCGS-A constitutes a major paradigm shift. It empowers analysts by providing rapid access to all sources of information at every classification level, advanced processing and data visualization tools, and the ability to rapidly collaborate with both local and distant counterparts.

Army Intelligence transformation is moving ahead aggressively and is fully integrated with the Army Campaign Plan and the transformational goals of the Under Secretary of Defense for Intelligence and the Director of National Intelligence. **Army Intelligence transformation is focused on four key vectors:**

- Increasing MI capacity and skills balance.
- Revitalizing Army HUMINT.
- Enabling BCT and battalion-level access to "flat," all-source information networks.
- Improving MI wartime readiness by:
  - equipping Soldiers for the asymmetric fight.
  - transforming intelligence training.

Implementing these initiatives allows Army intelligence to support the Army in all threat environments—traditional, irregular, disruptive and catastrophic. Army Intelligence transformation is a vital component of battlefield success, complementing, and fully exploiting the capabilities of emerging technologies, particularly future combat systems (FCS). Fully transformed Army intelligence will not only support ongoing counterterrorism, counterinsurgency (COIN) and stability operations in Iraq, Afghanistan, and the War on Terror; but also guard against potential threats across the full spectrum of current and future operations.

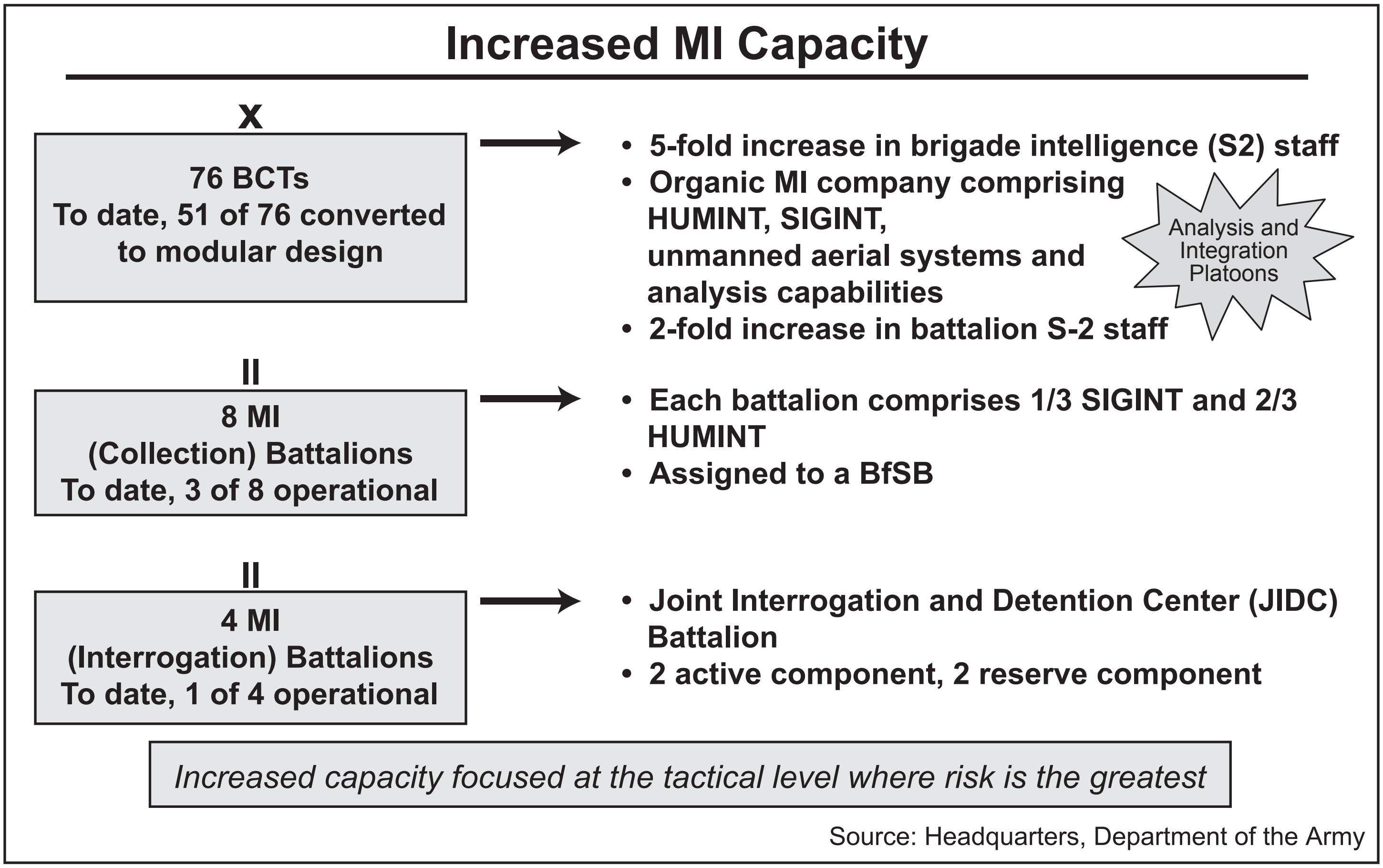
Increasing MI Capacity and Skills Balance

The principal building block of Army ground combat forces today is the modular BCT. Each modular BCT and maneuver battalion leverages close access to local populations to understand complex human and cultural dynamics and achieve intended effects.

MI force structure at the brigade and battalion levels prior to the 11 September 2001 terrorist attacks on the U.S. homeland has proved to be inadequate for the broad range of continuous collection and analytical tasks that current BCT and battalion intelligence elements must perform to ensure mission completion. Modular MI structure addresses these shortfalls—the Army has more than doubled the size of maneuver battalion S2 (intelligence) sections, and additional growth is being considered. BCT S2 sections have more than tripled in size en route to a fivefold increase by 2011 with concurrent expansion of the BCT's organic MI company, which now includes HUMINT, signals intelligence (SIGINT), unmanned aerial system (UAS) and increased analysis capabilities. To date, 51 brigades have transformed to the BCT modular design; the goal is 76 modular BCTs by 2013.

Battlefield experience has shown that even with expanded intelligence capacity at the BCT level and below, additional downward reinforcing MI capability is required for full-spectrum operations in complex environments. To meet this need, the Army is forming eight active component MI collection battalions; three have been formed to date. Each of these battalions is heavily weighted for HUMINT source and interrogation operations and includes advanced SIGINT capabilities and multifunctional HUMINT/SIGINT teams for autonomous support operations. These collection battalions form the core of five new BfSBs—three active and two reserve component; the first BfSB was formed in 2006. **The BfSBs and MI collection battalions are designed for direct, downward-focused reinforcing support to committed divisions, BCTs and battalions, where the risk is greatest**. They can also provide effective collection and reconnaissance support to Joint, Joint task force (JTF) and coalition forces as required. Active Army, Army National Guard, and Army Reserve structure will be based on a common force design.

To better support Joint interrogation operations at the JTF level, the Army is also building four joint interrogation and debriefing center (JIDC) battalions—two active and two reserve component; the



Increased MI Capacity

X

76 BCTs
To date, 51 of 76 converted to modular design

- 5-fold increase in brigade intelligence (S2) staff
- Organic MI company comprising HUMINT, SIGINT, unmanned aerial systems and analysis capabilities
- 2-fold increase in battalion S-2 staff

Analysis and Integration Platoons

II

8 MI
(Collection) Battalions
To date, 3 of 8 operational

- Each battalion comprises 1/3 SIGINT and 2/3 HUMINT
- Assigned to a BfSB

II

4 MI
(Interrogation) Battalions
To date, 1 of 4 operational

- Joint Interrogation and Detention Center (JIDC) Battalion
- 2 active component, 2 reserve component

Increased capacity focused at the tactical level where risk is the greatest

Source: Headquarters, Department of the Army first active JIDC was formed in 2006. Each provides robust, dedicated HUMINT exploitation capability that trains closely with military police detention forces and serves as the core for sister Service, Joint and National augmentation. JIDC battalions complement HUMINT skills resident within Army BCTs and BfSB MI collection battalions and enable effective collaboration and synchronization in support of ongoing operations.

By 2013, the Army will have added more than 7,000 MI Soldiers to its ranks. More than 90 percent of that growth is aligned with enhanced tactical collection, exploitation, and analysis. Army Intelligence transformation is producing a modular, better balanced MI force that can support not only the heavy demands inherent in the war on terror and regional contingency operations but also the full spectrum of operations.

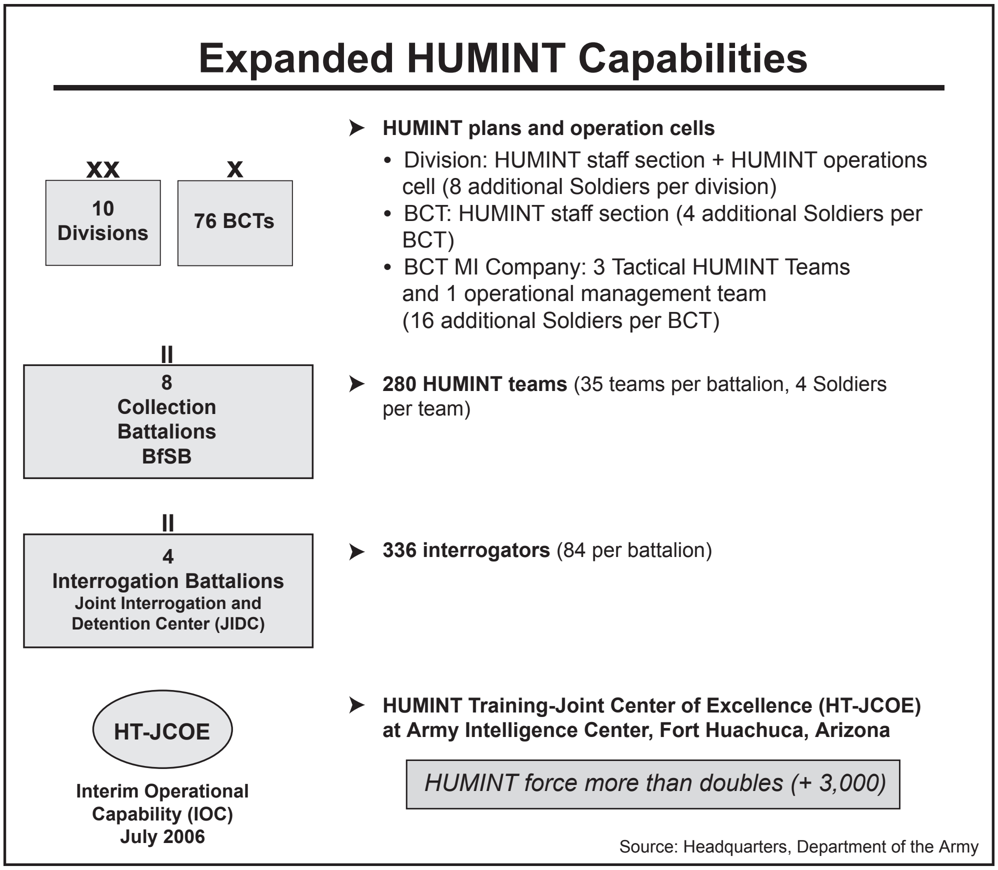
Today's Soldiers are smart, tough, dedicated, and technologically savvy. Each MI Soldier must also be an expert in his core specialty and competent in key related intelligence skills. (For example, analysis is a skill inherent in every MI discipline.) Army MI is accordingly growing its Soldiers in "MI Pentathlete" style to perform an expanded range of combat-essential intelligence tasks through instruction at basic, mid-level and advanced training courses.

Revitalizing Army HUMINT

Expansion of Army HUMINT capacity is a key component of military intelligence transformation. Army MI strength is increasing by at least 7,000 Soldiers, more than half of them going to HUMINT disciplines. **Army HUMINT strength will more than double in the coming years—from approximately 2,500 in Fiscal Year (FY) 2005 to more than 6,000 by FY 2011**.

Combat lessons learned reflect the overriding importance of robust HUMINT capability down to the BCT level. While essential across full-spectrum operations, HUMINT is especially critical in irregular warfare and stability operations, where understanding the "human dimension" is essential to achieving precise targeting, intended effects and operational success. Beyond force structure, Army HUMINT transformation is having a profound effect on the training and employment of the HUMINT force at all levels and is driving enabling technologies to improve HUMINT force performance.

HUMINT capabilities at the BCT level are expanding significantly to provide forward-based military source operations (MSO) and interrogation skills where the opportunities and operational risk are greatest. These HUMINT Soldiers collect information to satisfy intelligence requirements, to include threat identification, associations, locations and future plans. HUMINT Soldiers operate in the close-access human domain to collect this information through interaction with the indigenous population, to include local warlords and local tribal, political and military leaders. Analysts integrate this information with other sources of information to increase understanding and generate actionable intelligence. The commander manages HUMINT op-


Expanded HUMINT Capabilities
XX
10 Divisions
X
76 BCTs
II
8 Collection Battalions BfSB
II
4 Interrogation Battalions Joint Interrogation and Detention Center (JIDC)
HT-JCOE
Interim Operational Capability (IOC) July 2006

➤ **HUMINT plans and operation cells**
- Division: HUMINT staff section + HUMINT operations cell (8 additional Soldiers per division)
- BCT: HUMINT staff section (4 additional Soldiers per BCT)
- BCT MI Company: 3 Tactical HUMINT Teams and 1 operational management team (16 additional Soldiers per BCT)

➤ **280 HUMINT teams** (35 teams per battalion, 4 Soldiers per team)

➤ **336 interrogators** (84 per battalion)

➤ **HUMINT Training-Joint Center of Excellence (HT-JCOE) at Army Intelligence Center, Fort Huachuca, Arizona**

HUMINT force more than doubles (+ 3,000)

Source: Headquarters, Department of the Army erations through his HUMINT staff officer. **Each modular BCT contains three organic HUMINT teams and imbedded HUMINT plans and operations elements. Each reinforcing BfSB MI collection battalion brings 35 additional HUMINT teams of four Soldiers each.**

HUMINT at theater, operational and strategic levels is also being expanded, to include the four JIDC battalions, each with 84 interrogators and required command and staff support. The Army is also expanding advanced military source operations and debriefing support through expansion of Army Operations Activity (AOA) and Army Reserve Operations Activity (AROA) elements, which provide responsive support to Army Service Component Commands (ASCC). (For one example of an ASCC, see AUSA National Security Watch 06-5, "U.S. Army South and the Transition to 6th Army: Rising to Face New Challenges in Central and South America and the Caribbean," 1 December 2006, online at http://www.ausa.org/pdfdocs/NSW06_5.pdf.) **Army Intelligence remains the largest force provider for worldwide Department of Defense (DOD)-level Defense HUMINT operations and is working closely with the Defense Intelligence Agency (DIA) to establish and grow a full-spectrum Defense HUMINT enterprise encompassing all levels of HUMINT operational support.**

With respect to doctrine and training, in September 2006, the Army published **Field Manual (FM) 2-22.3, Human Intelligence Collector Operations**. It provides updated doctrine for full-spectrum HUMINT operations, to include military source operations, HUMINT analysis, debriefing and detailed guidance for the conduct of detainee interrogation operations. FM 2-22.3 is consistent with applicable DOD HUMINT policies and the Detainee Treatment Act of 2005. Although published as an Army Field Manual, it governs the conduct of interrogation operations for all military and civilian interrogators across DOD.

HUMINT training at the U.S. Army Intelligence Center (USAIC) at Fort Huachuca, Arizona, has been significantly expanded to incorporate wartime lessons learned and professionalize the HUMINT force. Toward that end, the Army G-2 (Deputy Chief of Staff for Intelligence) and USAIC partnered closely with DIA to establish a HUMINT Training-Joint Center of Excellence (HT-JCOE) at Fort Huachuca in April 2007, encompassing five advanced HUMINT training courses. The HT-JCOE will enable establishment of joint HUMINT training standards and expansion of joint HUMINT training across the Defense HUMINT Enterprise.

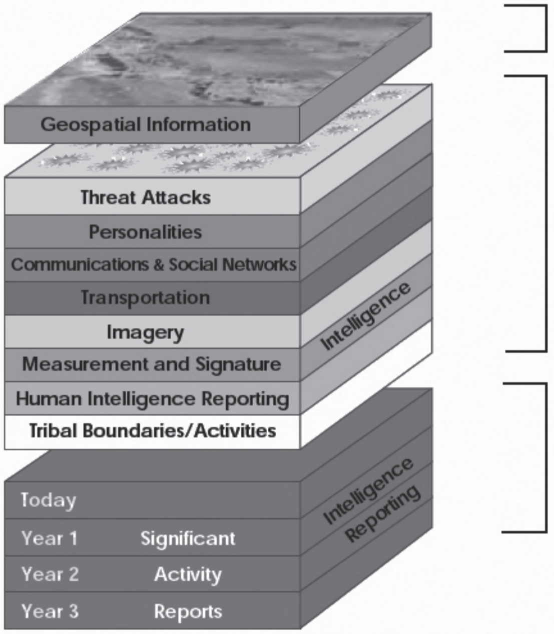
"Flat" Network Access: DCGS-A

Increasing Army MI capacity is essential but insufficient unless MI Soldiers at all levels are concurrently enabled with access to all sources of information at all classification levels as well as advanced software tools needed to rapidly search, visualize and analyze large quantities of data. Cold War-era information hierarchies and sequential filtering are no longer valid. To operate effectively in complex, dynamic environments, battalion, BCT and higher intelligence elements must have access to dozens of intelligence and non-intelligence databases to enable analysts to understand norms; detect change; discern linkages; appreciate significance; cue collection; and identify, track and target hostile forces within tactically useful timelines. The Army is delivering that capability now through accelerated development and fielding of DCGS-A workstations and network access down to battalion level in Iraq and Afghanistan en route to full force conversion and integration with future combat systems (FCS).

DCGS-A "flat" network operations have proven to be highly successful battlefield enablers. DCGS-A capabilities are in use today by every Army maneuver battalion and BCT (including deployed Marine regimental combat teams) in Iraq and Afghanistan. The DCGS-A network brings access to more than 200 databases and rapid collaboration through shared access to data regardless of type or classification. It enables analysts to rapidly mine, fuse and visualize data on top of geospatial intelligence data layers for better understanding. DCGS-A also allows forward deployed analysts to effectively reach

> *DCGS-A tools and "flat" network data access . . . have allowed us to fight the enemy versus fighting the information—[in] seconds and minutes instead of hours and days.*
>
> SFC Nicholas Psaki, NCO in
> charge of analysis within the 2nd
> BCT, 1st Infantry Division in Baghdad

“Flat” Network Capabilities Through Distributed Common Ground System-Army



- ► Common geospatial data layer
- ► All intelligence sources
- ► All classifications
- ► All tactical reporting
- ► Corporate “memory”

Source: Headquarters, Department of the Army

back to theater joint intelligence operations centers (JIOCs), service intelligence centers and national agencies. On today’s complex battlefields, the difference can be measured in lives and operational success.

Combat-bound MI Soldiers receive DCGS-A training—now integrated into intelligence training at USAIC—as part of pre-deployment preparation. DCGS-A capability is becoming increasingly available for home station use and training as DCGS-A capability proliferates across all Army units. Home station DCGS-A access enables MI Soldiers to stay “in contact with the enemy” when they return from combat and empowers them to perform tactical overwatch in direct support of units they will replace upon deployment. Tactical overwatch becomes a force multiplier for operationally deployed forces by enabling them to reach back effectively to “virtual” partners through use of the “flat” network. (See AUSA Torchbearer National Security Report *Key Issues Relevant to Actionable Intelligence*, June 2005, http://www.ausa.org/pdfdocs/TB_KeyIssues.pdf, for more information about tactical overwatch.)

“Last Tactical Mile”

Army Intelligence is also leading in efforts to extend DCGS-A “flat” network capabilities down to company, platoon, vehicle and individual Soldier levels—the “last tactical mile”—through rapid development and wartime assessment of advanced handheld and vehicle-mounted prototype devices. One of these programs is the TACTICOMP™ digital reporting and mapping system, which has been employed in combat within Iraq and favorably evaluated by U.S. forces. TACTICOMP™ uses “mesh” network technology to provide real-time situational awareness displays, messaging and video capabilities well suited to operations in complex environments. Wartime experience with this enabling technology will help ensure funding for this key informational need. DCGS-A remains a top intelligence priority at the forefront of the Army’s modernization effort that links directly into advanced situational awareness, analysis and targeting capabilities inherent within the Army’s FCSs. With DCGS-A, the future is now.

> “Flat” networks connect Soldiers to the full power of modern data networks and software tools to “mine” and manipulate large volumes of data from all sources of information and all classification levels along tactically useful timelines, enabling the complete “memory” of all that is knowable about persons, places, things and relevant events.

Improving Wartime MI Readiness

Equipping Soldiers for the Asymmetric Fight.

Improving Army Intelligence Readiness requires equipping Soldiers for the asymmetric fight through the expansion of persistent intelligence, surveillance and reconnaissance (ISR) capabilities plus improved training across the MI force. The Army is expanding persistent surveillance through both manned and unmanned systems, to include UAS, fixed-wing sensor platforms and ground systems with Imagery Intelligence (IMINT), SIGINT, Measurement and Signature Intelligence (MASINT), and biometrics capabilities. The Army is transforming intelligence training through several programs, to include Project Foundry, Cultural Awareness, Language Training, Red Teaming and "Every Soldier is a Sensor." Together these programs significantly advance MI wartime readiness.

The Army's "**Shadow" Tactical Unmanned Aerial System (TUAS)** program provides dedicated, responsive surveillance and targeting support to the BCT and battalion forces out to a range of 125 kilometers. Shadow gives commanders an assured capability to "look over the next hill" to detect enemy presence, confirm or deny ambiguous intelligence reporting, and support targeting. Shadow systems are deployed with all Army BCTs in Iraq and Afghanistan; service-wide fielding will be completed in FY 2011.

The "Warrior" Extended Range/Multi-Purpose (ER/MP) UAS fielding commenced in 2007 to provide long dwell, day/night, multi-sensor reconnaissance, surveillance and target acquisition support to maneuver commanders out to 300 kilometers. ER/MP fielding at the combat aviation brigade level complements TUAS capabilities, enables effective information sharing and allows target handoff across battalion, BCT, and divisional boundaries via One System Remote Viewing Terminals (OSRVTs) and integration with DCGS-A. Assured ER/MP presence in support of BCT operations, combined with long-loiter (greater than 30 hours) "persistent stare" capabilities, enables rapid fusion analysis and targeting synergies not previously available to conventional ground force commanders.

The Army's fleet of **Guardrail Common Sensor (GRCS)** and **Airborne Reconnaissance Low (ARL)** collection platforms remain today's aerial collection backbone, providing timely, accurate SIGINT and sensor surveillance support to deployed forces worldwide. Major GRCS and ARL system upgrades will extend the operational life of both systems, ensuring continued target access until the fielding of Aerial Common Sensor systems.

Aerial Common Sensor (ACS) is the Army's next generation manned, multidiscipline, multi-sensor airborne ISR collection system. ACS will incorporate incremental sensor upgrades from modernized GRCS and ARL systems; be capable of rapid worldwide deployment, and provide onboard fusion analysis in direct support of ground tactical commanders. ACS will be capable of fusing data collected by ER/MP and other ISR platforms in near real time and providing cueing necessary for effective manned-unmanned (MUM) teaming. ACS will

be capable of receiving data from non-Army ISR platforms and interfacing with the DCGS-A Joint integrated network for broadly distributed tactical, theater and National intelligence use.

With respect to **ground SIGINT,** Army MI partners closely with the National Security Agency (NSA) to field advanced SIGINT collection, processing, analysis and electronic attack capabilities. The **Prophet family of SIGINT systems** gives tactical commanders an effective means to detect and track enemy activity across the communications spectrum. With an architecture that supports future technical insertions, Prophet variants provide the baseline for tactical SIGINT operations. The newest system, Prophet Triton, is now in the hands of U.S. Soldiers in Iraq and has received high marks in combat.

The Army continues to develop and field advanced **MASINT** sensors and systems in support of persistent surveillance needs. Three ground MASINT systems are currently deployed in support of operations in Iraq and Afghanistan. Army MASINT enhances Soldier situational awareness and cues other intelligence systems to enemy presence and activity for positive identification and action. MASINT is a key enabler that provides relevant intelligence along tactically useful timelines today and holds great promise to meet future intelligence needs.

Biometrics is a MASINT application that is increasingly important in the hunt for adaptive, irregular enemies. Army MI actively supports Army Biometrics Task Force and DOD efforts to expand the tactical usefulness of biometric data collection and exploitation. Ongoing fielding of Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE) capabilities respond to warfighter requirements; both systems have proven effective for screening and positive identification of enemy personnel. More than 2,500 BAT collection systems are deployed in Iraq and Afghanistan; more than 5,000 HIIDE devices will be fielded during FY 2007.

Revitalizing Intelligence Training

***Project Foundry*. In 2006, the U.S. Army Intelligence and Security Command (INSCOM) initiated Project Foundry** to establish a single, "one stop" coordination hub for advanced intelligence skills training and certification across all levels of the modular force. It was specifically designed to ensure optimal support for wartime deploying forces synchronized with the Army Force Generation (ARFORGEN) model. (For information about ARFORGEN, see AUSA's Torchbearer National Security Report *2006 and Beyond: What the U.S. Army Is Doing,* March 2006, online at http://www.ausa.org/PDFdocs/TBSecRpt/TBear_March_06_optimizedpdf. Foundry also provides opportunities for advanced MI skills employment against "real" intelligence targets worldwide by enabling MI personnel to "maintain contact" with the enemy in support of ongoing operations and in preparation for wartime redeployment. With MI brigades supporting ASCCs in every theater and MI elements within each combat support agency, INSCOM is uniquely suited for

Project Foundry

U.S. Army Intelligence and Security Command (INSCOM) G-3* = "1 Stop Shop" for "Road to War" Intelligence Preparation

- Live environment operations (tactical overwatch)
- Advanced skills training and certification
- In Fiscal Year (FY) 2006, 2,467 Soldiers trained/28,015 man days of training provided
- Funding provided . . . unit funds not required

Focused on Army forces preparing for deployment

- FY 2006 Trained: 10th Mountain Division, 82d Airborne Division, 25th Infantry Division, 3d Infantry Division, 1st Cavalry Division, I Corps, III Corps, XVIII Airborne Corps
- FY 2007 Training: XVIII Airborne Corps, 3d Infantry Division, 1st Armored Division and 4th Infantry Division

Building Foundry: Home-station sites

FY 2007	FY 2008	FY 2009	FY 2010
◊ Fort Bragg, NC ◊ Fort Stewart, GA ◊ Fort Lewis, WA	◊ Fort Drum, NY ◊ Fort Campbell, KY ◊ Fort Hood, TX	◊ Fort Bliss, TX ◊ Fort Riley, KS ◊ Fort Carson, CO	◊ Outside the continental United States

*Operations

Source: Headquarters, Department of the Army

this mission and has aggressively expanded the program. (For one example of an Army Service Component Command, see AUSA National Security Watch 06-5, "U.S. Army South and the Transition to 6th Army: Rising to Face New Challenges in Central and South America and the Caribbean," 1 December 2006, online at http://www.ausa.org/pdfdocs/NSW06_5.pdf.)

Foundry has proven highly successful in helping BCTs and divisions prepare for wartime deployment and in sustaining hard won analysis and collection skills following return to home station. Foundry also enables units preparing for deployment to leverage DCGS-A "flat" network capabilities to conduct "tactical overwatch" support for the units they will replace in combat through the provision of workstations, communications and mentors.

Foundry has proven to be a very successful MI readiness program. INSCOM is expanding Foundry training to include Joint and National agency opportunities and establishing Foundry training platforms at major troop centers to ensure optimal warfighter support; the first Foundry Center was formed in 2006 at Fort Bragg, North Carolina.

***Cultural Awareness and Language Training*. Cultural Awareness and Language Training is a clear wartime readiness imperative at all levels.** Army MI efforts in this regard reflect battlefield lessons learned and DOD guidance. Success in stability and COIN operations requires detailed understanding of complex cultural and historical "human dimension" dynamics that USAIC is now teaching to units Army wide as an integral part of pre-deployment preparation.

USAIC runs the U.S. Army Training and Doctrine Command (TRADOC) Culture Center at Fort Huachuca, Arizona, and deploys mobile training teams (MTTs) to teach a broad range of cultural awareness skills tailored to mission need. In FY 2006, USAIC trained more than 11,000 Soldiers, Sailors, Airmen and Marines and developed more than 200 hours of regionally specific training in support of War on Terror operations. The Culture Center worked aggressively with the Army's combat training centers to ensure integration of cultural realism in "Civilians on the Battlefield" programs, which includes extensive use of foreign-born linguists. USAIC also works closely with deploying units, provides a wide range of web-based distance learning products, and manages training and integration of foreign-born Interpreter/Translator Soldiers in the new military occupational specialty (MOS) called "09L." More than 130 MOS 09L Soldiers now serve with Army units in Iraq and Afghanistan. On their return from wartime deployment, 09L Soldiers support home station cultural awareness predeployment training.

Army Foreign Language training, a critical component of cultural awareness training, has also been significantly expanded. Defense Language Institute Foreign Language Center (DLIFLC) language training programs and "outreach" initiatives have been significantly expanded across War on Terror related languages. DLIFLC has also leveraged commercial language training technologies to sustain and enhance perishable language skills at all levels. DLIFLC provides mobile language training teams, language "survival kits" for deploying forces, and web-based Global Language On-line Support System instruction in 12 target languages. Eleven DLIFLC language training detachments support Arabic language training for all services at unit home stations. To complement these training initiatives, during 2007 the Army increased the maximum monthly Foreign Language Proficiency Pay (FLPP) from $300 to $1,000 per month for active component Soldiers and is working toward similar compensation for reserve component Soldiers.

Red Teaming**. Critical thinking skills are imperative for success in wartime against adaptive enemies operating in complex threat environments.** Recent wartime experience has led the Army to establish formal "Red Team" training to impart critical thinking techniques at corps, division and BCT levels. In 2006 the Army established the University of Foreign Military and Cultural Studies (UFMCS) at Fort Leavenworth, Kansas, to train Red Teams consisting of planners from intelligence and non-intelligence disciplines in nontraditional analytic skills aimed at identifying dependencies, unintended effects and vulnerabilities, and developing mitigating strategies. In essence, "Red Team University" trains officers to dissect "friendly" plans during the planning process, so that when it comes time to execute the mission, key vulnerabilities and weaknesses will have been identified and reduced. (See John Milburn, "Red Team U. Creates Critical Thinkers," *Associated Press Online*, 18 May 2007, Lexis/Nexis.)

Red Teams are involved in all phases of the unit's planning process to provide alternative, independent perspectives to enhance and improve the planning effort. This unique perspective is made possible by incorporating subject matter expertise from warfighting staff sections as well as resources from academia and industry. The Red Team performs in a structured "devil's advocate" role to challenge assumptions made in the planning process and evaluate courses of action from the enemy's viewpoint. The Red Team enables the unit commander and battle staff to understand dependencies and unintended consequences related to proposed actions. Red Teaming is a dynamic, iterative process that enhances planning and mitigates risk.

UFMCS currently offers education and training via an 18-week Red Team Leaders Course (RTLC) and a nine-week variant tailored to meet immediate warfighter needs. UFMCS launched a six-week Red Team Members Course (RTMC) in July 2007. Through rigorous curriculum, UFMCS has certified more than 50 graduates in Red Team techniques since FY 2006. Many of those graduates are now deployed in support of operations in Iraq and Afghanistan. Red Team structure at the corps and division levels is pending final approval; evaluation of structure need for Red Teams at the BCT level is ongoing.

Every Soldier is a Sensor (ES2)**. Success on dynamic, and especially irregular, battlefields requires close Soldier interaction with the local populace and a clear understanding of the operational environment.** Unlike mechanical sensors, Soldiers process observations with savvy and speed that cannot be matched by technology to determine change, relevance and significance. Soldiers are trained to refine their observation skills and to report into the integrated "flat network" for enhanced situational understanding across the force. This observation and reporting entails a significant change in how Soldiers are trained from the earliest stages to inculcate "tactical curiosity" in every Soldier at every level.

Soldiers trained in ES2 concepts are taught to routinely observe and report patterns and changes in the operating environment through interaction with the local populace in the course of accomplishing their mission. They answer fundamental questions that shape their environment, such as who the leaders are; where the utilities come from and who controls them; the locations of the market places and their opening and closing times; the eating and sleeping patterns; what the streets look like (how crowded or empty they are at different times), and the traffic patterns. Once Soldiers understand what "normal" looks like, they are able to notice and report even subtle changes in the environment that may be critical to understanding and anticipating future enemy actions.

Intelligence fusion analysis is significantly enhanced with this richer local context provided through Soldier observations—sensor and HUMINT reporting becomes more understandable in the same vein. The net result is better understanding of norms, environmental change, linkages, and significance at all levels—a powerful addition the Army must fully leverage.

ES2 tasks are now incorporated in Army doctrine, all Initial Entry Training and collective training at Army combat training centers. ES2 integration into noncommissioned officer, warrant officer and officer training courses is ongoing.

The "Every Soldier is a Sensor Simulation" (ES3), a self paced ES2 simulation based on battlefield scenarios and lessons learned, is now available worldwide through Army Knowledge Online web access.

Torchbearer Message

Operations and intelligence are inseparable on today's battlefields in both conventional and irregular environments. The availability of actionable intelligence determines how the Army employs both lethal and nonlethal capabilities and greatly influences the effects achieved. Army Intelligence transformation is focused on increasing intelligence capacity and the ability to generate actionable intelligence at all levels across the force. Army modularity especially places demands on the ability of BCT forces to operate in rapidly changing, complex environments. That has created a significant increase in the size and capability of intelligence elements at battalion and BCT levels, expansion of the HUMINT force, and development and fielding of "flat" network DCGS-A capabilities down to battalion level to ensure distributed, all-source data access. These initiatives have resulted in major changes in the way Army MI trains and sustains combat readiness. Changing one piece is not enough—the Army needs to change them all for wartime operational success.

The following essential intelligence transformation vectors are critical enablers for the Army's modular force—essential for responsive, agile MI support at all tactical levels across the full spectrum of operations:

- **Increasing MI capacity and skills balance through major increases in tactical unit intelligence staff sections, establishment of organic intelligence companies in modular BCTs, establishment of new MI collection battalions in Army BfSBs and formation of new JIDC Battalions.**
- **Revitalizing Army HUMINT by more than doubling the HUMINT force with a focus on increasing organic HUMINT capability at the BCT level and expanding HUMINT training and integration with the Defense HUMINT enterprise.**
- **Enabling "flat" network access down to the battalion level through accelerated development and fielding of DCGS-A.**
- **Improving intelligence wartime readiness by:**
  - **Equipping Soldiers for the asymmetric fight through manned and unmanned aerial systems, ground sensors, biometrics and other persistent intelligence capabilities.**
  - **Transforming intelligence training through Project Foundry, Cultural Awareness, Language Training, Red Teaming and "ES2."**

Intelligence transformation reflected in these vectors modernizes Army intelligence, making it immediately responsive to commanders and Soldiers regardless of threat posture.

Soldiers expect and deserve the best possible intelligence tools and analysis the nation can provide as they execute challenging missions in unforgiving, complex environments worldwide. Army Intelligence, as part of the Joint intelligence team, is taking aggressive action to meet these challenges in close collaboration with Joint, DOD, and National intelligence partners. **With continued full, timely and predictable funding of Army requirements, the Army remains on course to expand its ability to provide actionable intelligence to Soldiers, combatant commanders, and Joint warfighters, and across the U.S. Intelligence Community.**

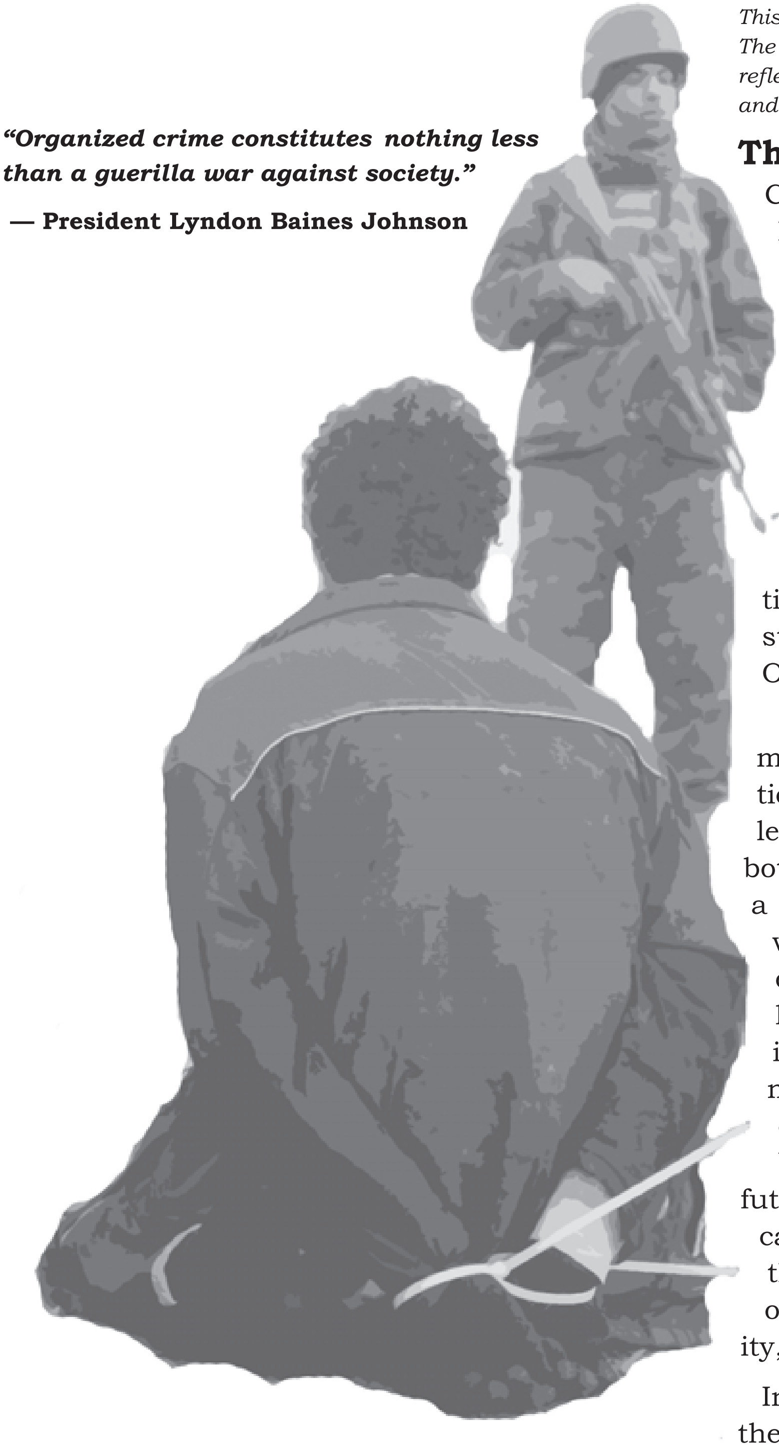
Focused Operations Against Organized Crime in a Mature Peace Operations Environment

By Major Oliver Mintz and Second Lieutenant Tory House

This article first appeared in January February 2007 issue of Infantry. The views expressed in this article are those of the author and do not reflect the official policy or position of the Departments of the Army and Defense, or the U.S. Government.

"Organized crime constitutes nothing less than a guerilla war against society."

— President Lyndon Baines Johnson



The Insidiousness of Organized Crime

Conditions in a peace operations environment allow for the robust application of conventional forces toward information collection. This collection could be focused against organized crime (OC) in a manner that allows the continual exploitation and reduction of OC as an obstacle to societal progress. While the daily activities against OC are typically police actions, the long term effect of OC poses a substantial threat to a safe and secure environment, and the growth of a stable government and economy. It is imperative that leaders in peacekeeping missions understand the nature, environment, and targeting of OC.

In peacekeeping operations, intelligence is the most vital of all commodities. It drives all operations, and all operations should be conducted, at least in part, to gain more of it. As conditions in both Iraq and Afghanistan evolve and move toward a future of peace operations, the Army would do well to look forward and reexamine the conduct of such missions. Currently the best example of how Iraq and Afghanistan may look in a few years is Kosovo. Admittedly, the cultural differences are many, but the multinational environment focused on maintaining the peace and assisting civil rebirth is likely to be very similar to an Iraq of the future. It is important for leaders, at both the tactical and operational levels, to understand some of the particular dynamics of that situation, which of these pose the greatest threats to civil instability, and how to combat them.

In peace operations the situation is often ripe for the success of OC. A number of particular conditions exist, beyond the obvious lack of police support and other corrupt individuals who would support OC. A fundamental understanding of these environmental conditions will prove helpful to commanders as they plan to enforce the peace.

When a government does not or cannot provide for its citizens, people will work outside the system. This is a fundamental breach of social contract theory.

OC is not a problem that affects *only* the economics, politics, legal systems, or reconstruction efforts of a region; it affects all of them. In the former Soviet states OC has become an integral part of the economy and is a tremendous hindrance to their emergence into the modern political and economic world. Pervasive OC has a number of effects; fundamentally it prevents the growth of legitimate economy where legitimate businesses compete for business and the laws of capitalism and economics govern the market. This symbiotic relationship is the building block for many other functions.

Legitimate businesses establish a link of accountability with the government, according to Fareed Zakaria in his book, *The Future of Freedom*. That linkage functions as such—businesses grow and generate revenues, and all of that income is taxed by the government. By levying taxes the government then becomes accountable to the business class that can rightfully demand improved transportation networks, security, beneficial trade policy, etc. enabling economic growth.

OC networks do not operate within this framework; its proceeds are largely cash, and are not taxed. They do not compete fairly, but rather contribute to the growth of markets that operate outside of honest capitalism. They contribute to instability and insecurity which discourages foreign investment (a staple of ignition for emerging nations). In order to protect its interests OC can very easily corrupt the law enforcement and legal systems due to the meager wages often paid to public servants, and particularly so in emerging nations.

Without question an ineffective or corrupt judiciary prevents the function of legitimate rule of law. In addition to not meting out just punishment it brings discredit upon the local police. The average citizen, who sees a wrongdoer arrested and then back on the street days or hours later, makes the connection that the government did not do its job.

Oftentimes, the populace lacks a fundamental understanding of the particulars that govern the functioning of the system, and the laws by which the police must abide. A judicial system that cannot or will not prosecute offenders not only keeps dangerous individuals on the street, but lessens the power of the police in the public's eyes, according to Cesar Beccaria's 1764 work *On Crimes and Punishments*. This perception has a cumulative and negative effect on the perceived ability of the policing arm, and begins to make their job that much more difficult.

Oftentimes a judiciary fails due to internal corruption, or on a more practical level, because of the sheer caseload. Lack of experience in managing dockets, controlling evidence legitimacy, and enforcing distinctions between hearsay and testimony all contribute to the practical failings of emerging judicial systems. Societies emerging from upheaval and under control of international organizations or multinational coalitions are often at the behest of many masters, and are subject to complex processes and regulations. Additionally, political infighting, which often goes unchecked as outsiders try to either allow the process owners to solve their own problems or smooth political feathers, slow the appointment of judges or resolution of cases. The actions of the judiciary are often guided by other forces related to OC. It is possible for OC groups to intimidate judges, or simply buy a favorable decision. Whatever the reason, the real result is a negative perception of the local police as the judicial system often struggles to keep up with the caseload and overcome the corrupting influences of OC.

When a government does not or cannot provide for its citizens, people will work outside the system. This is a fundamental breach of social contract theory. Social contract theory posits that individuals in a society subjugate their individual rights in return for security and a better society. This idea is an underlying premise in the governmental system of most developed nations. States in transition often function in a breach of this contract. For states that have been struggling to emerge from the Third World even the average person is forced to commit minor crimes simply to get by; buying black or grey market goods, paying a police officer or official to process paperwork, or paying an inspector to overlook a minor deficiency are but a few examples. Thus, people become complicit in the corruption, and corrupt themselves. This activity becomes so ingrained in the daily fabric of life that "organized criminals" are often thought of as simply efficient and organized businessmen. Moreover, the populace becomes dependent on the black or grey market goods and services, and actions taken against OC negatively impact the populace's standard of living. While most of these same people would otherwise favor the rule of law, their need to maintain what is often a minimal standard of living trumps that preference. This type of corruption can be characterized as "functional corruption" wherein people pay for an illegal product or service. In emerging nations this is often viewed as capitalism. This is in contrast to "dysfunctional corruption" where officials are bribed or coerced into looking the other way while OC violates a fellow citizen's personal or property rights. The key difference between functional and dysfunctional corruption is the introduction of a victim.

One of the hallmarks of a legitimate government and system of justice is the monopoly of the use of force to enforce law or government policy, according to the article, *"Mature Peacekeeping Operations as Facilitators of Organized Crime* " by Irv Marucelj. A notable example of a government failing to maintain this power is in the case of the Colombian government and the narcotics kingpin Pablo Escobar. If a government does not have the mandate and ability to utilize overwhelming force then OC can violently exert itself to fill this vacuum. This becomes particularly dangerous when the government that is usurped by OC is going through a period of transition of limited sovereignty (*"Transnational Crime, Corruption, and Security"* by William L. Smith.)

In emerging societies OC often maintains the ability to use force to settle disputes with the local populace, other criminals, businessmen, and law enforcement and government authorities. This ability to use force, without fear of judicial retribution, can range from direct action attacks to the threat of force against business rivals and judicial figures.

This situation is brought about by the weaknesses of governmental authorities as described above, and is exacerbated by the ubiquity of weapons. The ownership and use of weapons is, in all likelihood, not a new phenomenon. Likely, previous governments or regimes were unable to protect the populace who were thus forced to arm themselves for various reasons. This goes hand in hand with the pervasive public attitude that selective lawbreaking is an accepted part of life. This fact, coupled with the reality that a fallen totalitarian regime can lead to a loss of control of weapons accountability, lead to a situation where weapon possession is a part of daily life.

In many respects OC operates just as a legitimate business, and the public often sees it as such. This creates a number of additional hurdles. In terms of economic and business theory OC moves into markets where there is both a customer and a need. OC fulfills that need; after all, nature abhors a vacuum. OC experiences a growth cycle like a normal business, and becomes integrated into the economy. As it grows it seeks to set favorable conditions for its success by currying the favor of politicians and decision makers. Unlike legitimate business, OC violates the "felicitation principle" wherein the aim of laws and governance is to give the greatest happiness to the largest number of people in a society. Instead, OC is self-serving, closed to outsiders, and focuses on the baser desires of its markets. Just as legitimate businesses carry goods in inventory, so do OC groups. Typically this inventory expands beyond legitimate products and into narcotics, prostitution, protection rackets, counterfeiting, and theft of intellectual property.

One of the largest obstacles to overcome in terms of a successful information operations (IO) campaign, against both the criminals and the populace, is the notion that criminality is acceptable as a way of life, and is in fact a necessity to a life of any worthwhile quality. In the example of Kosovo, and the former Yugoslavia in general, it is the widely held belief that the government should provide the necessities such as electricity and water. When the government fails to provide these things the average person can more easily rationalize turning to the black or grey market or other nefarious methods; "The government isn't helping me so I have to help myself." This mindset becomes so pervasive that criminal networks have literally "incorporated" it.

Just like any entrepreneur, OC networks are drawn to good markets. However, a good market to a criminal entrepreneur includes both a good market (a place where a seller meets the needs of a buyer) and certain favorable market conditions such as a weak judiciary and a populace willing to conduct business. Such market conditions often exist where there is an ambiguity of law enforcement responsibilities, or during a period of transition to increased sovereignty. Once in these markets the growth of OC networks will go through a growth cycle much the same as a legitimate business.

Such businesses may arise from local criminal entrepreneurs who see an opportunity in their local area, from established criminal networks within the region, or worldwide (Chinese gangs in New York). This influx of criminal outsiders is not unlike the globalization of legitimate businesses. This criminal globalization takes place using the same tools and systems, namely ease of worldwide travel and the advantages of information technology that connect the globe. Once established in an area, criminals will set up supply chain and distribution systems, carve out, and expand their markets. They will continue to expand and solidify their market share against criminal competitors, law enforcement, and military forces conducting peacemaking or peacekeeping operations.

They will do this through both legal and illegal methods. They will compete traditionally in terms of price and meeting legitimate and illegitimate needs of buyers. They will also hedge their investment using strong arm techniques from general thuggery, including menacing, coercion, assaults, outright attacks, and intimidation against all parts of a competitor's supply and distribution chain. An atmosphere of fear is established so that these tactics, along with solidifying their sway with leaders, ensures that they will retain the freedom to grow and run their business.

The lobby business in Washington is a multibillion-dollar industry. Any major corporation hoping to successfully compete will seek to influence the conditions that affect its business environment. Drug companies spend huge sums attempting to gain favorable rulings from lawmakers, and "big boxes" spend many a day in city board meetings trying to alter local zoning laws. In fact, third world criminal networks are rank amateurs when it comes to gaining political or legal ruling favorable to business. However, the big difference is revealed when it comes to methods. Admittedly, in developed nations there are those who engage in extreme and illegal acts to gain favorable political actions. However, they are on the extreme fringe of the normal pattern of business. In an environment characterized by ongoing peace operations, criminals maintain the threat or actual application of force as a tool to achieve their political and legal ends. Although their means may differ from the accepted standards in the U.S. or Europe, the goal of an OC group is the same as a legitimate businessman; the acquisition of wealth.

Despite looking and acting like a legitimate business OC is, in fact, a cancer that prevents the growth

A car belonging to individuals associated with criminal activity is searched by Kosovo Police Officers under the watch of Kosovo Force (KFOR) Soldiers in Letnica, Kosovo.

of that very thing they pretend to be. Understanding this fact and the impact of OC is the first step toward building a plan to combat it.

Conditions for Kinetic Intelligence Collection

In contrast to the operating environment in Iraq and Afghanistan, troops in Kosovo and other peace operations enjoy relative freedom of maneuver (currently referred to as a permissive environment.) There is little risk or cost associated with a mission anywhere in the region with a low likelihood of direct attack. This freedom of action creates the conditions that are ripe for collection against OC.

The chance of any criminal launching any type of attack against peacekeeping forces is extremely unlikely for a number of reasons. OC thrives on blending into the population and being invisible to military forces, who are often concerned with other threats as well. Criminals maintain this anonymity by fully cooperating, almost to the level of patronizing, with the military forces. To launch an attack would be bring a storm of attention that would negatively impact its business in the worst possible way. Moreover, OC factions lack the manpower and firepower to overcome military forces in a protracted fight. Worse for them, to do so could likely taint their reputation within the local populace, on whom they rely to sustain their business. This is particularly true in Kosovo where KFOR is held in high regard by many of the Albanian majority. It is often in the OC group's best interest to simply wait for the peacekeeping forces to forget about the group and move on to other missions.

Forces available to the commander in modern peace operations are often limited. Peace operations, by their nature, are manpower intensive. Coupled with increasing political pressure to get troops home as soon as the combat phase of operations has ended, commanders in peace operations must fight with an economy of force. Despite a high troop to task ratio, conventional forces can be dedicated to intelligence collection.

The term "presence patrol" has made its way into the military vernacular. While some would argue that "reconnaissance and surveillance" patrol is a more accurate term, the fact is many patrols are merely presence. Presence patrols reassure both potential wrongdoers and the law abiding populace that their remote location has not been forgotten. While these patrol leaders have been briefed on their collection requirements, those requirements usually take a back seat to presence.

By sending patrols to actively collect, the focus of the patrol leader and its members is on intelligence. One successful method to ensure the destruction of the "presence patrolling" mindset is by conducting longer patrols that give the leader more latitude. For example a patrol is given 72 hours to collect five basic pieces of information on a specified OC-related high value target (HVT) (location of home, location of work, work hours, car with license plate, and a photograph of the person.) This technique gives the leader the freedom to move when and where he sees fit, and is loosened from the constraints of a six hour patrol. By focusing on the intelligence target rather that time spent in a certain place, patrols will be present over a wide area, while still gaining valuable intelligence.

One concern is that the patrols will begin to try to take on the characteristics of a Human Intelligence (HUMINT) Collection Team (HCT). To mitigate this risk the patrol leader is thoroughly briefed on the specific requirements that the patrol can collect on without crossing over. Soldiers must be trained on the techniques of tactical questioning, use of interpreters, and overt and covert LP/Ops. As always, the targets selected must be nested within the collection emphasis and meet the commander's intent.

The ability to orient patrols on a long term intelligence objective is a luxury enjoyed less in combat environments than in peace operations. Conventional troops patrolling in Baghdad have far less ability to focus on an intelligence target because they are not afforded the ability to move with relative impunity. The very ubiquity of Soldiers and military vehicles that move freely around a mature peacekeeping environment allows Soldiers focused on an intelligence objective to hide in plain sight. This ability, in conjunction with the greatly reduced risk of attack, grants the freedom of movement that is necessary for an intelligence oriented patrol.

Targeting Organized Crime

The identification of an OC element by uniformed peacekeepers begins by earning the trust of the local populace. Upon arriving in theater, the primary task of any unit should be to get their Soldiers talking to the local populace. Doing this achieves many goals. It initiates, through effective dialogue, relationships between the peacekeeper and populace. This personal involvement demonstrates the peacekeepers' resolve, and by talking face to face with the peacekeeper, preconceived notions can be dispelled through respectful, yet candid, dialogue. Over time if these conversations are managed effectively and occur on a consistent basis, they will result in a willingness of the populace to begin to inform the peacekeepers about security threats in their area. This is especially true if they see that the peacekeepers taking an active role in undermining the authority of OC elements.

Consistently developing useful and constructive relationships with the populace requires discipline by the Soldiers and leaders to explain the mission completely. Patrols remain *focused events* and do not evolve into routine events where individual Soldiers are simply going through the motions. Additionally, all information that Soldiers collect must be passed higher for fusion with previously collected information. That information can be analyzed and used to drive follow-on missions. Soldiers given actionable intelligence and a meaningful mission will perform splendidly. Conversely, it should surprise no one that when Soldiers are given "cookie cutter" lists of things to look for and vague missions, these Soldiers will begin to go through the motions, especially as long deployments wear on.

Over time the peacekeeper can develop a good rapport with the local populace. Both Soldiers speaking to average people or leaders engaging spheres of influence need to be cognizant of the subtle signs that locals want to talk discreetly about topics. When dealing with OC elements, retaliation can be severe against individuals who assist peacekeepers or law enforcement. As such, care needs to be taken when discussing such matters with the locals. Collect information from the local national about the OC group in as detailed a manner as possible uses the 5Ws and H principle (Who, What, When, Where, Why, and How). Upon receiving this information, corroborate the information provided. Some items to consider are whether the information was provided by a disgruntled neighbor, a competitor, or is it a genuine concern. Additionally, how should this person be handled during follow on visits? Is it safe for the local to continue to talk with uniformed peacekeepers about this topic, or does this person need to be handed off to an HCT which has a lower profile than the uniformed soldier? Two key considerations that will drive the decision regarding how to handle this local will be what the likely threat to this local is if the OC element discovers the transfer of information, and will it look unusual for Soldiers to be speaking with this individual. Again, if it is decided to continue collection on the local populace using conventional assets, leaders need to ensure that their Soldiers clearly understand the legal limitations placed on non-HUMINT collectors. The bottom line is all Soldiers can talk to the populace and ask direct questions. However, non-HUMINT collectors can not task, recruit, or coerce, according to **Special Text 2-91.6, Small Unit Support in Intelligence**.

In developing a better picture of the OC group, key questions need to be answered. From the perspective of operations and intelligence officers in a permissive theater, one of the most important questions to answer is whether the local government/law enforcement is willing, and/or able to effectively combat/confront the OC element. A collection plan is required to answer this question.

The first question when considering a strategy to target OC must be "Can the local government confront this problem on their own?" If they have the capability, then continue to guide them in that direction. If this is not possible then leaders must determine what needs to be done so the local government can eventually confront this problem. In determining a course of action key questions about the local government, judiciary, military, and police force need to be answered to determine how to proceed. Is the local government, or elements of it, willing to confront the OC element but paralyzed by the fear of retaliation? Are parts of the government and/or police force assisting the OC element? If law enforcement is in collaboration with OC, which other parts of the government can be reasonably expected to assist? A detailed collection plan needs to be developed to learn who one can and cannot work within the government and police force to remove or reduce the threat posed by the OC element. Techniques that can be used to collect information on the local government are:

- ✦ Periodic meetings with local government and police to gauge their ability to confront the OC threat.
- ✦ Observation by patrols on how the police conduct themselves in regards to the OC threat.

- Conversations with the local populace to determine its opinions about the local government and police force's ability to confront the OC threat.

It will likely be determined that some individuals are colluding with the OC element and therefore need to be targeted. There are multiple ways to target these individuals and each approach depends on the specifics of the situation and the rules of engagement (ROE.)

As previously mentioned the monopoly of the threat of force is a basic pillar of a legitimate law enforcement structure. When the threat of force by OC groups becomes so extreme as to be a fundamental impediment to a safe and secure environment, it then becomes a military problem to be confronted by peacekeepers. When developing an OC targeting and collection plan, part of the critical path must include a system to give to the local government, a monopoly on the threat of force. The following plan is proposed.

Disrupt/Deceive/Inform/Influence

One cautionary note before beginning any disruption operation: insure that prior to targeting individuals or businesses that your information has been corroborated by at least two sources of intelligence and ideally by different intelligence disciplines such as Imagery or HUMINT, etc.

The first step in restoring the local authorities' monopoly on the threat of force may be for a peacekeeping force to degrade the OC element. This will not often be as simple as acting on intelligence and capturing an individual. The ROE will likely forbid such straightforward solutions because in mature peacekeeping environments a large degree of sovereignty has been handed back to the local authorities. This alone restricts the peacekeepers' ROE. An OC member can be captured and handed over to the local police only to be released because of corrupt and/or frightened prosecutors and/or judges. The answer to this peacekeeping challenge may be to conduct overt disruption operations on the OC element in conjunction with an aggressive IO campaign targeting the local populace, police, and judiciary.

The purpose for the overt disruption operations directed against the OC element is multifaceted. The first is the reduction of the invincible image that the local populace and police force may have about the OC element. Each disruption is also an intelligence collecting opportunity. The third purpose is to co-opt OC to do what you want them to do. By making your disruption seem like a cause and effect scenario (i.e., if the criminal stops threatening other people, the peacekeepers will stop disruption of his business) you can effectively shape some of his actions. The final purpose is to enter his decision cycle, forcing him to take actions in reaction to the actions of the peacekeeping forces, not the other way around. Furthermore, effectively focused operations should hurt the OC element financially, thus driving up the cost of doing business. Finally, the purpose for the IO campaign is an explanation to the local populace of why they had to be inconvenienced during an operation. These encounters demonstrate resolve to confront this criminal problem and encourage the local populace and police to stand up against the OC element.

Effectively targeting OC requires an understanding of their center of gravity (COG). The COG for OC is most often profit, rarely are OC groups ideals-based. Even in Iraq criminal gangs are beginning to emerge. Their actions are driven by profit, not religious zeal. Money is the driver which makes all other things possible for OC; it allows them to sustain themselves, and to keep their enterprises functioning. Money also allows them to buy political favor outright, or buy the tools and weapons that allow them to coerce favorable actions.

Soldiers examine and catalog large amounts of cash discovered during disruption operations aimed against organized crime in Kosovo.

Material possessions beget power and prestige with communities that often have very little. Negatively impacting an OC group's cash flow can have a very profound effect on the organization as a whole, and should be a major action undertaken by peacekeepers within the ROE.

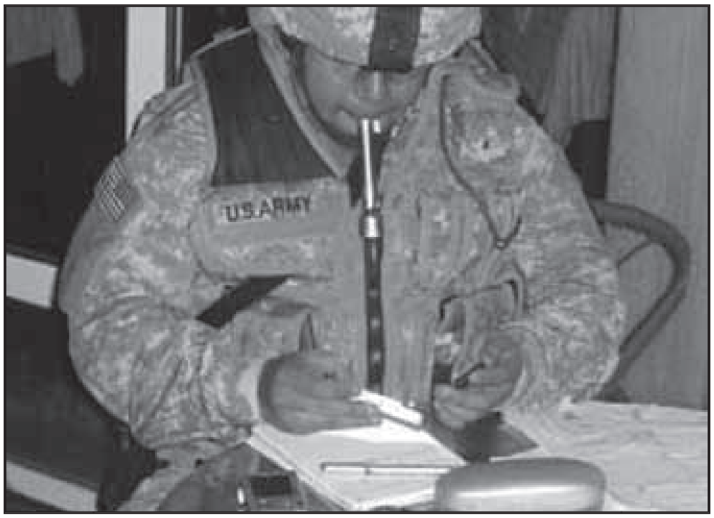
To effectively target this type of organization the peacekeeper needs to understand how the OC element functions. Identify how the OC operation works and look for opportunities to disrupt those operations. OC elements typically operate in a reverse cycle. This presents peacekeepers with a window of time during normal day operations to target OC groups in their rest cycle, denying them the opportunity to rest and tend to family issues. Tired criminals are careless criminals. This opportunity as well as night operations aimed at impacting the places of business of OC groups present the peacekeepers and law enforcement authorities multiple options. To determine the best option, or operational mix of the two, leaders must consider the situation as a whole.

Do the OC elements have legitimate businesses that act as a front for their illicit operations? If business fronts are identified they can be targeted to both disrupt operations and collect intelligence on those establishments. Restaurants, bars, and factories are a few examples of legitimate business fronts that OC elements can use to conceal their illicit activities. These business fronts can act as meeting locations as well. During disruption operations these businesses can be effectively shut down for hours during a search, or days with the use of posted peacekeepers preventing access, depending on the desired effect on the OC element.

Upon entering one of these establishments as part of a disruption team, all individuals need to be tactically questioned and photographed to develop a baseline of information regarding who possibly associates with the OC element. The photography is particularly important as it serves to both document and intimidate the OC figures. Next, the establishment needs to be searched to exploit any incriminating documents or reveal concealed grey or black market goods. Additionally, messages need to be delivered to the suspected OC members and a separate message to individuals that may have been incidentally caught up in the disruption operations. The message to the OC members can be used to inform, influence, or deceive. In addition to the verbal or written messages, the mere presence of peacekeepers during the disruption operation will send a non-verbal message to the OC members and the local populace alike. The message to individuals who may have just been incidentally caught up in the operations is needed to explain why the peacekeepers conducted this operation. This message is needed to mitigate some of the 2nd and 3rd order effects associated with conducting such aggressive operations.

The timing and frequency of these disruption operations can be used as a leverage to influence behavior of the OC members or group. Disruption operations will drive away customers and employees and this fact needs to be used against the OC element. The desired result of disruption operations directed against these establishments demonstrates peacekeeper resolve to the local populace and police force, and publicly degrades the OC element's standing in the community.

It is also useful to examine the transportation networks that the OC element uses to move their grey and black market goods. A holistic, production to customer approach needs to be taken to determine how OC elements move their grey and black market goods. Pieces of the OC logistics network to be evaluated are: production facilities, post production cache sites, inter-modal transportation methods, cross border transportation methods, long range transportation methods, consolidation/deconsolidation cache sites, and customer pick up points. Each one of these logistic nodes needs to be evaluated to identify vulnerabilities for exploitation. The



A Soldier with the 1st Battalion, 141st Infantry Regiment examines and catalogs information from cell phones during disruption operations aimed against organized crime in Kosovo.

goal is the drive up the cost of doing business for the OC element through intelligence driven disruption operations of their logistics network. When crime no longer pays, it will stop.

It is vital to identify the individuals that work for or help prop up the OC group. Conversations with the local populace and the police force and observation of suspected OC frequented establishments enhance the knowledge base of which individuals are involved with the OC element. Once OC members are identified, attempt to limit their freedom of movement and collect additional information such as: vehicle description, work location, home location, times at work and at home, and a photo of the individual. This information can be used in follow on missions directed against this individual.

Re-assessment

Periodic reassessment of both OC capabilities and local authorities' reaction to disruption operations is necessary. If local authorities' actions directed against the OC element have increased, the peacekeeping task force needs to decrease disruption operations accordingly. In conjunction with the reduction in disruption operations, the peacekeeper should continue to periodically assess local authorities' ability to confront this threat. However, if local authorities' actions directed against OC threat do *not* increase, then develop a collection plan to determine why not. Has the OC element been sufficiently degraded that the local police can confidently confront them? Upon re-assessment increase disruption operations in conjunction with IO messages. Is the leadership within the police force colluding with the OC element (and therefore no amount of degradation of the OC element will spur action from the police force)? While working within the ROE of that specific theatre, determine a plan targeting the police officers who are colluding with the OC element. There may be an international organization which provides oversight for local police and other government officials. If this is the case, attempt to coordinate with oversight officers to apply additional pressure on the local police. Each theatre will be different in regards to the degree of sovereignty that has been handed over to the local police force and what powers the international community retains. Apply that power to bring additional pressure on the local police force to reprimand, fire, or arrest suspected corrupt police officers or leadership. Finally, messages directed at the local populace regarding the societal threat that OC presents also applies pressure on the local police force to act. Be careful not to undermine the police force. The 2nd and 3rd order effects of publicly identifying corrupt police officers will likely outweigh the benefits gained by outing the corrupt officer.

The re-assessment and adjustment cycle will continue based on local authorities' abilities and OC threat. If progress slows or stops a return to implementing phase one (disrupt/deceive/inform/influence) may be required.

The long term endstate is local government regaining a monopoly on the threat of force. This is a strategic level achievement. On a battalion or brigade level, positive movement toward that endstate during the course of a deployment is a reasonable goal. Setbacks should be expected during this long and incremental process. Persistence is the keystone to success. Although the peacekeeping force is capable of dealing with the OC threat in the short term, it is imperative that the local authorities become more involved in combating the OC threat. Successful progression towards an exit strategy requires the peacekeeper to constantly seek opportunities to get the local authorities involved.

Conclusion

OC's pervasiveness reaches all aspects of an emerging state. Leaders in a peacekeeping mission must understand the effect of this enemy on a free and healthy society—both political and economic. Despite the challenges of a peacekeeping mandate, certain conditions do exist to effectively target OC. By understanding OC as a business, it is possible to craft a targeting and collection cycle that not only strikes the heart of that business but also targets its enablers. As the hotspots of today's conflict slowly cool and turn toward a more permissive state, Army leaders would do well to keep abreast of the lessons from today's situation in the Kosovo as a handrail for tomorrow's operations in Afghanistan and Iraq.

Major Oliver Mintz is a graduate of the United States Military Academy and has held positions from Infantry Platoon Leader to Infantry Battalion S3. At the time of writing he was completing a tour in Kosovo where he held positions as a Brigade Battle Captain and the Battalion S3 for 1-141 IN (TF ALAMO) Texas National Guard.

Second Lieutenant Tory House served as the Tactical Intelligence Officer for 1-141 IN (TF ALAMO) Texas National Guard and deployed to Kosovo as part of KFOR 7 from December 2005 to December 2006. 2LT House is a graduate of St. Edwards University with a degree in Computer Systems Management.

CONTACT AND ARTICLE
Submission Information

This is your magazine. We need your support by writing and submitting articles for publication.

When writing an article, select a topic relevant to the Military Intelligence or Intelligence Communities (IC).

Articles about current operations and exercises; tactics, techniques, and procedures; and equipment and training are always welcome as are lessons learned; historical perspectives; problems and solutions; and short "quick tips" on better employment or equipment and personnel. Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the IC at large. 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 discuss how new technology will change the way we operate.

When submitting articles to MIPB, please take the following into consideration:

- Feature articles, in most cases, should be under 3,000 words, double-spaced with normal margins without embedded graphics. Maximum length is 5,000 words.
- Be concise and maintain the active voice as much as possible.
- We cannot guarantee we will publish all submitted articles.
- Although ***MIPB*** targets themes, you do not need to "write" to a theme.
- Please note that submissions become property of ***MIPB*** and may be released to other government agencies or nonprofit organizations for re-publication upon request.

What we need from you:

- A release signed by your local security officer or SSO stating that your article and any accompanying graphics and pictures are unclassified, nonsensitive, and releasable in the public domain **OR** that the accompanying graphics and pictures are unclassified/FOUO. Once we receive your article, we will send you a sample form to be completed by your security personnel.
- A cover letter (either hard copy or electronic) with your work or home email addresses, telephone number, and a comment stating your desire to have your article published.
- Your article in MS Word. Do not use special document templates.
- A Public Affairs release if your installation or unit/agency requires it. Please include that release with your submission.
- Any pictures, graphics, crests, or logos which are relevant to your topic. We need complete captions (the who, what, where, when, why, and how), photographer credits, and the author's name on photos. Please ***do not embed*** graphics or photos within the article's text, attach them as separate files such as .tif or .jpg. Please note where they should appear in the article.
- The full name of each author in the byline and a short biography for each. The biography should include the author's current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications. Please indicate whether we can print your contact information, email address, and phone numbers with the biography.

We will edit the articles and put them in a style and format appropriate for ***MIPB***. From time to time, we will contact you during the editing process to ensure a quality product. Please inform us of any changes in contact information.

Send articles and graphics to sterilla.smith@conus.army.mil or by mail on disk to:

ATTN ATZS-CDI-DM (Smith)
Military Intelligence Professional Bulletin (MIPB)
Box 2001
Bldg. 51005
Fort Huachuca, AZ 85613-7002

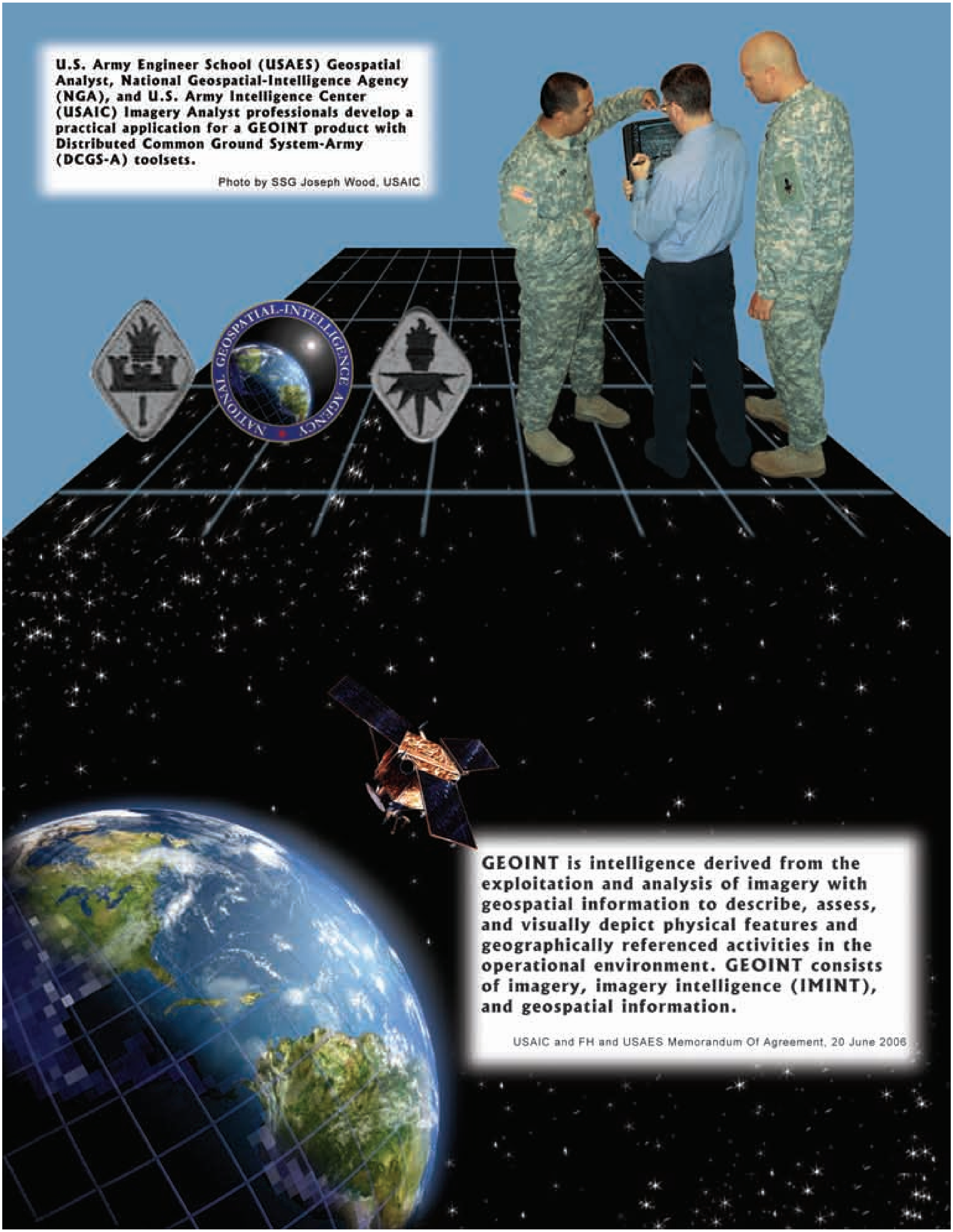
If you have any questions, please email us at sterilla.smith@conus.army.mil or call COM 520.538.0956 DSN 879.0956. Our fax is 520.533.9971.

Upcoming Themes and Deadlines

January - March 08 Issue:

Knowledge Management	31 Dec 07

08 Upcoming Themes and Deadlines
available in the
October - December 07 issue.



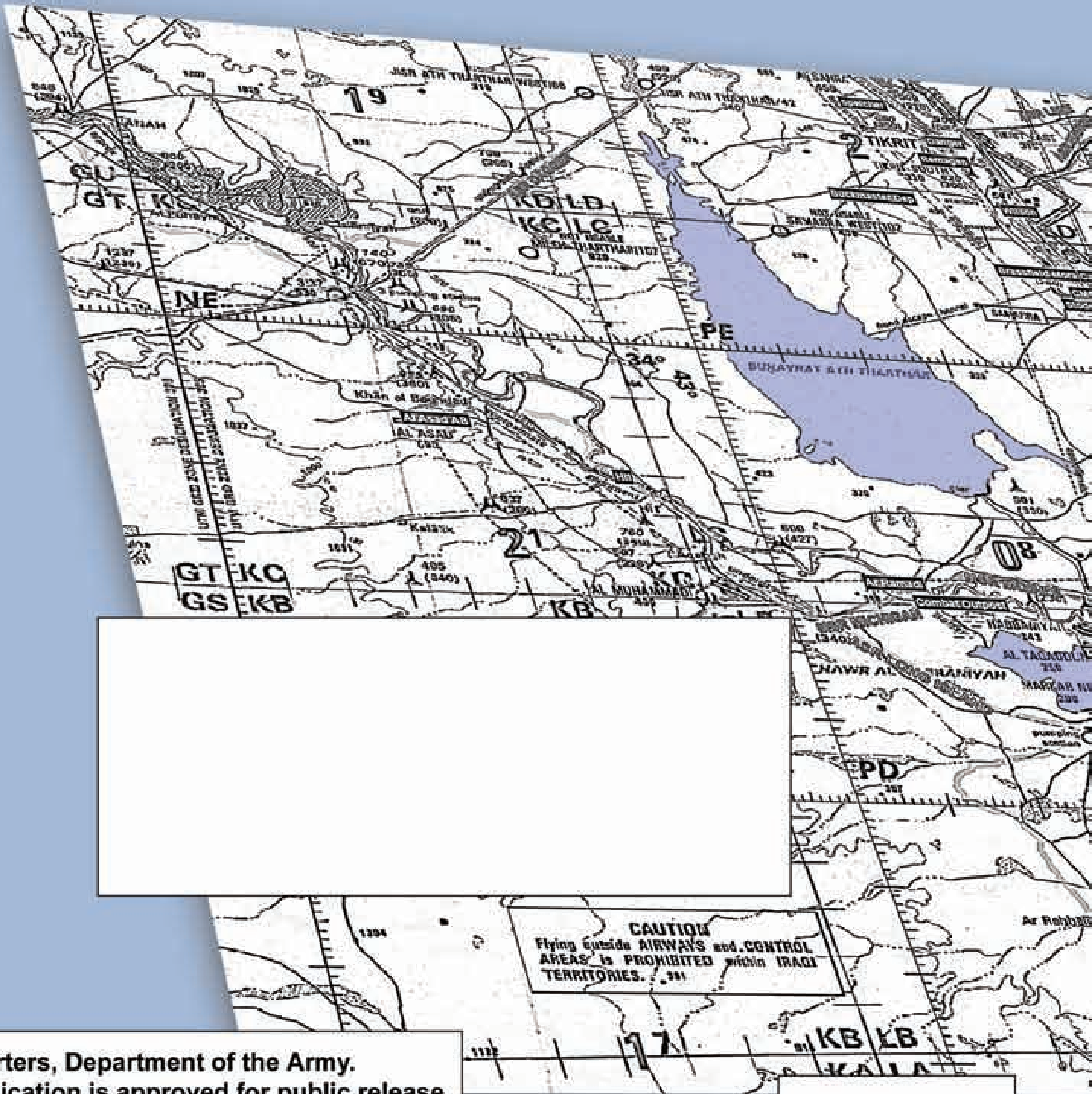
U.S. Army Engineer School (USAES) Geospatial Analyst, National Geospatial-Intelligence Agency (NGA), and U.S. Army Intelligence Center (USAIC) Imagery Analyst professionals develop a practical application for a GEOINT product with Distributed Common Ground System-Army (DCGS-A) toolsets.

Photo by SSG Joseph Wood, USAIC

GEOINT is intelligence derived from the exploitation and analysis of imagery with geospatial information to describe, assess, and visually depict physical features and geographically referenced activities in the operational environment. GEOINT consists of imagery, imagery intelligence (IMINT), and geospatial information.

USAIC and FH and USAES Memorandum Of Agreement, 20 June 2006

ATTN: MIPB (ATZS-CDI-DM)
BOX 2001
BLDG 51005
FORT HUACHUCA AZ 85613-7002



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

PIN: 084118-000