MIPB

Military Intelligence Professional Bulletin

January - March
2007
PB 34-07-1

Counterinsurgency

From the Editor

This issue focuses on counterinsurgency operations(COIN); the articles ranging from tactical level to support to Joint operations.

Increasingly, the articles we receive for publication are being designated as unclassified/For Official Use Only (FOUO), requiring protection. Please access the following MIPB FOUO articles at the University of Military Intelligence: www.umi-online.us/mipb; Intellink-SBU: www.mipb.osis.gov, and on ICON: https://icon.army.mil

January-March 07

RSTA Squadron Operations in the Stryker Brigade Combat Team
by Captain John C. Griswold

Logical Lines of Operations: A Planning Construct for Full Spectrum Operations
by Jack D. Kem, PhD

CJTF Effects Assessments: a Paradox in Military Decision Making
by Lieutenant Colonel James D. Lee

October-December 06

NRO's Web based Access and Retrieval Portal (WARP) Training Initiative
by Donald Smith, NRO

Geospatial Intelligence in Urban Areas
by Steven E. Rogan, NGA

The National Counterterrorism Center (currently unavailable)

by Keith M. Preising

April-June 06

Department of the Army Intelligence Information Services (DA IIS)
by Dennis F. Murphy

January-March 06

MIRC Mission and Organization
by Lieutenant Colonel Michael Sands

Lessons Learned Trends: August 2005 Through March 2006
by Lessons Learned Team, Directorate of Doctrine, USAIC&FH

October-December 2005

History of Open Source Exploitation in the Intelligence Community
by Douglas Peek

OpenSource.gov
by Douglas Peek

SIR: The Value of Sound
by Dr. John N. Monroe, Jr., PhD

Every Dog Has Its Day, and Every Soldier is a Sensor (ES2)
by Robert A. Cuddeback

Sterilla A. Smith

Sterilla A. Smith
Editor

MILITARY INTELLIGENCE

PB 34-07-1 Volume 33 Number 1 January - March 2007

Commanding General
Major General Barbara G. Fast

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

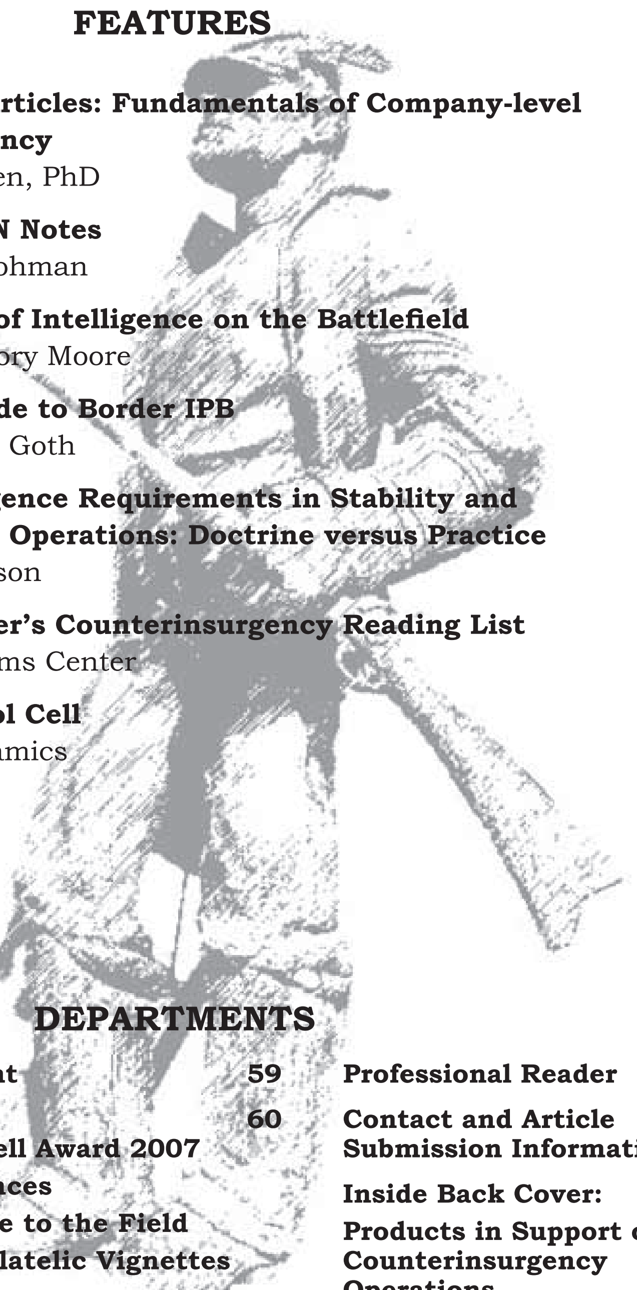
Associate Design Director/NCOIC
SSG Philip M. MacCluskey

Design and Layout Team
SSG Patrick N. Franklin

Cover Design and Inside Back Cover:
SSG Patrick N. Franklin

Issue Photographs:
Courtesy of the U.S. Army

FEATURES



DEPARTMENTS

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.

By order of the Secretary of the Army:
Official:

Joyce E. Morrow
JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0704304

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

ALWAYS OUT FRONT

by Major General Barbara G. Fast
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. My goal in this article is to update you on our efforts to ensure GEOINT is fully incorporated into the Military Intelligence strategic goal—to provide the force with integrated Intelligence capabilities. In February 2006, I approved the designation of GEOINT as an Army Intelligence discipline and directed a full functional review of GEOINT 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/statements for the Commanding General (CG), USAIC.
- ✦ Facilitate the integration of solutions.

Our C2G effort is done in coordination with a wide range of GEOINT players to include National Geospatial-Intelligence Agency (NGA), INSCOM, USAES, 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 the U.S. Army Engineer School (USAES), the other armed services, and the 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/MCRP-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 cells and structures at the brigade through Army Service Component levels to facilitate information sharing and GEOINT production. The proposals, if approved, 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 military occupational specialties (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 Intelligence (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 96H/35H. Upon acquiring additional resources we will expand

(Continued on page 4)

CSM FORUM

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

Note from the 111th Military Intelligence (MI) Brigade CSM

First of all let me introduce myself, I am CSM Gerardus Wykoff coming out of the 101st Airborne Division (AASLT) where I served as the G2 SGM for about five months and then as the 2-101 Brigade Troops Battalion CSM for the last 23 months. Now that I have given you a little background on myself I would like to talk about the great things the 111th MI Brigade is doing to ensure that our MI Warriors are trained and ready to leave the training base and move out to the theaters of operation. For the first time in history we are making changes to the Program of Instruction (POI) on a monthly basis. We are working with units that are down range, getting the latest tactics, techniques, and procedures (TTPs) and trends to ensure we are training our MI Warriors to meet today's challenges. I want to break it down by battalion on how we are accomplishing this and the challenges we are facing in order to provide the field with the best trained MI Warriors.

304th MI Battalion

Within the 304th MI Battalion numerous changes have been made and continue to be made to the POIs for the Officer courses: Basic Officer Leader Course (BOLC); MI Captains Career Course (MICCC): Areas of Concentration (AOCs) 35C, 35G; G2/S2X; Warrant Officer Basic Course (WOBC) and WO Advanced Course (WOAC); Sensitive Site Exploitation, Cultural Awareness, Intelligence Support to Counterinsurgency Operations; Warrior Tasks and Battle Drills; Urban Intelligence Preparation of the Battlefield; Distributed Common Ground Station-Army (DCGS-A) training, and most noteworthy the Joint Intelligence Combat Training Center (JI-CTC). Not one course in the battalion is taught the same as the class before. Lessons learned and TTPs from the War on Terror (WOT) are incorporated during each course that effect change in the next iteration. Experienced captains and WOs attending class bring their lessons learned directly from the MI portion of the WOT battlefield and most are incorporated into the learning environment.

After reflecting on the lessons learned from Operations Enduring Freedom (OEF) and Iraqi Freedom (OIF), the U.S. Army Intelligence Center and School at Fort Huachuca identified a need to train both officers and Soldiers to perform intelligence analysis and support operations against a con-

(Continued on page 5)

(Continued from page 2)

MOS 96D/35G training to ensure we more thoroughly train these new skills.

Our MOS 96D/35G and 96H/35H Skill Level 10 through 40 soldiers, warrant officers and officers are exposed to division level GEOINT Cell 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 cells include:

- FMV exploitation.
- Unmanned Aerial System (UAS) basic flight operations, mission planning.
- Joint Surveillance Target Acquisition Radar System (J-STARS) MTI exploitation.
- Cross-cueing of assets, emphasis on UAS and MTI.
- Writing reports hyperlinked to Imagery Derived Product (IDP) and raw imagery in concert with the Distributed Common Ground Station-Army (DCGS-A), video clip 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 (GOB) analysis.
- Briefing skills.
- Communications skills and systems.
- 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 (Version two) GEOINT toolsets and applications

JI-CTC GEOINT training today includes sister services and 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 tools sets. The Engineer's Digital Topographic Support System (DTSS) will be integrated with DCGS-A 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 level skills one needs to understand to fully exploit GEOINT and all its components–Imagery, IMINT and Geospatial Information and Services (GI&S). We have begun to analyze these skills, reviewing what and where we currently train, and then looking towards expanding and updating that training.

Personnel. Along with possible organizational changes we have been looking at what MOSs we will need for the future. The first changes are in our MOSs 96H/35H Common Ground Station Analyst and 96D/35G Imagery Analyst. With the transition of CGS from a stand alone station to its inclusion into DCGS-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 MOSs 96D/35G and 96H/35Hs, we have proposed merging these MOSs by fiscal year 2011 and provide reclassification training for 96H/35Hs to become 96D/35Gs. Reclassification training is currently planned to last 10 weeks.

Other personnel issues include a detailed examination of 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 35C AOC should be a Skill Identifier (SI) and taught only to those projected to go to an IMINT assignment.

Facilities. While Army wide GEOINT production does not require new facilities, we are examining whether GEOINT training facilities are adequate.

Conclusion

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 need today but will also be able to provide more detailed, accurate, timely, and relevant visualization products to the warfighter 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!

CSM Forum

(Continued from page 3)

temporary enemy in a tactical environment using the same equipment and resources available in Afghanistan and Iraq. The JI-CTC was initially established in the officer training battalion to train and test these requirements. Today, the JI-CTC conducts over 20 rotations per year, preparing over 2,200 Soldiers to conduct their intelligence mission in a Joint, Interagency, Intergovernmental, and Multinational environment.

During the intense week-long exercise Soldiers are challenged to meet three training objectives, all of which support the commander’s visualization and understanding of the enemy and the operational environment. The first objective is to support situational understanding by establishing and maintaining the enemy common operating picture, conducting pattern and predictive analysis, and providing intelligence assessments. The second objective is to conduct intelligence, surveillance, and reconnaissance (ISR). Students will recommend priority intelligence requirements, develop ISR overlays and matrices, and manage ISR assets and their employment. The final objective is to provide intelligence support to effects by developing a high value individual list, preparing both lethal and non-lethal target packages, and conducting combat assessments.

JI-CTC is the culminating event for intelligence personnel trained at Fort Huachuca. The exercise replicates the Intelligence Battle Staff from the Chief of the Division Analysis and Control Element all the way down to the junior analyst at the maneuver battalion. In order to integrate Soldiers from multiple military occupational specialties (MOSs) and training conducted at multiple locations, a scenario has been developed that is based on the current situation in Iraq.

On Training Day Zero, the division ACE, brigade combat team, and supporting battalions all go through a relief in place briefing to prepare them for upcoming operations. As the students begin their Tactical Operations Center (TOC) set up, the enemy senses vulnerability due to the transition and insurgent activity increases. Students from Advanced Individual Training courses, noncommissioned officers (NCOs) from the ANCOC and BNCOC, warrant officers from WOBC, lieutenants from the BOLC, and captains from the MICCC must quickly identify and track the threat, analyze the data passed on from the unit they replaced, and then make recommendations to their leadership on what actions to take in order to protect U.S. personnel, to support the Iraqi government and the local community, and to target the insurgents. A digital operating environment links students training at Rowe Hall, Site Maverick, and Sites Uniform and Papa with Signals Intelligence (SIGINT) Soldiers training at Goodfellow Air Force Base in Texas. In addition, international officers are integrated into JI-CTC through their participation in the Coalition TOC.

To ensure all students are well prepared intelligence specialists upon their arrival at their next duty station, the exercise at JI-CTC is fought using the latest computer based hardware and software. The scenario incorporates over 100,000 messages from all intelligence disciplines and the availability of the DCGS-A platform provides students with multiple resources to collect, process, analyze, and disseminate intelligence information. Prior to attending JI-CTC all students receive training on the DCGS system and its applications and are therefore expected to utilize all of their resources to keep the commander apprised of the enemy situation and able to make informed decisions.

The JI-CTC is unique as it allows students from all ranks and intelligence specialties to work together in a (simulated) tactical environment. It provides many of them with their first taste of what to expect when they enter a battalion or brigade TOC for the first time. This capstone event will continue to evolve as new insurgent TTPs are incorporated into the scenario and Army Intelligence adapts based on lessons learned from those currently engaged with the enemy.

305th MI Battalion

The 305th MI Battalion trains our MOSs 33W (MI Systems Maintainer/Integrator), 96B (Intelligence Analyst), 96D (Imagery Analyst) and 96H (Common Ground Station Operator). Soldiers and continues to expand the courses in depth but not time. It has initiated Every Soldier is a Sensor (ES2) and Cultural Awareness training into all classes. All Soldiers receive Drivers' Training and should arrive at the new unit with a DA 348, Equipment Operator's Qualification Record. We have included in all courses Military Operations in Urbanized Terrain (MOUNT) Training, Warrior Tasks and Drills (WTD), a Convoy Live Fire Exercise (with a new range opening in May), and Combatives training. For specific MOSs we are adding new skill sets to help ensure that students are being trained in the latest systems available in the school house. We continue to request and receive some of the latest devices that are being used down range.

We are incorporating DCGS-A and a field training exercise (FTX) updated with battalion/brigade/division TOCs (currently an eight day FTX) into 96B training. For 96H we train moving target indicator forensic tools and for 96D skill level I we are adding a geospatial intelligence (GEOINT) program. On the 33W side of the house we are updating new systems training (TROJAN/PROPHET), are no longer training on outdated systems (i.e., TRQ/TLQ), and awaiting the new Critical Task List (Computer Network Operations), LANs, and Establishing Computer networks.

309th MI Battalion

For all 309th MI Battalion courses there is an increase in WTD with ES2. WTD are integrated and trained deliberately as well as integrated into daily activity to increase muscle memory. Cadre question and test Soldiers on awareness of their surroundings such as "What was different on the way to class?". The battalion is also including cultural awareness training. It is taught formally as well as integrated into the POI and the company area (*foreign language* word of the day). We are integrating 96Bs into the 97E (Human Intelligence Collector) FTX and JI-CTC. The training includes Convoy Live Fire Exercise (CLFX) and Advanced Rifle Marksmanship (ARM). Students from the 304th (second lieutenants) are sometimes included in CLFX.

We have added a rural block into the Source Operations Course (SOC). The block is approximately 10 days long and is designed to replicate Source Operations outside urban areas, like 95 percent of Afghanistan. We also updated the scenarios to replicate current U.S. Army Central Command (CENTCOM) operations. Due to the course classification; a location of the final phase is in Tucson. The U.S. Air Force assists us with space on Davis-Monthan Air Force Base for TOC operations.

MOS 97B (Counterintelligence Agent (CI) changes from a skill level 10 level course to a 20/30 level. The course is no longer an enlistment option but is a reenlistment option. The goal is to produce a mature agent with some "life experience." The course includes blocks on Terrorism, Cultural Awareness, Use of an Interpreter, Military Source Operations, Investigations, and Surveillance. The course is very intense so proper preparation and screening via the CI screening process is a must.

MOS 97E has changed scenarios to replicate the CENTCOM area of responsibility (AOR). We teach a skill set that is applicable everywhere, however since the current push is CENTCOM, we use that AOR as a backbone. The student ratio is reduced to allow cadre to better evaluate Soldiers and provide increased feedback. The booth iterations increased from three to nine. That means a Soldier has at least 27 hours of interrogations training prior to completing the course. We introduce all 97E10s to source operations and they have a minimum of 18 source meets with cadre personnel. We have increased the FTX to ten days. During the FTX Soldiers replicate living on a forward operating base in the CENTCOM AOR. They are required to conduct source operations, screening, interrogations and walk-in debriefs. The NCOs in the class are given the opportunity to run their teams for MI operations as well as troop leading procedures. To facilitate this, teams are rotated through a Traffic Control Point, a Forward Collection Point, and a small populated (cadre) village. There is heavy emphasis on the Laws of War. If a student gets a 100 percent on a practical exercise (PE) such as Interrogations and violates a Law of War, the Soldier fails that PE.

344th MI Battalion

The 344th MI Battalion trains four diverse MOSs ranging from firefighters to intelligence Soldiers. This presents unique challenges when trying to ensure our graduates are both technically and tactically proficient. The goal of every member of this unit, whether they are a Drill Sergeant or instructor, is to ensure the Soldiers who graduate can be an immediate asset to their unit, regardless of whether that unit is at Buckley Air Force Base, Fort Stewart, or Fort Bragg. To achieve this goal, training throughout the battalion has to mirror the doctrine and current TTP. To accomplish this, command emphasis is placed within all levels of command to ensure all trainers are trained on the most up to date TTPs used by our units currently deployed to OEF/OIF as well as the methods used by our adversaries.

The battalion accomplishes this through the use of one of its most important resources—*our combat veterans*. Through the incorporation of first hand knowledge of all combat experienced members of the unit, our students receive the know-how needed to be an effective and productive member of a unit as soon as they arrive. As new cadre members, recently returning from missions around the world, arrive at the unit, we incorporate their experiences into our tactical and technical training. This continuous influx of experience and skills is probably the most important aspect of keeping our technical and technical training realistic and relevant.

The battalion also changes its training to satisfy the needs of units receiving our Soldiers. A recent example is when feedback from units indicated a deficiency in our Soldier's ability to safely handle their weapons during deployments. In response, the Battalion initiated Weapons Immersion Training (WIT). This month long training having students keep and safeguard their personal weapons has led to increased awareness and weapons safety. It is hoped this program will mitigate negligent discharge incidents during deployments. Feedback from units since the training started indicates the training has proven very successful.

Complementing the Battalion's efforts, each company leads its own initiatives to tailor training to meet MOS specific technical and tactical needs. These efforts, outlined below, reflect personal initiatives of the Soldiers of this command, and reflect greatly on their professionalism.

- ✦ Alpha Company's current efforts center on preparing all its SIGINT Analyst Soldiers to be tactically and technically proficient through the incorporation of lessons learned from Special Operations veterans currently assigned to the unit. These lessons learned have been included into the FTX scenarios and small unit tactics. The Special Operations veterans have had excessive experience with patrols outside the wire and were involved in the planning of the training objectives used in the FTX scenarios. These veterans' experiences were also used to update OPFOR on cultural tendencies and behaviors to more closely mimic what realistically happens in theater. We have also incorporated a methodical Crawl-Walk-Run approach to Army Warrior Training to ensure that our trainers and potential trainers have a thorough understanding of the fundamentals and procedures of tactical maneuvers before they supervise training or take a leadership role in the training. Current efforts also include the standardization of TTPs taught within the company with extensive participation by combat experienced Drill Sergeants and cadre to ensure all students achieve a minimum level of tactical proficiency.
- ✦ Bravo Company is a prime example where, regardless of MOS, all soldiers must be trained to the same standard. The company trains initial military training (IMT) Soldiers to be Firefighters and Voice Interceptors, two very diverse skills that we hold to the same standard of tactical training. Both groups of students participate in a combined FTX with Alpha Company. The company's technical training is constantly being updated to reflect any changes in order of battle, communications equipment and procedures, as well as weapons systems and tactics in numerous target languages to include standard Arabic as well as the Iraqi dialect.
- ✦ Charlie Company is responsible for six different courses in three platoons: Manual Morse, 98Y (Signals Collector/Analyst) Phase II (IMT), 98C (Signals Intelligence Analyst) Transition, 98Y (formerly 98K) Transition, Prophet Analyst, and Prophet Operator courses. The company has initiated a successful effort to incorporating tactically oriented lessons learned from currently deployed or re-deploying forces throughout the Middle East using scenario based training. The training focuses on familiarizing Soldiers on the methods currently being used during conventional patrolling operations, and imparts valuable cultural awareness considerations. Emulating the Joint Readiness Training Command and National Training Command and incorporating an array of training events (multiple obstacle courses, Engagement Skills Trainer 2000, Maneuver on Urban Training Complex), the field training exercises impart a greater ability to Soldiers to problem solve and rapidly advance in tactical understanding and skill.

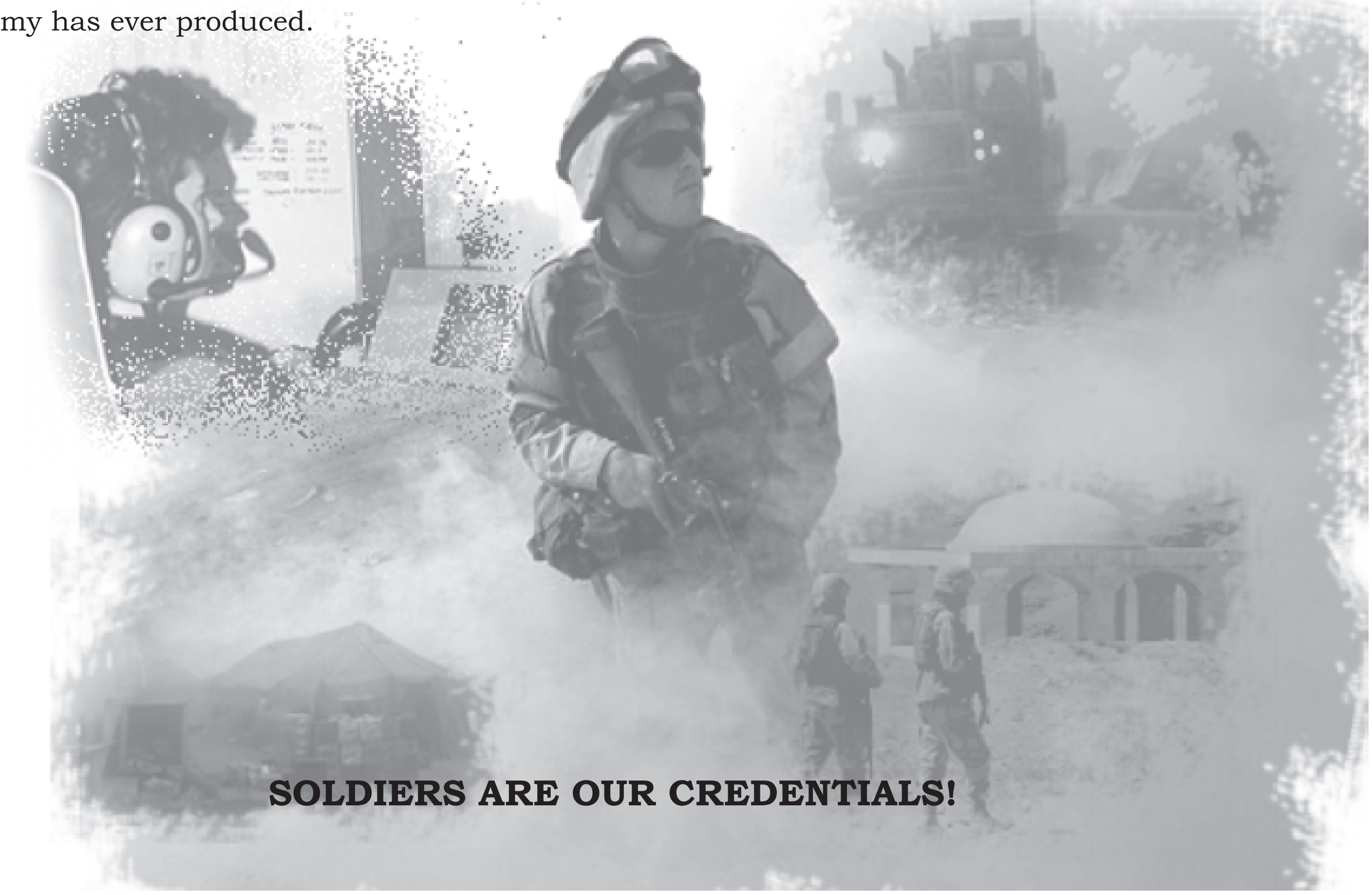
✦ Delta Company trains SIGINT Analysts to perform a highly technical world-wide, Joint analysis mission. Following the battalion's emphasis, the company currently conducts a week-end long FTX which is a culminating event used to evaluate each Soldier's level of tactical proficiency. Technical training for Soldiers has focused on increasing awareness as how Signals Analysts can best support the warfighter conducting real-world operations.

The 344th MI Battalion is committed to producing the best SIGINT and Firefighting Soldiers in the world. While integrating recent veterans' experiences into the training we conduct here, we ask that units currently engaged provide us feedback so we can address them immediately. We have established a web page on NSA Net for that purpose. http://www.gdflw.f.nsa/344th_MI_BN/. Units can provide immediate feedback, TTPs, and material so that we may continually improve the training.

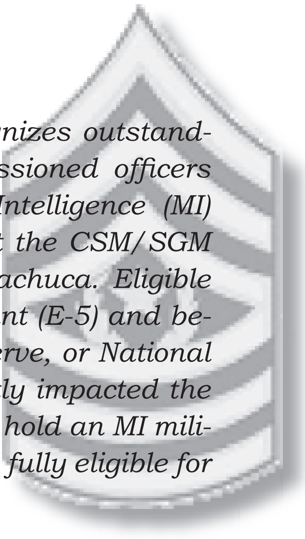
11/100th MI Battalion

The 11/100th MI Battalion is a mobilized reserve battalion composed of a total volunteer staff and cadre from ten separate Army Reserve and National Guard units. The 11/100th was originally mobilized to Fort Huachuca in January 2004 as the 2/84th MI Battalion. Since their initial deployment the unit has graduated over 700 MI professionals in MOSs 97B10, 97E10, and MI NCOES courses. The 11/100th currently teaches a 10 week 97E10 course versus. the active component 18 week 97E10 course. The 11/100th was selected to re-write and transition to the 10 week course, which will eventually be utilized by all of the Army Reserve and National Guard MI schools.

As you can see we are doing a lot of things to ensure you are getting the best trained MI Warriors the Army has ever produced.



CSM Doug Russell Award 2007



The CSM Doug Russell Award recognizes outstanding achievement by junior noncommissioned officers within or on behalf of the Military Intelligence (MI) community. It is awarded annually at the CSM/SGM Conference held in March at Fort Huachuca. Eligible Soldiers must be in the rank of Sergeant (E-5) and below; be in the Active Army, Army Reserve, or National Guard, and whose actions have directly impacted the MI Corps. The Soldier does not need to hold an MI military occupational specialty but must be fully eligible for re-enlistment.

Corporal Steven Heigh distinguished himself through meritorious conduct and outstanding service to the U.S. Army and the Military Intelligence (MI) Corps as the team leader of Human Intelligence (HUMINT) Team (HCT) 630, C Company, 163rd MI Battalion during Operation Iraqi Freedom VI. Corporal Heigh's display his leadership potential early on when he was selected to fill this position, normally held by a staff sergeant or above, just days before moving from Kuwait into Iraq. Corporal Heigh took immediate charge and moved with his team to Forward Operating Base (FOB) Caldwell. His team provided direct support to the 5/73 Cavalry Squadron, 82nd Airborne Division at this remote FOB near the Iranian border. As a Corps level HCT, he and his team had never before worked with their supported unit and the HCT he inherited was unfocused and mismanaged. Despite this, Corporal Heigh quickly integrated him team into the squadron's operations and built a diverse and effective HUMINT source network from nothing.

In just the first three months of the deployment, Corporal Heigh and his three-man team used their HUMINT source operations to produce 65 draft Intelligence Information Reports to meet the squadron's requirements. The previous team produced just 89 reports during the year prior to Corporal Heigh's arrival at Caldwell. Corporal Heigh fiercely targeted insurgent networks engaged in anti-coalition activities. His reporting led to multiple combat operations that detained a prolific Tawhid Wa Al Jihad financier; identified and neutralized a Sunni insurgent training camp, and seized six substantial weapon caches containing more that 500,000 small arms rounds, 50 mortar rounds, an 82 mm recoilless rifle, grenades, and artillery rounds. Additionally, Corporal Heigh and his team produced intelligence that led to the seizure of a vehicle containing a large quantity of improvised explosive device (IED) making materials. Corporal Heigh's collection and dissemination of accurate, actionable information enabling the squadron to take a proactive stance toward combating insurgent networks in their area and greatly contributed to the change from a reactive posture to offensive operations.

Corporal Heigh's many accomplishments are all the more notable in that his area of operations encompassed all of eastern Diyala Province and was non-permissive to HUMINT collection operations. One hun-

(Continued on page 19)

Twenty-Eight Articles:

Fundamentals of Company-level Counterinsurgency

by David Kilcullen, PhD

The views expressed in this article are those of the author and do not reflect the official policy or position of any department or agency of the U.S. Government or any other government.

This paper was first formally published in *Military Review* Insights (May June 2006), accessible at http://usacac.leavenworth.army.mil/CAC/milreview/English/MayJun06/webpdf/BoB.

Introduction

Your company has just been warned for deployment for counterinsurgency operations in Iraq or Afghanistan. You have read David Galula, T.E. Lawrence and Robert Thompson. You have studied **FM 3-24, Counterinsurgency Operations**, and now understand the history, philosophy, and theory of counterinsurgency.[1] You have watched *Black Hawk Down* and *The Battle of Algiers*, and you know this will be the most difficult challenge of your life.[2]

But what does all the theory mean, at the company level? How do the principles translate into action at night, with the global positioning system (GPS) down, the media criticizing you, the locals complaining in a language you don't understand, and an unseen enemy killing your people by ones and twos? How does counterinsurgency actually happen?

There are no universal answers, and insurgents are among the most adaptive opponents you will ever face. Countering them will demand every ounce of your intellect. But be comforted: You are not the first to feel this way. There are tactical fundamentals you can apply to link the theory with the techniques and procedures you already know.

What is Counterinsurgency?

If you have not studied counterinsurgency theory, here it is in a nutshell: *Counterinsurgency is a competition with the insurgent for the right and the ability to win the hearts, minds, and acquiescence of the population. You are being sent in because the insurgents, at their strongest, can defeat anything with less strength than you. But you have more combat power than you can or should use in most situations. Injudicious use of firepower creates blood feuds, homeless people and societal disruption that fuels and perpetuates the insurgency. The most beneficial actions are often local politics, civic action, and beat-cop behaviors. For your side to win, the people don't have to like you but they must respect you, accept that your actions benefit them, and trust your integrity and ability to deliver on promises, particularly regarding their security. In this battlefield popular perceptions and rumor are more influential than the facts and more powerful than a hundred tanks.*

Within this context, what follows are observations from collective experience, the distilled essence of what those who went before you learned. They are expressed as commandments, for clarity, but are really more like folklore. Apply them judiciously and skeptically.

Preparation

Time is short during pre-deployment, but you will never have more time to think than you have now. Now is your chance to prepare yourself and your command.

1. Know your turf. Know the people, the topography, economy, history, religion, and culture. Know every village, road, field, population group, tribal leader, and ancient grievance. Your task is to become the world expert on your district. If you don't know precisely where you will be operating, study the general area. Read the map like a book, study it every night before sleep and re-draw it from memory every morning until you understand its patterns intuitively. Develop a mental model of your area, a framework in which to fit every new piece of knowledge you acquire. Study handover notes from predecessors; better still, get in touch with the unit in theater and pick their leaders' brains. In an ideal world, intelligence officers and area experts would brief you; however this rarely happens, and even if it does, there is no substitute for personal mastery. Understand the broader area of influence which can be a wide area, particularly when insurgents draw on global grievances. Share out aspects of the operational area among platoon leaders and non-commissioned officers (NCOs), have each individual develop a personal specialization and brief the others. Neglect this knowledge, and it will kill you.

2. Diagnose the problem. Once you know your area and its people, you can begin to diagnose the problem. Who are the insurgents? What drives them? What makes local leaders tick? Counterinsurgency is fundamentally a competition between each side to mobilize the population in support of their agenda. So you must understand what motivates the people and how to mobilize them. You need to know why and how the insurgents are getting followers. This means you need to know your real enemy, not a cardboard cut-out. The enemy is adaptive, resourceful and probably grew up in the region where you will be operating. The locals have known him since he was a boy. How long have they known you? Your worst opponent is not the psychopathic terrorist of Hollywood, it is the charismatic follow-me warrior who would make your best platoon leader. His followers are not misled or naive, much of his success may be due to bad government policies or security forces that alienate the population. Work this problem collectively with your platoon and squad leaders. Discuss ideas, explore the problem, understand what you are facing, and seek a consensus. If this sounds unmilitary, get over it. Once you are in theater, situations will arise too quickly for orders or even commander's intent. Corporals and privates will have to make snap judgments with strategic impact. The only way to help them is to give them a shared understanding, then trust them to think for themselves on the day.

3. Organize for intelligence. In counterinsurgency, killing the enemy is easy. Finding him is often nearly impossible. Intelligence and operations are complementary. Your operations will be intelligence driven, but intelligence will come mostly from your own operations, not as a product prepared and served up by higher headquarters. So you must organize for intelligence. You will need a company S2 and intelligence section (including analysts.) You may need platoon S2s and S3s, and you will need a reconnaissance and surveillance (R&S) element. You will not have enough linguists, you never do, but carefully consider where best to employ them. Linguists are a battle-winning asset, but like any other scarce resource you must have a prioritized "bump plan" in case you lose them. Often during predeployment the best use of linguists is to train your command in basic language. You will probably not get augmentation for all this, but you must still do it. Put the smartest soldiers in the S2 section and the R&S squad. You will have one less rifle squad, but the intelligence section will pay for itself in lives and effort saved.

4. Organize for inter-agency operations. Almost everything in counterinsurgency is interagency. And everything important, from policing to intelligence to civil-military operations to trash collection, will involve your company working with civilian actors and local indigenous partners you cannot control, but whose success is essential for yours. Train the company in inter-agency operations, get a briefing from the State Department, aid agencies, and the local police or fire brigade. Train point-men in each squad to deal with the interagency. Realize that civilians find rifles, helmets, and body armor intimidating. Learn how not to scare them. Ask others who come from that country or culture about your ideas. See it through the eyes of a civilian who knows nothing about the military. How would you react if foreigners came to your neighborhood and conducted the operations you planned? What if somebody came to your mother's house and did that? Most importantly, know that your operations will create temporary breathing space, but long-term development and stabilization by civilian agencies will ultimately win the war.

5. Travel light and harden your combat service support (CSS). You will be weighed down with body armor, rations, extra ammunition, communications gear, and a thousand other things. The enemy will carry a rifle or rocket-propelled grenade, a *shemagh (head scarf)* and a water bottle if he is lucky. Unless you ruthlessly lighten your load and enforce a culture of speed and mobility, the insurgents will consistently out-run and out-maneuver you. But in lightening your load, make sure you can always reach back to call for firepower or heavy support if needed. Also, remember to harden your CSS. The enemy will attack your weakest points. Most attacks on Coalition forces in Iraq in 2004 and 2005, outside preplanned combat actions like the two battles of Fallujah or Operation Iron Horse, were against CSS installations and convoys. You do the math. Ensure your CSS assets are hardened, have communications, and are trained in combat operations. They may do more fighting than your rifle squads.

6. Find a political/cultural adviser. In a force optimized for counterinsurgency, you might receive a political/cultural adviser at company level–a diplomat or military foreign area officer able to speak the language and navigate the intricacies of local politics. Back on planet Earth, the corps and division commander will get a political/cultural adviser (POLAD); you will not, so you must improvise. Find a POLAD from among your people, perhaps an officer, perhaps not (see Article 8). Someone with people skills and a feel for the environment will do better than a political science graduate. Don't try to be your own cultural adviser, you must be fully aware of the political and cultural dimension, but this is a different task. Also, don't give one of your intelligence people this role. They can help, but their task is to understand the environment; the POLAD's job is to help shape it.

7. Train the squad leaders; then trust them. Counterinsurgency is a squad and platoon leader's war, and often a private's war. Battles are won or lost in moments. Whoever can bring combat power to bear in seconds, on a street corner, will win. The commander on the spot controls the fight. You must train the squad leaders to act intelligently and independently without orders. If your squad leaders are competent, you can get away with average company or platoon staffs. The reverse is not the case. Training should focus on basic skills: marksmanship, patrolling, security on the move and at the halt, and basic drills. When in doubt, spend less time on company and platoon training, and more time on squads. Ruthlessly replace leaders who do not make the grade. But once people are trained, and you have a shared operational diagnosis, you must trust them. We talk about this, but few company or platoon leaders really trust their people. In counterinsurgency, you have no choice.

8. Rank is nothing; talent is everything. Not everyone is good at counterinsurgency. Many people don't understand the concept, and some can't execute it. It is difficult, and in a conventional force only a few people will master it. Anyone can learn the basics, but a few naturals do exist. Learn how to spot these people and put them into positions where they can make a difference. Rank matters far less than talent, a few good men under a smart junior NCO can succeed in counterinsurgency, where hundreds of well-armed soldiers under a mediocre senior officer will fail.

9. Have a game plan. The final preparation task is to develop a game plan, a mental picture of how you see the operation developing. You will be tempted to try and do this too early. But wait, as your knowledge improves, you will get a better idea of what needs to be done and a fuller understanding of your own limitations. Like any plan, this plan will change once you hit the ground and may need to be scrapped if there is a major shift in the environment. But you still need a plan, and the process of planning will give you a simple robust idea of what to achieve, even if the methods change. This is sometimes called "operational design." One approach is to identify basic stages in your operation, for example, "establish dominance, build local networks, marginalize the enemy." Make sure you can easily transition between phases, both forward and backward in case of setbacks. Just as the insurgent can adapt his activity to yours, you must have a simple enough plan to survive setbacks without collapsing. This plan is the solution that matches the shared diagnosis you developed earlier. It must be simple, and known to everyone.

The Golden Hour

You have deployed, completed reception and staging, and (if you are lucky) attended the in-country counterinsurgency school. Now it is time to enter your sector and start your tour. This is the golden hour. Mistakes made now will haunt you for the rest of the tour, while early successes will set the tone for victory. You will look back on your early actions and cringe at your clumsiness. So be it. But you must act.

10. Be there. The most fundamental rule of deployment in counterinsurgency is to be there. You can almost never outrun the enemy. If you are not present when an incident happens, there is usually little you can do about it. So your first order of business is to establish presence. If you can't do this throughout your sector, then do it wherever you can. This demands a residential approach, living in your sector, in close proximity to the population, rather than raiding into the area from remote, secure bases. Movement on foot, sleeping in local villages, night patrolling—all these seem more dangerous than they are. They establish links with the locals, who see you as real people they can trust and do business with, not as aliens who descend from an armored box. Driving around in an armored convoy, day-tripping like a tourist in hell, degrades situational awareness, makes you a target and is ultimately more dangerous.

11. Avoid knee jerk responses to first impressions. Don't act rashly; get the facts first. The violence you see may be part of the insurgent strategy, it may be various interest groups fighting it out, or it may be people settling personal vendettas. Normality in Kandahar is not the same as in Seattle, you need time to learn what normality looks like. The insurgent commander wants to goad you into lashing out at the population or making a mistake. Unless you happen to be on the spot when an incident occurs, you will have only second-hand reports and may misunderstand the local context or interpretation. This fragmentation and "disaggregation" of the battlefield, particularly in urban areas, means that first impressions are often highly misleading. Of course, you can't avoid making judgments. But if possible, check them with an older hand or a trusted local. If you can, keep one or two officers from your predecessor unit for the first part of the tour. Try to avoid a rush to judgment.

12. Prepare for handover from Day One. Believe it or not, you will not resolve the insurgency on your watch. Your tour will end, and your successors will need your corporate knowledge. Start handover folders, in every platoon and specialist squad, from day one. Ideally, you would have inherited these from your predecessors, but if not you must start them. The folders should include **lessons learned**, details about the population, village and patrol reports, updated maps, photographs—anything that will help newcomers master the environment. Computerized databases are fine, but keep good back-ups and ensure you have hard copy of key artifacts and documents. This is boring, tedious, but essential. Over time, you will create a corporate memory that keeps your people alive.

13. Build trusted networks. Once you have settled into your sector, your key task is to build trusted networks. This is the true meaning of the phrase "hearts and minds", which comprises two separate components. "Hearts" means persuading people their best interests are served by your success; "minds" means convincing them that you can protect them, and that resisting you is pointless. Note that neither concept has to do with whether people like you. Calculated self-interest, not emotion, is what counts. Over time, if you successfully build networks of trust, these will grow like roots into the population, displacing the enemy's networks, bringing him out into the open to fight you, and letting you seize the initiative. These networks include local allies, community leaders, local security forces, nongovernmental agencies (NGOs) and other friendly or neutral non-state actors in your area, and the media. Conduct village and neighborhood surveys to identify needs in the community, then follow through to meet them. Build common interests and mobilize popular support. This is your true main effort; everything else is secondary. Actions that help build trusted networks serve your cause. Actions—even killing high-profile targets that undermine trust or disrupt your networks—help the enemy.

14. Start easy. If you were trained in maneuver warfare you know about surfaces and gaps. This applies to counterinsurgency as much as any other form of maneuver. Don't try to crack the hardest nut first, don't go straight for the main insurgent stronghold; try to provoke a decisive showdown, or focus efforts on villages that support the insurgents. Instead, start from secure areas and work gradually outwards. Do this by extending your influence through the locals' own networks. Go with, not against, the grain of local society. First win the confidence of a few villages and then see who they trade, intermarry, or do business with. Now win these people over. Soon enough the showdown with the insurgents will come. But now you have local allies, a mobilized population and a trusted network at your back. Do it the other way round and no one will mourn your failure.

15. Seek early victories. In this early phase, your aim is to stamp your dominance in your sector. Do this by seeking an early victory. This will probably not translate into a combat victory over the enemy. Looking for such a victory can be overly aggressive and create collateral damage—especially since you really do not yet understand your sector. Also, such a combat victory depends on the enemy being stupid enough to present you with a clear-cut target, a rare windfall in counterinsurgency. Instead, you may achieve a victory by resolving long-standing issues your predecessors have failed to address, or co-opting a key local leader who has resisted cooperation with our forces. Like any other form of armed propaganda, achieving even a small victory early in the tour sets the tone for what comes later and helps seize the initiative, which you have probably lost due to the inevitable hiatus entailed by the handover-takeover with your predecessor.

16. Practise deterrent patrolling. Establish patrolling methods that deter the enemy from attacking you. Often our patrolling approach seems designed to provoke, then defeat, enemy attacks. This is counter-productive, it leads to a raiding, day-tripping mindset or, worse, a bunker mentality. Instead, practise deterrent patrolling. There are many methods for this, including multiple patrolling in which you flood an area with numerous small patrols working together. Each is too small to be a worthwhile target, and the insurgents never know where all the patrols are, making an attack on any one patrol extremely risky. Other methods include so-called blue-green patrolling, where you mount daylight overt humanitarian patrols, which go covert at night and hunt specific targets. Again, the aim is to keep the enemy off balance and the population reassured through constant and unpredictable activity which, over time, deters attacks and creates a more permissive environment. A reasonable rule of thumb is that one- to two-thirds of your force should be on patrol at any time, day or night.

17. Be prepared for setbacks. Setbacks are normal in counterinsurgency, as in every other form of war. You will make mistakes, lose people, or occasionally kill or detain the wrong person. You may fail in building or expanding networks. If this happens, don't lose heart, simply drop back to the previous phase of your game plan and recover your balance. It is normal in company counterinsurgency operations for some platoons to be doing well, while others do badly. This is not necessarily evidence of failure. Give local commanders the freedom to adjust their posture to local conditions. This creates elasticity that helps you survive setbacks.

18. Remember the global audience. One of the biggest differences between the counterinsurgencies our fathers fought and those we face today is the omnipresence of globalized media. Most houses in Iraq have one or more satellite dishes. Web bloggers; print, radio and television reporters and others are monitoring and reporting your every move. When the insurgents ambush your patrols or set off a car bomb, they do so not to destroy one more track, but because they want graphic images of a burning vehicle and dead bodies for the evening news. Beware of the scripted enemy, who plays to a global audience and seeks to defeat you in the court of global public opinion. You counter this by training people to always bear in mind the global audience, to assume that everything they say or do will be publicized, and befriend the media. Get the press onside, help them get their story and trade information with them. Good relationships with non-embedded media, especially indigenous media, dramatically increase your situational awareness and help get your message across to the global and local audience.

19. Engage the women, beware of the children. Most insurgent fighters are men. But in traditional societies, women are hugely influential in forming the social networks that insurgents use for support. Co-opting neutral or friendly women, through targeted social and economic programs, builds networks of enlightened self-interest that eventually undermine the insurgents. You need your own female counterinsurgents, including interagency people, to do this effectively. Win the women, and you own the family unit. Own the family, and you take a big step forward in mobilizing the population. Conversely, though, stop your people fraternizing with local children. Your troops are homesick; they want to drop their guard with the kids. But children are sharp-eyed, lacking in empathy, and willing to commit atrocities their elders would shrink from. The insurgents are watching, they will notice a growing friendship between one of your people and a local child, and either harm the child as punishment, or use them against you. Similarly, stop people throwing candies or presents to children. It attracts them to our vehicles, creates crowds the enemy can exploit, and leads to children being run over. Harden your heart and keep the children at arm's length.

20. Take stock regularly. You probably already know that a body count tells you little, because you usually can't know how many insurgents there were to start with, how many moved into the area, how many transferred from supporter to combatant status, or how many new fighters the conflict has created. But you still need to develop metrics early in the tour and refine them as the operation progresses. They should cover a range of social, informational, military and economic issues. Use metrics intelligently to form an overall impression of progress, not in a mechanistic traffic-light fashion. Typical metrics include: percentage of engagements initiated by our forces versus those initiated by insurgents; longevity of friendly local leaders in positions of authority; number and quality of tip-offs on insurgent activity that originate spontaneously from the population; and economic activity at markets and shops. These mean virtually nothing as a snapshot; it is trends over time that are the true indicators of progress in your sector.

Groundhog Day

Now you are in "steady state." You are established in your sector and people are settling into that "groundhog day" mentality that hits every unit at some stage during every tour. It will probably take you at least the first third of the tour to become effective in the environment, if not longer. Then in the last period you will struggle against the short-timer mentality. So this middle part of the tour is the most productive—but keeping the flame alive, and bringing the local population along with you, takes immense leadership.

21. Exploit a "single narrative". Since counterinsurgency is a competition to mobilize popular support, it pays to know how people are mobilized. In most societies there are opinion-makers: local leaders, pillars of the community, religious figures, media personalities, and others who set trends and influence public perceptions. This influence, including the pernicious influence of the insurgents, often takes the form of a "single narrative", a simple, unifying, easily expressed story or explanation that organizes people's experience and provides a framework for understanding events. Nationalist and ethnic historical myths, or sectarian creeds, provide such a narrative. The Iraqi insurgents have one, as do al-Qaeda and the Taliban. To undercut their influence you must exploit an alternative narrative, or better yet, tap into an existing narrative that excludes the insurgents. This narrative is often worked out for you by higher headquarters, but only you have the detailed knowledge to tailor the narrative to local conditions and generate leverage from it. For example, you might use a nationalist narrative to marginalize foreign fighters in your area, or a narrative of national redemption to undermine former regime elements that have been terrorizing the population. At the company level, you do this in baby steps by getting to know local opinion-makers, winning their trust, learning what motivates them, and building on this to find a single narrative that emphasizes the inevitability and rightness of your ultimate success. This is art, not science.

22. Local forces should mirror the enemy, not the Americans. By this stage, you will be working closely with local forces, training or supporting them, and building indigenous capability. The natural tendency is to build forces in the U.S. image, with the aim of eventually handing our role over to them. This is a mistake. Instead, local indigenous forces need to mirror the enemy's capabilities, and seek to supplant the insurgent's role. This does not mean they should be irregular in the sense of being brutal or outside proper control. Rather, they should move, equip, and organize like the insurgents, but have access to your support and be under the firm control of their parent societies. Combined with a mobilized population and trusted networks, this allows local forces to hard-wire the enemy out of the environment, under top-cover from you. At the company level, this means that raising, training, and employing local indigenous auxiliary forces (police and military) are valid tasks. This requires high-level clearance, of course, but if support is given, you should establish a company training cell. Platoons should aim to train one local squad, then use that squad as a nucleus for a partner platoon. Company headquarters should train an indigenous leadership team. This mirrors the growth process of other trusted networks, and tends to emerge naturally as you win local allies who want to take up arms in their own defense.

23. Practise armed civil affairs. Counterinsurgency is armed social work, an attempt to redress basic social and political problems while being shot at. This makes civil affairs a central counterinsurgency activity, not an afterthought. It is how you restructure the environment to displace the enemy from it. In your company sector, civil affairs must focus on meeting basic needs first, then progress up Maslow's hierarchy as each successive need is met. You need intimate cooperation with inter-agency partners here—national, international and local. You will not be able to control these partners, many NGOs, for example, do not want to be too closely associated with you because they need to preserve their perceived neutrality. Instead, you need to work on a shared diagnosis of the problem, building a consensus that helps you self-synchronize. Your role is to provide protection, identify needs, facilitate civil affairs and use improvements in social conditions as leverage to build networks and mobilize the population. Thus, there is no such thing as impartial humanitarian assistance or civil affairs in counterinsurgency. Every time you help someone, you hurt someone else—not least the insurgents—so civil and humanitarian assistance personnel will be targeted. Protecting them is a matter not only of close-in defense, but also of creating a permissive operating environment by co-opting the beneficiaries of aid (local communities and leaders) to help you help them.

24. Small is beautiful. Another natural tendency is to go for large-scale, mass programs. In particular, we have a tendency to template ideas that succeed in one area and transplant them into another, and we tend to take small programs that work and try to replicate them on a larger scale. Again, this is usually a mistake; often programs succeed because of specific local conditions of which we are unaware, or because their very smallness kept them below the enemy's radar and helped them flourish unmolested. At the company level, programs that succeed in one district often also succeed in another (because the overall company sector is small), but small-scale projects rarely proceed smoothly into large programs. Keep programs small; this makes them cheap, sustainable, low-key and (importantly) recoverable if they fail. You can add new programs—also small, cheap and tailored to local conditions—as the situation allows.

25. Fight the enemy's strategy, not his forces. At this stage, if things are proceeding well, the insurgents will go over to the offensive. Yes, the *offensive*, because you have created a situation so dangerous to the insurgents, (by threatening to displace them from the environment) that they have to attack you and the population to get back into the game. Thus it is normal, even in the most successful operations, to have spikes of offensive insurgent activity late in the campaign. This does not necessarily mean you have done something wrong (though it may, it depends on whether you have successfully mobilized the population). At this point the tendency is to go for the jugular and seek to destroy the enemy's forces in open battle. This is rarely the best choice at company level, because provoking major combat usually plays into the enemy's hands by undermining the population's confidence. Instead, attack the enemy's strategy. If he is seeking to recapture the allegiance of a segment of the local population, then co-opt them against him. If he is trying to provoke a sectarian conflict, go over to peace enforcement mode. The permutations are endless but the principle is the same, fight the enemy's strategy, not his forces.

26. Build your own solution; only attack the enemy when he gets in the way. Try not to be distracted or forced into a series of reactive moves by a desire to kill or capture the insurgents. Your aim should be to implement your own solution, the game plan you developed early in the campaign and then refined through interaction with local partners. Your approach must be environment-centric (based on dominating the whole district and implementing a solution to its systemic problems) rather than enemy-centric. This means that, particularly late in the campaign you may need to learn to negotiate with the enemy. Members of the population that supports you also know the enemy's leaders. They may have grown up together in the small district that is now your company sector, and valid negotiating partners sometimes emerge as the campaign progresses. Again, you need close interagency relationships to exploit opportunities to co-opt segments of the enemy. This helps you wind down the insurgency without alienating potential local allies who have relatives or friends in the insurgent movement. At this stage, a defection is better than a surrender, a surrender is better than a capture, and a capture is better than a kill.

Getting Short

Time is short, and the tour is drawing to a close. The key problem now is keeping your people focused, maintaining the rage on all the multifarious programs, projects, and operations that you have started and preventing your people from dropping their guard. In this final phase, the previous articles still stand, but there is an important new one.

27. Keep your extraction plan secret. The temptation to talk about home becomes almost unbearable toward the end of a tour. The locals know you are leaving, and probably have a better idea than you of the generic extraction plan. Remember, they have seen units come and go. But you must protect the specific details of the extraction plan, or the enemy will use this as an opportunity to score a high-profile hit, recapture the population's allegiance by scare tactics that convince them they will not be protected once you leave, or persuade them that your successor unit will be oppressive or incompetent. Keep the details secret within a tightly controlled compartment in your headquarters.

Four "What Ifs".

The articles above describe what should happen, but we all know that things go wrong. Here are some "what ifs" to consider:

What if you get moved to a different area? You prepared for ar-Ramadi and studied Dulaim tribal structures and Sunni beliefs. Now you are going to Najaf and will be surrounded by al-Hassan tribes and Shi'a communities. But that work was not wasted. In mastering your first area, you learned techniques you can apply—how to "case" an operational area and how to decide what matters in the local societal structure. Do the same again, and this time the process is easier and faster since you have an existing mental structure and can focus on what is different. The same applies if you get moved frequently within a battalion or brigade area.

What if higher headquarters doesn't "get" counterinsurgency? Higher headquarters is telling you the mission is to "kill terrorists" or pushing for high-speed armored patrols and a base-camp mentality. They just do not seem to understand counterinsurgency. This is not uncommon, since company-grade officers today often have more combat experience than senior officers. In this case, just do what you can. Try not to create expectations that higher headquarters will not let you meet. Apply the adage "first do no harm." Over time, you will find ways to do what you have to do. But never lie to higher headquarters about your locations or activities, they own the indirect fires.

What if you have no resources? You have no linguists, the aid agencies have no money for projects in your area and you have a low priority for civil affairs. You can still get things done, but you need to focus on self-reliance. Keep things small and sustainable and ruthlessly prioritize effort. The local population is your ally in this. They know what matters to them more than you do. Be honest with them, discuss possible projects and options with community leaders, get them to choose what their priority is. Often they will find the translators, building supplies, or expertise that you need, and will only expect your support and protection in making their projects work. And the process of negotiation and consultation will help mobilize their support and strengthen their social cohesion. If you set your sights on what is achievable, the situation can still work.

What if the theater situation shifts under your feet? It is your worst nightmare—everything has gone well in your sector, but the whole theater situation has changed and invalidates your efforts. Think of the first battle of Fallujah, the al-Askariya shrine bombing, or the Sadr uprising. What do you do? Here is where having a flexible, adaptive game plan comes in. Just as the insurgents drop down to a lower posture when things go wrong, now is the time to drop back a stage, consolidate, regain your balance, and prepare to expand again when the situation allows. But see Article 28—if you cede the initiative, you must regain it as soon as the situation allows, or you will eventually lose.

Conclusion

This, then, is the tribal wisdom, the folklore which those who went before you have learned. Like any folklore it needs interpretation and contains seemingly contradictory advice. Over time, as you apply unremitting intellectual effort to study your sector, you will learn to apply these ideas in your own way, and will add to this store of wisdom from your own observations and experience. So only one article remains; and if you remember nothing else, remember this:

28. Whatever else you do, keep the initiative. In counterinsurgency, the initiative is everything. If the enemy is reacting to you, you control the environment. Provided you mobilize the population, you will win. If you are reacting to the enemy, even if you are killing or capturing him in large numbers, then he is controlling the environment and you will eventually lose. In counterinsurgency, the enemy initiates most attacks, targets you unexpectedly, and withdraws too fast for you to react. Do not be drawn into purely reactive operations; focus on the population, build your own solution, further your game plan, and fight the enemy only when he gets in the way. This gains and keeps the initiative.

Endnotes

[1] **Field Manual 3-24, Counterinsurgency Operations** (Washington, D.C.: U.S. Government Printing Office, 2006).

[2] *Black Hawk Down* (Los Angeles, California: Scott Free Productions, 2002); *The Battle of Algiers* (Casbah Film and Igor Film, 1967).

David Kilcullen, PhD, served 21 years in the Australian Army. He commanded an infantry company during counterinsurgency operations in East Timor, taught counterinsurgency tactics as an exchange instructor at the British School of Infantry, and served as a military advisor to Indonesia Special Forces. He has worked in several Middle Eastern countries with regular and irregular police and military forces since 9/11, and was a special advisor for irregular warfare during the 2005 U.S. Quadrennial Defense Review. He is currently seconded to the U.S. State Department as Chief Strategist in the office of the Coordinator for Counterterrorism and remains a Reserve Lieutenant Colonel in the Australian Army. His doctoral dissertation is a study of Indonesian insurgent and terrorist groups and counterinsurgency methods.

CSM Doug Russell Award 2007

(Continued from page 10)

dred percent of HCT 630's collection was obtained from sources Corporal Heigh spotted and assessed during 40 combat patrols covering nearly 2,000 miles over three months. During that time, the team was engaged four times with IEDs and sustained small arms fire. Corporal Heigh and all the members of his team earned the Combat Action Badge.

Although only a private first class when the 163rd MI Battalion was reactivated in January 2006 and with no assigned noncommissioned officer, Corporal Heigh recognized his own need for development in preparation for deployment. He aggressively sought resources and tirelessly studied available HUMINT and tactical skills publications. He used much of his personal time to maintain a 3/3 score on the Persian Farsi Defense Language Proficiency Test. These qualities and skills proved instrumental in his ability to effectively train his HCT, and plan and conduct the HUMINT collection mission.

Corporal Heigh's supported squadron and brigade commanders commented on a regular basis as to how greatly they valued his professionalism and focus on intelligence collection that drove their operations. The 5/73 Cavalry Squadron recognized Corporal Heigh and his contributions by awarding him combat spurs and the 82nd Airborne Division combat patch. Finally, HCT 630 provided reporting and tactical HUMINT support that drove a major squadron operation that resulted in approximately 60 insurgent KIA and was featured in the 21 November 2006 Mideast edition of the *Stars and Stripes*. This recognition of Corporal Heigh's achievements strongly emphasizes the relevance of HUMINT collection in the Global War on Terrorism.

Additional COIN Notes

by Jeffrey T. Strohman

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.

One of the hardest challenges the U.S. Army faces is finding the proper balance between improving its ability to defeat an insurgency and maintaining the ability to fight a conventional war. Insurgencies and conventional combat differ so fundamentally that many of the things that help to ensure success in one can be liabilities in the other.

In particular, the ability to mass fires at a particular point in time and space on the battlefield—the essence of conventional combat—is extremely unhelpful if misapplied in a counterinsurgency. *Success in counterinsurgency instead demands the precise application of force after dedicated and exacting intelligence work*—not the core competencies of conventional armies.

U.S. enemies have learned that *asymmetric conflicts* offer them the best chance of success; so counter that.

The Army's historical experience with counterinsurgency is marked by cases of success and failure. Although the Army overcame an insurgency in the Philippines at the turn of the twentieth century, it was less successful in Vietnam. Unprepared for the demands of counterinsurgency at the beginning of the Vietnam conflict, the Army was slow in adapting during the course of the conflict.

One result of America's defeat in Vietnam was a decision by the Army to avoid counterinsurgency campaigns in the future. The U.S. would prepare for conventional wars and swiftly depart after defeating its enemies in major combat operations. Unfortunately, the enemy has a vote, and our adversaries worldwide learned from Desert Storm that fighting the U.S. conventionally is a recipe for self-destruction. However, successful attacks in Lebanon, Somalia, Saudi Arabia, and the Gulf of Aden demonstrated that fighting the U.S. asymmetrically offers a much better chance for success. The endurance of the insurgencies in Afghanistan and Iraq has underlined the truth of this lesson for those who wish to do us harm to further their objectives. Insurgencies are the types of conflict we are most likely to face for the foreseeable future, and therefore we must learn how to defeat enemies who practice this kind of war.

The relative paucity of strategic thinking about counterinsurgency since Vietnam doubtless contributed to our difficulty in grasping the emergence of the insurgency in Iraq. The absence of recent counterinsurgency doctrine and training in the Army and Marine Corps prior to Operation Iraqi Freedom has similarly contributed to the uneven application of counterinsurgency principles at the tactical and operational levels there.

At the small-unit level, where counterinsurgency is conducted on a daily basis, some units in Iraq have demonstrated a remarkable ability to adopt effective counterinsurgency techniques. Others have too often persisted in an over reliance on military force, despite the fact that such techniques are generally unproductive in developing the intelligence from the local population that is the basis of success in counterinsurgency.

Counterinsurgency is a long and slow process requiring all elements of national power.

Defeating an insurgency is not primarily a military task. David Galula, the French counterinsurgency expert, estimated the task was eighty percent political and twenty percent military. Counterinsurgency is a long, slow process that requires the integration of all elements of national power—military, diplomatic, economic, financial, intelligence, and informational—to accomplish the tasks of creating and supporting legitimate host governments that can then defeat the insurgency that afflicts them.

Insurgencies are rarely defeated militarily; some degree of political accommodation is essential in convincing all but the most committed insurgents that politics rather than force is a viable way to pursue their objectives. Historically, successful counterinsurgents have defeated their opponents by peeling off the less ideologically committed sub-elements with promises of political progress toward their ultimate goals.

In the case of the Sunni minority in Iraq, political outreach would provide promises of a greater degree of political power than the Sunnis have believed would be granted to a minority population in such an immature democracy. The recent acceptance by Iraq's Shiite and Kurdish populations that to end the fighting they will have to yield some political power to their Sunni brethren is a large step toward ultimate stability in Iraq.

Insurgents have "filled the media and internet vacuum" left by the U.S.

Insurgency is ultimately a war of ideas. An insurgency grows based on its ability to convince fighters to risk their lives against a conventionally superior opponent and survives in the face of a stronger enemy only because it is able to convince or coerce the people to provide it with what it needs to fight: weapons, ammunition, food, money, and most important concealment and cover among the civilian population. Recognizing this fact, successful counterinsurgents have devoted as much effort to defeating the enemy's propaganda as they have to defeating his fighters. Winning the war of ideas has often been the decisive line of operations in successful counterinsurgency campaigns.

The U.S. has not done an adequate job of explaining to the American people, to its allies overseas and, most important, to the people of Iraq and the broader Islamic world what we are fighting for in Iraq and what we hope to achieve there. Nature abhors a vacuum, and insurgents love one; they have filled the airwaves and the Internet with their versions of the truth and have found willing listeners worldwide. In the words of the former Secretary of Defense, "Our enemies have skillfully adapted to fighting wars in today's media age, but for the most part we, our country, our government, have not."

A dedicated corps of Public Affairs professionals funded and equipped to speak to Muslims in their own languages could over time help win the war of ideas by providing vital support to moderate Muslims. Truth is the best weapon to use and over time, the American people and the Arab Nations will appreciate that fact.

Intelligence collection/analysis is the key to capturing or killing insurgents.

The prime requirement for a successful counterinsurgency effort is intelligence derived from a supportive population. While in conventional war the successful army is generally the side that masses firepower at the decisive point in time on the battlefield, a wily insurgent enemy rarely provides his superior conventional foe with a massed target, preferring to hide in "the sea of the people." Massing intelligence collection and analysis resources, rather than firepower, is the key to capturing or killing insurgents.

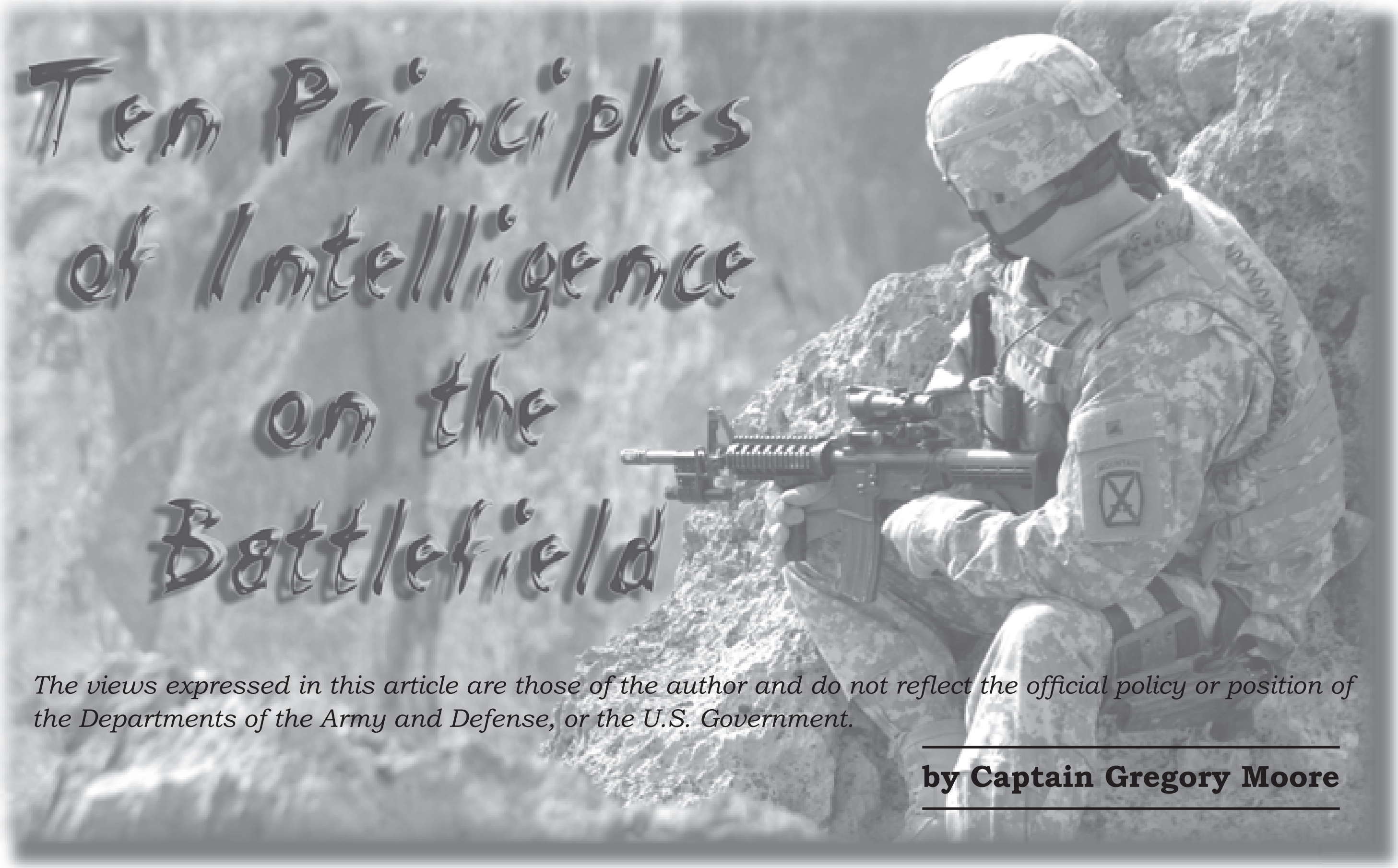
Chief among the skills required, but currently lacking in all but a few of the Soldiers and Marines in Iraq, is facility in the Arabic language. The ability to talk with and thus gain intelligence from the local population allows the trained Soldier to turn an everyday presence patrol into an opportunity to identify the enemy—the crucial and most difficult step on the road to defeating him. While the ability to talk with the local population is inherent in the ever increasing number of capable Iraqi units, Americans will be required to serve alongside and within Iraqi units for many years to come. To make them as effective as possible, they need more translators and greater familiarity with Arabic language and Iraqi culture.

The recent decision by the Marine Corps to require that every Marine develop expertise in a foreign area and language is a step in the right direction, one that the Army—and the State Department, the CIA, the U.S. Agency for International Development, and the FBI—would be well-advised to emulate.

The "Language Mission" can be done months ahead of time and in every training evolution, so listening to and speaking the Arab language becomes almost second nature. Learning cultural traits, eating the food and immersing the troops in the culture is a "Warrior Tactic" in and of itself!

Jeffrey T. Strohman is the Antiterrorism (AT)/Force Protection Program Manager at Camp Lejeune, North Carolina. He also instructs AT Level II and Homeland Security as well as IED Response and Awareness and Prevention and Response to Suicide Incidents. He is retired from the U.S. Marine Corps with assignments as Close Quarter Battle Training Chief, Special Reaction Team Training Chief, and Senior Instructor for Army, Marine Corps, and civilian SWAT and Sniper Teams.

Ten Principles of Intelligence on the Battlefield



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.

by Captain Gregory Moore

The Situation

Since 9/11, getting better Intelligence has increased in importance and priority for commanders from the Infantry company to the Commander-in-Chief. While we have entered a new period of transformation focused on lighter, more expeditionary forces enabled by superior situational awareness, our attempts to leap forward in Information Superiority have made progress but we have not made a revolutionary change.

Even as a debate goes on over increasing or decreasing the number of soldiers deployed to Operations Iraqi Freedom (OIF) and Enduring Freedom, in many units nine or more maneuver companies over a hundred soldiers each depend on a couple of dozen intelligence soldiers–many junior enlisted straight from the schoolhouse to the battlefield–in order to provide situational understanding, develop targets, and provide predictive intelligence assessments for decision makers. This shortage of intelligence support at the tactical unit level reduces the effectiveness of having additional combat units when only a few are conducting intelligence-driven operations.

Information systems limitations and increased intelligence support needs are at the center of many after action reports. The senior commander who wants to see the environment, see his force, and see the enemy is often frustrated by the lack of timeliness, accuracy, and depth of detail available to him despite huge headquarters full of systems and personnel. The junior commander in the fight is frustrated by being cut off from technology and information that could protect his soldiers and make his unit more capable and successful in their mission. In the Information Age, what factors are preventing the realization of Information Superiority? This article will explore some of the essential principles of Intelligence that determine success or failure.

Principle 1. *"Ground Truth" comes from the bottom up.*

Planned improvements in intelligence capability continue to focus on the corps and division level, but are beginning to shift to the brigade combat team (BCT). The battalion and company are either low priority or there is a perception that they do not need the powerful tools, since the real analytical work is being done at higher headquarters and pushed down. Feel free to ask any battalion intelligence officer past or present in Iraq, Afghanistan, Kosovo, Bosnia, or a joint readiness training center how valid that theory is. Despite hundreds of additional analysts, databases, and systems at the corps headquarters, the best source of accurate information on what the real situation is continues to be picking up the phone and calling the commander on the ground. There is an essential fault built into our doctrine and our information system architecture that higher knows best and will tell lower what is going on. As a result, hierarchical information systems fail and are put on the shelf, and emails and phone calls asking for the subordinate unit's read on the situation are the favored tool.

When it comes to collecting, analyzing, and producing accurate intelligence the lower the echelon, the more insight and accurate information the analyst has. However, focusing capabilities at the company runs into two problems. First is that the company lacks the perspective to put their situational understanding into a larger context, and secondly the company is focused on the urgency of the current situation and lacks the available time to develop predictive models and assessments. This means that higher echelons still need to play a role in stepping back and putting things into the context of the "big picture."

Principle 2. *The "Unit of Action" is becoming the Company.*

The discussion revolving around defining the terms "Unit of Action" and "Unit of Employment" was fascinating until the answers came out, and the brigade and division were defined as those echelons. These terms really describe what is being done on the ground by the company and battalion. Maneuver companies are responsible for battlespace, require the highest level of situational understanding to take immediate actions on the ground, and provide the greatest level of detailed knowledge on the battlespace they are in. Higher echelons, battalion and above, employ companies in assigned battlespace to accomplish tasks. Only in large urban operations or armor formations in movement to contact in wide open unpopulated areas does the battalion become a unit of action, actually controlling companies. Rarely does the brigade make that transition any more, and usually not with improved effectiveness. Not every company employed is the same, task organized companies can accomplish different tasks.

But whenever intelligence needs to be collected, influence needs to be gained, or effects need to be delivered, the best method to achieve it is to task organize a company to own that space for that period of time, and to give them the task to accomplish there. This requires that the Military Intelligence (MI) company or the Civil Affairs company with a task to accomplish in an area be given the survivable vehicles, quick reaction force, fire support, and medical aid capabilities to accomplish their mission, rather than soft-skin HMMWVs in someone else's battlespace. Alternatively a battalion commander could task a maneuver company commander with the priority task in his zone of gathering intelligence, developing Civil Affairs projects, or training indigenous security forces and task organize that company with the capabilities needed to accomplish that mission.

Principle 3. *"Hard" intelligence is most useful at the lowest level.*

As the separate collection silos represented by the "INTs" are fused and tailored for use on the battlefield, they sort themselves into two areas. "Hard" intelligence, for the purposes of this article, is intelligence primarily from non-human sensors that can be quickly interpreted using automation tools. This includes Measurement and Signature Intelligence (MASINT), Imagery Intelligence (IMINT), and Signals Intelligence (SIGINT) externals. "Soft" intelligence is dependent on human processing and analysis, including SIGINT content and almost all Human Intelligence (HUMINT) collection.

"Hard" intelligence can be processed with little human involvement or interpretation and should be the focus of streamlined "sensor to shooter" links. It needs to get to the tactical user (at company level) quickly. Many of the best capabilities provided by Tactical Exploitation of National Capabilities (TENCAP) systems are under- or unused at the echelon they are available. A cavalry squadron on the border of Iraq could have tremendously improved effectiveness using the IMINT, SIGINT, and MASINT available at corps, but will probably never see any of it. This information can be used in real-time by forces on the ground when they get the information who can then use it as timely actionable intelligence. One of the greatest capabilities to provide to the warfighter in the future is "hard" sensor data to the Force XXI Battle Command, Brigade and Below (FBCB2), where it can be immediately reacted to and acted on by ground units.

Principle 4. *"Soft" intelligence requires intensive analysis, fusion, and context.*

While "hard" intelligence can go directly to shooters, transcripts of intercepted communications and reports from single human sources require significant effort by linguists and analysts to process and interpret meaning, significance, and truthfulness. Currently a young private straight from the schoolhouse can write a report after a contact meet which is shared throughout the National system and his peer listening on headphones can write a SIGINT report that does the same, but the assessment of the analyst who knows and works and lives in that area of operations only travels as an attachment to an email to the next higher headquarters. Many battalion Intelligence Officers have been frustrated to see that the division commander is asking questions about what a soldier on a HUMINT Collection Team reported about the situation in a village directly up his single-source silo, while his assessment from HUMINT, SIGINT, IMINT, Open Source Intelligence (OSINT) patrol debriefs, meetings with local leaders, and often his own visit to the village never made it past the brigade staff's inboxes. When a senior, experienced analyst (such as an MOS 96B Intelligence Analyst staff sergeant) works for a maneuver company and has access to multiple "INTs" covering his sector, he can provide a fused, timely, accurate intelligence product. This product is valuable to his company, adjacent companies, and higher headquarters. The mission of higher echelons becomes providing him additional information relevant to his area, and providing a larger context for what his assessment addresses.

Principle 5. *Debriefing is the best source for situation development.*

Despite all of the sensor capabilities out there, nothing beats being there for developing situational understanding. Over the course of a combat deployment, Intelligence Officers and maneuver commanders usually spend increasing time and effort **to capture information by debriefing units after patrols and missions**. Many aviation units and some logistics units have become experts in debriefing and capturing this information into reporting, and it is often more useful than other "INTs" in providing context and focusing additional collection. Success in this area depends on requiring maneuver units to share their knowledge after missions and patrols, training maneuver soldiers in report writing, and training intelligence analysts and officers to be experts in conducting debriefings. If Fort Huachuca made one change to the intelligence analyst and officer curricula this year, this could be the most valuable. It would also be **a great candidate for inclusion in the Basic Officer Leader Course for junior officers of all branches**.

Principle 6. *Interrogation and exploitation are the best sources for targeting.*

HUMINT and SIGINT collection tend to dominate the focus of intelligence officers working on targeting high value individuals, and competence in their use can help a unit post a high number of detainees captured on the scoreboards briefed in nightly battle updates. In the current environment, where targeting and detention is only the first step in prosecution and transition to indigenous law enforcement for incarceration, quick action on every "pretty good" target doesn't lead to long term success. In fact overloading the system leads to mass releases including many enemy leaders and facilitators who, while not captured with a smoking gun, are more dangerous on the street than the trigger pullers.

There are many techniques and methods for good targeting, but the units with the most successful effects from targeting have a noticeable difference–they are good at interrogation of detainees and exploitation of objectives. The best intelligence for determining composition of threat organizations, current leadership and likely succession, their tactics, techniques and procedures, their security measures, morale, intelligence collection methods, logistics, past operations and future plans is capturing the right people and exploiting what they know and what their documents and materials reveal. The probability and amount of payoff from exploitation is reduced as time and space from the point of capture increase. The most effective method is to have interrogators and experts in document and equipment exploitation located with the capturing unit. The lack of resources and focus on this at the small unit level is a major detriment to the targeting effort. The payoff of doing this well leads not only to better future targeting but to some of the best insights into the enemy's organization, leadership, capabilities, and intentions.

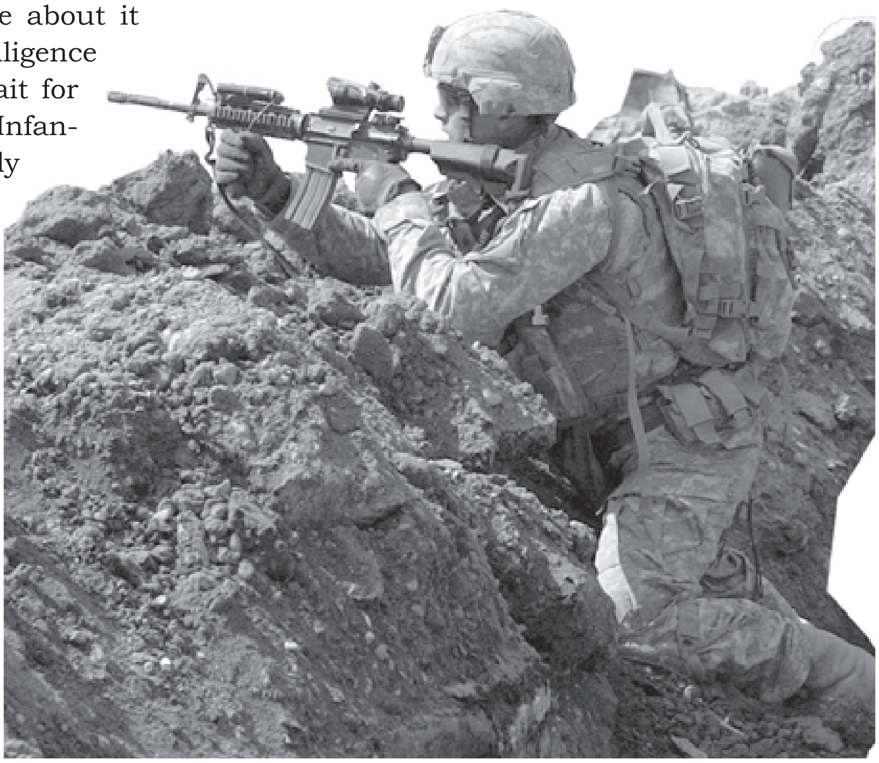
Principle 7. *Intelligence personnel need to be on the front lines.*

The vision of intelligence as a support function happening behind the lines has been overrun by the frequent necessity for collectors to be alongside maneuver units and for analysts to be with commanders closer and closer to the fight. Plans for providing intelligence capabilities to the lowest echelon units and for training and equipping intelligence personnel for a tactical role on the battlefield need to catch up to what is happening on the ground. Collection of intelligence is increasingly the focus of lower and lower echelon commanders. The low ratio of intelligence capability to combat power in frontline units leads to two frequent occurrences. The first is companies and battalions getting tasked to "move to contact" with little knowledge of what's in front of them, resulting in a maneuver unit that rolls over a hill and is surprised to find the enemy (conventional or insurgent forces). The second is forward operating bases taking mortar fire, sniper fire, or other attacks and being able to do little about it besides send out patrols, have non-intelligence personnel try to develop HUMINT, or wait for intelligence from a higher echelon. An Infantry battalion commander after an early OIF rotation recommended in his After Action Review (AAR) that "Conduct Intelligence, Surveillance, and Reconnaissance" be added to the infantry battalion's Mission Essential Task List (METL). Special Forces teams training the Iraqi Army (IA) rewrote the IA's company METL for counterinsurgency operations to include intelligence collection and target development and exploitation at the company level. A recent corps-level AAR suggests creating an military occupational specialty for an intelligence soldier focused on police-style crime scene investigation (CSI) for site exploitation on objectives.

Marine Corps HUMINT Exploitation Teams (HET) at maneuver battalions are large enough to split sub-teams to each maneuver company and this is how they operate. SIGINT teams are increasingly removing their equipment from their authorized soft-skinned vehicles and placing it into Strykers, Bradleys, and Up-Armored HMMWVs to accompany combat units on missions and patrols. None of these units leaves the wire on a real-world battlefield without being attached to a combat arms escort. Battalion intelligence officers are operating forward in assault command posts, meeting directly with indigenous security forces, and conducting tactical questioning on objectives. Current schoolhouse training and doctrinally authorized equipment for intelligence units treats them like rear echelon support personnel. When they actually deploy and are sent forward onto the objective with the Infantry, they frequently have inferior equipment and training to shoot, move, and communicate with a combat arms company. The training, doctrine, and equipping for MI needs to catch up to the realities of the current battlefield.

Principle 8. *Transparency reduces duplication between higher and lower echelons.*

In the current environment where analysts at brigade and below are in critically short supply, there



are reservations about pushing them down to company level despite the demonstrated success in doing so. The problem is that higher echelons are continually duplicating the efforts of the echelons below them. Some of this comes from the ubiquitousness of raw reporting and only informal availability of fused and analyzed assessments from lower echelon analysts. The focus on the daily Intelligence Summary as a stiff, just-the-facts collection of reporting with a few analyst comments also contributes to this, rather than making it a thorough product sharing the knowledge and 'gut feel' that the lower echelon has for the situation in that area.

Bandwidth restrictions in sharing data also contribute, along with doctrine and a system architecture designed to provide a common operating picture from higher to lower instead of from lower to higher. As a result, many of the daily products and detailed tactical products being worked on at the higher echelons with lots of analysts were already created—with greater accuracy and familiarity with the situation—by junior analysts in lower echelon units. When lower echelons provide good assessments with a real feel for what's going on, this should be a simple cut and paste at higher echelons reducing the required staffing and footprint for the G2/J2 section. Reducing analysts at higher echelons fills vacancies in the units that are actually producing the intelligence, resulting in better products, and even better situational understanding at the higher headquarters. The higher headquarters requires a few analysts with advanced training, education, and experience to develop the situational awareness of companies and battalions into predictive assessments that are the basis of command decisions. They also need to quality control and provide the big picture context for what the companies and battalions are describing as their view on the ground.

Principle 9. *The indigenous population is the 'key terrain'.*

Key terrain provides a significant advantage to the side which holds it. In modern warfare where battles take place in cities and villages and political outcomes are influenced by individual actions on the ground, both sides focus on effects that influence the population. Whether conducting offensive operations or nation building, the local population cannot be reduced to the status of "Civilians on the Battlefield." There is a lot of focus on providing "atmospherics," which translates into subjective assessments of whether a given area is leaning more "red" or "blue" and what issues are pressure points in that area. Terrorist and insurgent tactics focus on influence and effects on the population as much or more than on directly affecting coalition units. Improvised explosive devices which do not destroy Coalition vehicles but which intimidate the population from getting close to or interacting with Coalition patrols can be a shaping tool to bring an area under insurgent control without causing military casualties. Large numbers of detainees captured from an area that are quickly released can cause anger when the innocent are taken away unjustly or fear of Coalition impotence when the guilty return quickly to take revenge on informers. Crime, poverty, family linkages, cultural and religious ties, political ideology, economic interest, and other factors shape the population's response to the Coalition and to the enemy. The ability of local police to find, arrest, and incarcerate gangs and organized crime reduce the freedom of action and the infrastructure of insurgent and terrorist cells. Confidence in local government and security determines cooperation with indigenous and coalition security forces, and creates a non-permissive environment for the enemy to move and operate. In order to be successful, our intelligence collection, analysis, and assessments need to incorporate characterizing the population and the influence of friendly and enemy forces within that environment.

Principle 10. *The Army is getting smaller, but more capable.*

At the unit level, the Army is focusing on creating the BCT. This step of Transformation was recognition of what was already being done within the divisions in the 1990s, rather than the development of a new concept. Today capabilities within the BCT are already being divided and task organized lower to create more autonomous and expeditionary battalions and, in many cases, companies. In Afghanistan and Iraq, companies may operate from their own operating bases over a hundred miles from their battalion headquarters. As OIF draws down in size, units will be increasingly spread out and lower echelon units will have to assume larger areas, requiring more decentralized capabilities. The efforts to push more capabilities down to battalion and company level make deployments of smaller units with less overhead more realistic. An additional factor shaping capability is high reenlistment rates and lower recruitment rates. A smaller force of more experienced, trained, and senior soldiers can equal or outperform a larger force. This fact is employed both by enemy cells as well as our own Special Operations Forces.

The Future Architecture

As the 130,000 plus footprint in OIF sees its sunset while the Global War on Terrorism (GWOT) continues into the future, a reality that many face with dread will be the future reduction of funding and political will to support large deployments. A potential reality is that OIF may be the last corps-size deployment. Development and evolution of our Army into the Future Combat System and whatever its follow-on generation will be will proceed. But the process is likely to shift from building up the modified Table of Organization and Equipment (MTOE) to paring down to what is most needed, and detailing its functions at lower echelons. Large chunky organizations will give way to more complex and capable small units. What will the future look like?

Horizontal Networking. Current hierarchies will flatten. There will be fewer layers of command between the Theater commander and tactical (company) commanders on the ground. Companies and battalions will share more information horizontally; collect, analyze, and fuse information at their level, and share the information laterally as well as vertically to build situational understanding. This could require re-looking the rank structure in these small unit headquarters.

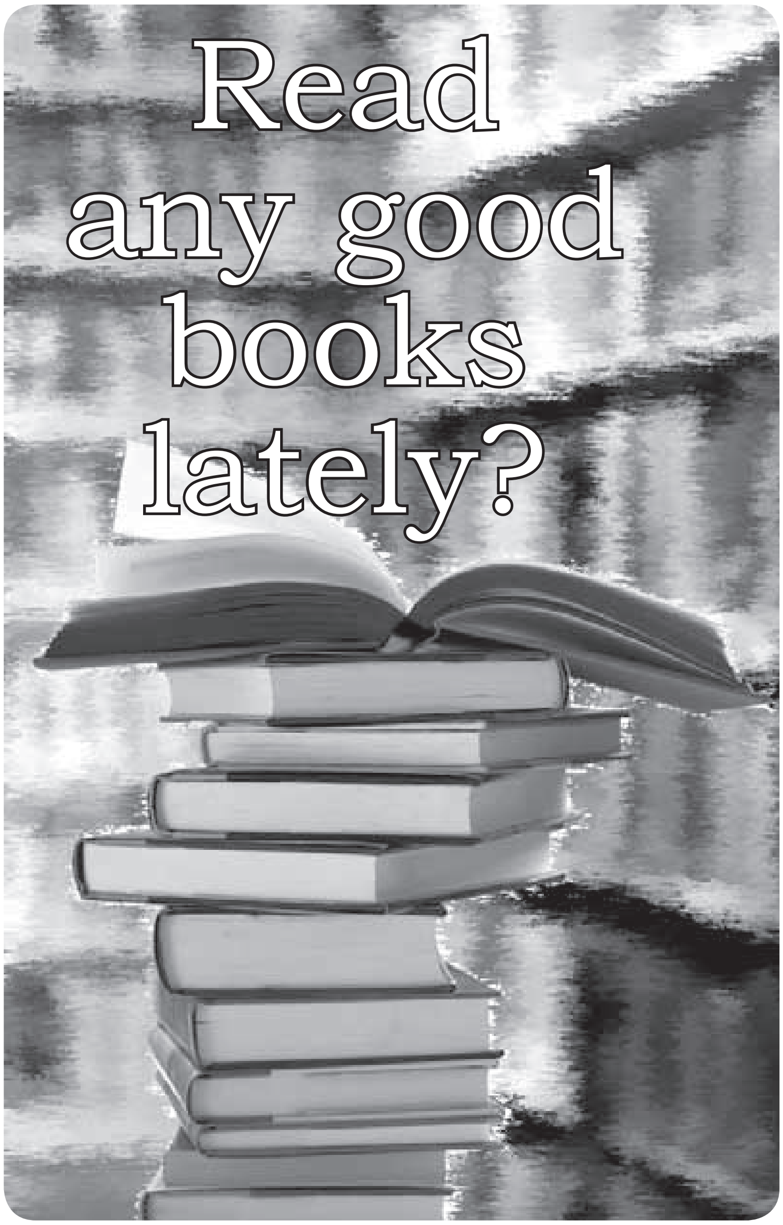
Employment versus Command and Control. The GWOT as well as many stability and support operations have involved small unit deployments for a particular mission. Future deployments may be headquartered by a battalion, and certainly there will continue to be brigades as operational headquarters. Brigades will give missions and battlespace to battalions and then become resource providers–providing logistics and financing, as well as coordinating reachback support from military and National agency direct and general support sites in the United States. Battalions will straddle the line, as a resource and support headquarters when their companies operate from decentralized locations and as a combat headquarters when multiple companies are employed together in a fight. This consolidation will continue to be common in urban offensive missions. No mission—combat, humanitarian, or other—will be able to be accomplished without collecting, analyzing, and producing intelligence, and this will increasingly be done at the company level by analysts on the ground with the company or providing direct support from a reachback location. Additional fusion and context will be added by battalion analysts, who may be augmented by dedicated analysts out of Theater. Senior experts in single source "INTs" or specific capabilities will be at battalion or available by reachback to provide technical oversight and control of the companies' ISR operations.

Individual Productivity and Capability. In order to make smaller, more capable units work, the individuals in them must be more capable. Initially this will require more training. This will also require changes to traditional rank structures as more senior noncommissioned officer positions for analysts and collectors will be required to have experts instead of novices working at the tactical level. MI second lieutenants may go away and the branch may require a graduate degree for commissioning or branch transfer. Systems will be focused on providing advanced tools to trained skilled intelligence professionals rather than a focus on fielding and manning systems with mass-produced junior soldiers.

Greater Coalition Capabilities. One benefit of the increasing shift towards smaller units of greater capability will be that increasingly, Coalition partners will be able to provide like capability expeditionary companies and battalions. This will require standards and flexibility for not only British and Australian but Polish, Italian, Japanese or Korean company-sized units to be integrated into a U.S. battalion, including horizontally integrated intelligence and operations information systems for a common operating picture. Another great leap that is not far in the future will be small U.S. unit employment under the headquarters of another nation's military forces. Our forces must have the intelligence and logistics capabilities needed to operate effectively in that environment, as well as already having procedures in place to share classified products with coalition partners.

The Evolution of Conflict. All the principles outlined above are intended to highlight some of the issues for the Intelligence Warfighting functions due to the continuing evolution of conflict, and that how we fight today comes from what works on the battlefield and not the way we wish it would work. Resistance to change can restrict our readiness to respond to future situations we will find ourselves in, but it can't deny the reality of what that those situations will be. We can't force the enemy to change because we had the perfect plan and the way he's fighting doesn't fit it. We can't force the way battles and warfare unfold on the real-world battlefield because they don't fit the doctrine and systems we have developed. Just as we study the enemy in order to predict what is coming next, we need to step back and study ourselves and the contemporary operating environment, and predict what we must become to be successful in that environment.

Captain Gregory Moore has completed two deployments to Operation Iraqi Freedom as a Battalion Intelligence Officer with 10th Mountain Division and 5th Special Forces Group.



We welcome reviews of books related to Intelligence or Military History. Please review our list of available books and book review submission standards under the Professional Reader Program at www.umi-online.us/mipb.

Email your book reviews along with your contact information to mipb@hua.army.mil.

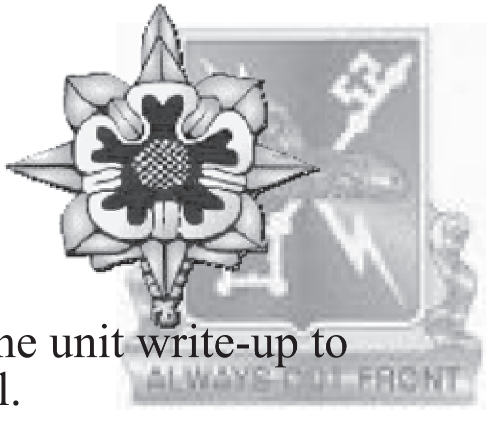
Unit Profiles

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

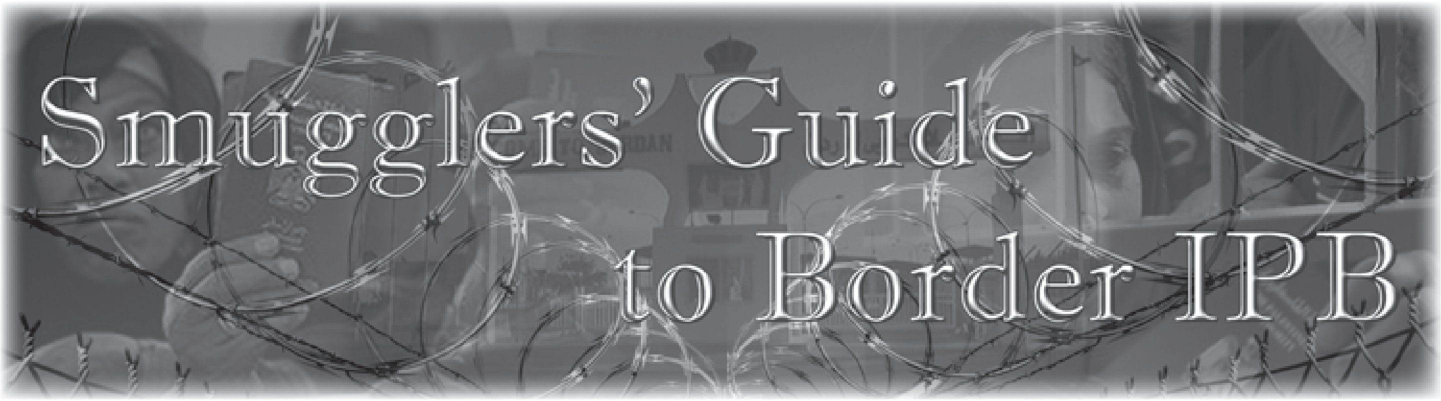
- High resolution color photographs or high resolution soft copy (preferred) of the unit crest.
- History of the unit to include campaigns and decorations.
- Current unit subordination, status and mission (unclassified).
- Operations your unit has supported in the last 15 to 20 years.
- Recent special 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 the any photographs at the earliest possible time to:

ATTN ATZS-CDI-DM
USAIC&Ft. Huachuca
550 Cibeque St.
Bldg 61730, Room 124
Ft. Huachuca, AZ 85613-7017



Please send the soft copy crest and the unit write-up to mipb@hua.army.mil.



Smugglers' Guide to Border IPB

by Captain Tedd Goth

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.

The purpose of this article is to address the question, "What challenges do cross border operations pose for the Intelligence Warfighting Function (WFF) that may require a different analytical approach to the Intelligence Preparation of the Battlefield (IPB) process?" Since the majority of the world's population is located within 200 miles of an ocean or sea (littoral outlines), the dynamic relationship between entities of a land locked border situation is often overlooked and even more difficult to effectively reconcile within a unit's operational framework. As counterinsurgency (COIN) operations continue to embody the bulk of current U.S. combat missions, the "people" factor as an enemy combat multiplier can decisively become the enemy center of gravity. Smuggling, or the process of moving people and/or goods across a nation state's declared border without permission from the state, inherently becomes a key enemy combat support function within the COIN environment.

Borders create a non-doctrinal problem set that requires an atypical approach to IPB and intelligence, surveillance, and reconnaissance (ISR) operations. The underlying challenge continues to evolve around the Intelligence WFF's ability to effectively conduct ISR focused against the far side of the border. This "denied area" is often difficult to reconnoiter because of diplomatic or regional geopolitical relationships. Unlike the geometry of the traditional forward line of own troops (FLOT) or the nodal geometrics of the asymmetric fight, a border creates a linear intelligence curtain. Effective, atypical IPB is required to gain a comprehensive understanding of operational dynamics that exist across the border in the denied area. Similar to entering a cinema to watch a movie that is half complete, activity in the denied area requires the analyst to visualize activity in the denied area as it develops; relying heavily on correlated activity occurring on the near side. Additionally, elements crossing the border may be afforded the legal protection of the far side nation state prior to breaching and entering the near side, making it difficult to acquire fleeing targets before they enter the near side. Thus, shaping the operations must begin at the border, but the intelligence required to shape the fight is limited unless extensive cross-border IPB has been conducted correlate activity on both sides of the border.

The objective of this primer is to illustrate the effectiveness of historically proven tactics, techniques, and procedures by focusing on the analysis of border dynamics. It outlines theories developed to assist the analyst in understanding of the dynamics that borders create. The focus is on insurgent elements found in a low intensity conflict that likely have some degree of a partial environment 'safe haven' within the denied area across the border.

Border Environment Definitions

Before assessing the areas of operation and areas of interest, it is important to understand the area of influence. Borders are bilateral in nature, in that what crosses in one direction may eventually traverse back. Borders are also bilinear in nature and create several parallel zones that create multiple axes of potential decision points.

It is imperative not to confuse borders with boundaries. A boundary is no more than a delineation of a physical piece of battle space whether it is ground, air, or sea in nature. A border on the other hand is a point at which one nation state's authority or jurisdiction ends and another one begins.

Whether agreed upon or disputed, a border in question is actually two borders not yet defined. As such the question is "Where in space does each nation state's authority terminate?" For IPB purposes, it is understood that the termination point of the last physical location a nation state can effectively exercise its authority is the actual border versus the perceived border delineated through agreements, maps, etc. The following are characteristics of borders—

- A border is not a defined linear agreement between two nation states per se (although it can be perceived to be that); rather it is the understood agreement or possible disagreement where one nation state's authority begins and another ends.
- The borderline is the perceived point or agreed upon point (what is shown on a map) at the terminus of one nation state's authority and where another begins. In this primer the borderline is labeled the ***line of demarcation*** **(LOD)**.
- A border can be "people" driven, as often seen in tribal agreements in which the LOD is where one tribe's ethnic influence ends and another begins. Borders, more often than not, are terrain driven, where the land within the border is under assumed ownership. Borders can also be industry driven where there is an understanding that as far as space is concerned encroachment on one corporation does not occur by another. It is important to delineate what drives the border's creation prior to the initiation of the IPB process.

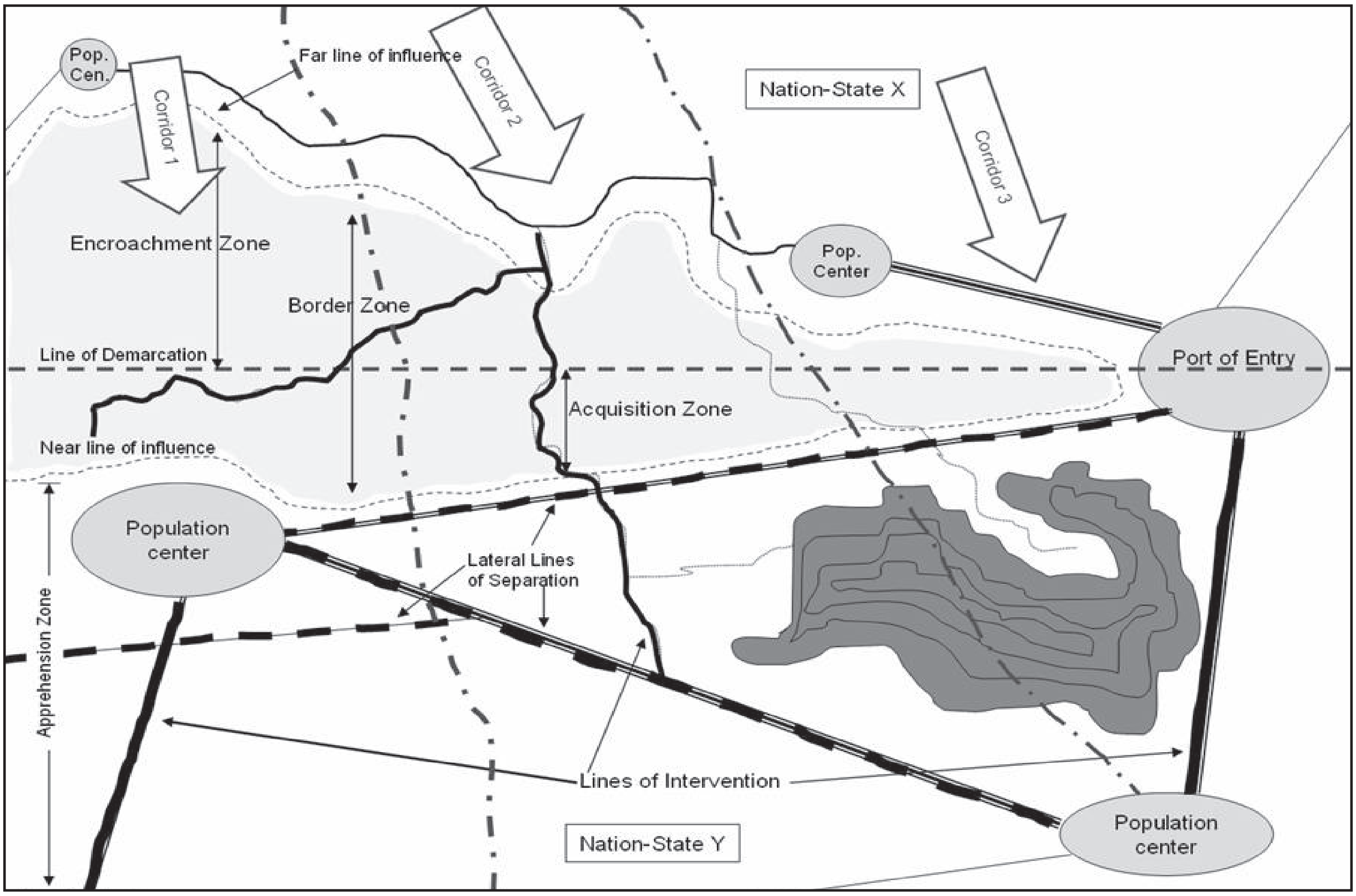


Figure 1. The Border Environment.

There are multiple efforts or reasons why a border is encroached upon or breached. In this primer the word effort can be replaced by whatever the situation is on the border in question. For example, if it is a trafficking situation, then the term effort can be replaced with trafficking.

The first step in dissecting the given areas of operations and interest is to identify the "understood" LOD (see Figure 1). More often than not this is the point delineated on the map. Over time and especially in conflict, the LOD may not be as obvious and some research with the host nation may be required. Once the LOD is delineated, identify and mark all population centers which may provide sanctuary. Consider all population centers on either side of the LOD that provide support and seclusion to the effort. If a population center has a certain percentage of ethnic balance in favor of the effort, or industrial, religious, or political relationship, then that population center is considered an area of sanctuary. Special attention should be placed on ports of entry or population centers on the LOD that allow for the legal processing of transients, shipments, etc across lines of communication.

The ***line of influence*** is the terminal point at which authority, whether civil or military can effectively control movement away from or towards the LOD. The lines of influence are used to delineate the realistic physical border in which a nation state can actually execute its authority. For instance, if the nearest town at one point along the border is sixty miles away with no militia and a small police force, then the actual area the nation state may exercise its authority may lie within only twenty miles of that town, leaving forty miles of battle space between the border and the line of influence. Thus the "real" border for that nation state begins to develop. The *far line of influence* is that area on the far side of the LOD where the far nation state's ability to exercise its authority ends. The ***near line of influence*** lies on the near side of the LOD and delineates the farthest point at which the friendly influence ends.

The ***border zone*** is the area between the near line of influence and the far line of influence that encompasses the LOD. The wider areas of the border zone realize the least amount of threat to the breaching effort.

The encroachment zone is the area between the far line of influence and the LOD which the far nation state's authority is still understood. It is in the encroachment zone where the decision to breach the LOD occurs. Unlike a disruption zone or the far side of a FLOT the effort may still have legal protection within the encroachment zone.

The ***acquisition zone*** is the battle space between the LOD and the near line of influence where shaping operations occur using ISR resources to acquire and identify movement from the LOD. The acquisition zone is the battle space where ISR shapes the operation.

The ***apprehension zones*** are located behind the near line of influence and about the acquisition zone. The apprehension zone is the battle space where perpendicular movement through the acquisition zone is intercepted and/or engaged by maneuver.

The ***lines of intervention*** are lines of communication (LOCs) that run *perpendicular or semi-perpendicular* from the LOD, and provide for movement away from and towards the LOD. Once these lines are influenced by maneuver the effort is intervened forcing the effort into a lateral line of separation and possibly into another corridor.

The ***lateral lines of separation*** are LOCs that run *parallel or semi-parallel* to the LOD and bisect lines of intervention. Lateral Lines of Separation are LOCs that provide cross corridor movement.

A ***corridor*** is a series of lines of intervention (perpendicular LOCs) that begin on the far line of influence and extend across the LOD, and beyond the near line of influence. A corridor extends from a midway point between two lines of intervention, laterally to the next midway point between two lines of intervention. (See figure 1) The corridor with the largest border zone area is the most preferred since it affords the least risk when the breach occurs. If the corridor does not provide a feasible avenue of approach, then the next best corridor is chosen. For example, in Figure 1, Corridor 1 is the best choice since the least amount of nation state influence is available on either side of the LOD. However, it does not offer a mounted or dismounted avenue across the LOD. Corridor 2 then is the next best choice.

Effects of Weather, Terrain, and Illumination on the IPB Process

Weather Factors.

- **Visibility**. Without the ability to reconnoiter, infiltration across the LOD into the acquisition zone is not likely to occur, unless the effects of low visibility are offset with artificial detection means.
- **Precipitation**. Mobility is highly dependent upon the composition of LOCs that are utilized to breach the LOD. Rain or snow can affect the soil composition.
- **Temperature and Humidity**. Unless the effort is dismounted or the road surface is icy, temperature has minimal effects on most mounted infiltration efforts across the LOD. Temperature can drive the decision in a dismounted effort to abort and launch at more conducive times (night for cooler periods, days for warmer) or force a mounted infiltration.
- **Wind**. Similar to temperature in that wind has low to moderate effects on dismounts and little to no effect on mounted infiltration. Visibility is degraded in sand or snow for both dismounted and mounted efforts.

Terrain Factors.

- **Observation**. This factor is most important for the effort while it is in the encroachment zone preparing to breach the LOD and a decisive factor in determining time to commit to the breach of the LOD.
- **Cover and Concealment**. The LOD is the critical and most desired location for concealment. Concealment within the acquisition zone is also desired if the effort has not transitioned from dismounted to mounted.
- **Obstacles**. The composition of the LOD (in reference to obstacles and terrain) and its effects on perpendicular movement across it will have a major influence on speed, timing, and cross-corridor movement. Obstacles placed at the right locations will force a decision point to move into another corridor or breach the obstacle.
- **Key Terrain**. The most likely breach points along the primary and secondary corridor are considered key terrain as are areas of sanctuary which provide key logistical and command and control (C2) capability. Terrain within the apprehension zone that provides for intervention of the effort should not be discounted. Population nodes within areas of sanctuary that will provide support to the effort are also key terrain.
- **Avenues of Approach**. Focus is on lines of intervention that run perpendicular and semi-perpendicular to the LOD. When interlocked they form a single LOC providing for movement away from and towards the LOD. Additionally, lateral lines of separation provide for cross corridor movement when a decision must be made to change corridors.

Illumination Factor.

- **Lunar cycle.** For many efforts the availability of night vision devices is slim. The lunar cycle will play a heavy role in the mission cycle of most LOD breach efforts. Dismounted nighttime breaches are more likely to occur during periods of mid to high illumination, whereas dismounted efforts during low to mid illumination may likely force a decision to mount for the breach.

Enablers to Border Crossing

Unlike the standard IPB based on order of battle and doctrine, border IPB is more a question of the enablers used to breach the LOD and the subsequent movement through the acquisition zone. Enablers can be broken down into the following four categories:

- **Category I (Reconnaissance and Guides).** Those individuals with direct involvement in the active movement of people and/or goods across the LOD.

- **Category II (Command and Control (C2) and Logistics).** Those individuals with direct involvement in the planning, C2, and logistical support of the movement of people and/or goods across the LOD.
- **Category III (Facilitators).** Those individuals with passive involvement in the support of the movement of people and/or goods across the LOD.
- **Category IV (Nonparticipants)**. Those individuals with unintentional involvement in the support of the movement of people or goods across the LOD.

Reconnaissance Teams (Category I) can and often are located on both sides of the LOD. They are most likely to have some sort of C2 ability in order to report findings. They will work in one 2-to-3 man team and can be either mounted or dismounted. Reconnaissance teams focus on verification or denial of uncompromised access along the lines of intervention through the designated corridor. Over time, reconnaissance can occur rapidly as teams look to simply identify changes and abnormalities of an often used corridor. Reconnaissance elements within the encroachment zone are likely to be from the nation state in that zone. Reconnaissance elements within the acquisition zone may or may not be from that nation state. It is likely and most desirable that an ethnic, political, industrial, or religious ideological cohabitation exists between the populations of the two nation states where the breach of the LOD is to occur.

Guides (Category I) are familiar with routes and will actively conduct the movement in one of three fashions:

- Link up with the package (personnel or goods) prior to the far line of influence and move the package through the encroachment zone, then create the breach and move the package through the acquisition zone to a link up point around or beyond the near line of influence.
- Link up with the package prior to the far line of influence and move the package through the encroachment zone, then create the breach and link up with a second guide in the acquisition zone. The second guide will then assume control of the package and move it through the acquisition zone to a point around or beyond the near line of influence.
- Link up with the package prior to the far line of influence and move the package through the encroachment zone. Conduct link up with a second guide who will assume control of the package, create the breach, and move the package through the acquisition zone close to or beyond the near line of influence.

Guides will have a working knowledge of mounted and dismounted routes within the area of operations. They will most likely be inhabitants of the nearest population center and for the most part operate within their own backyard. They will have a motive as to why they must be out beyond certain restricted limits (i.e., farmer, industry, law enforcement, etc). Guides face threat of capture and will likely abandon the package if apprehension is imminent. Many guides will not fully understand or have a working knowledge of the bigger picture. They more often than not are armed and have some sort of communications capability. Guides are replaceable but the loss of an experienced guide can be a decisive point for the use of one or more corridors.

C2 (Category II) in border crossing operations is often fragmented and disjointed. The ability to direct and influence the C2 element is a difficult task without two well-secured nodes on either side of the LOD. Expect one of three forms of C2 during the breach operation:

- One C2 cell located on the far side of the LOD with another C2 cell located on the near side of the LOD. There is a pre-determined passage and link up point designated to move the package to an established decision making authority on either side of the LOD for contingencies.
- A C2 cell located only on the far side of the LOD with the decision making authority on the near side of the LOD given to the guide.
- A C2 cell located only on the near side of the LOD with the decision making authority on the far side of the LOD given to the guide.

C2 operatives have a working knowledge of the mission, package requirements, and diversion and abort authority. They will most likely coordinate for the timing, size and composition, and location of the package.

Logistical support (Category II) makes use of mounted assets which can rapidly and effectively move the package. This effort can occur in several ways:

- Mounted support is provided prior to the far line of influence, and continues through the encroachment zone, across the LOD, through the acquisition zone, and beyond the near line of influence. This Course of Action (COA) requires the least amount of C2.
- Mounted support is provided prior to the far line of influence to the LOD where a second support effort from the near side assumes control of the package and conducts the movement from the LOD to beyond the near line of influence. This COA requires minimal C2.
- Mounted support is provided prior to the far line of influence to a point within the encroachment zone where the package is dismounted and moved across the LOD into the acquisition zone or nearest sanctuary. Link up with a second mounted effort occurs within the acquisition zone or area of sanctuary. This COA requires the most amount of C2.

Logistical cell personnel will often be involved in vehicle theft as well as having close ties with trafficking organizations associated with capital ventures. They will have extensive defensive driving skills and a working knowledge of local law enforcement limitations and countermeasures. They will most likely not have a working knowledge of the bigger picture. Many will be paid for their services, thus having a monetary motive for their actions.

Facilitators (Category III) provide passive support through funding, safeguarding, propaganda, recruiting, and passive surveillance. They will have an ideological, ethnic, religious, or political tie to the effort and will, in limited ways, lend their support. Facilitator support is needed by the effort on the near side of the LOD. Apprehended facilitators will not have a damaging effect on the effort, but a concerted psychological and information operations campaign targeted at a community of facilitators will have significantly effect the motivation of facilitators to support the effort. Those who feel threatened stop participating until they feel the limited amount of risk is worth the effort.

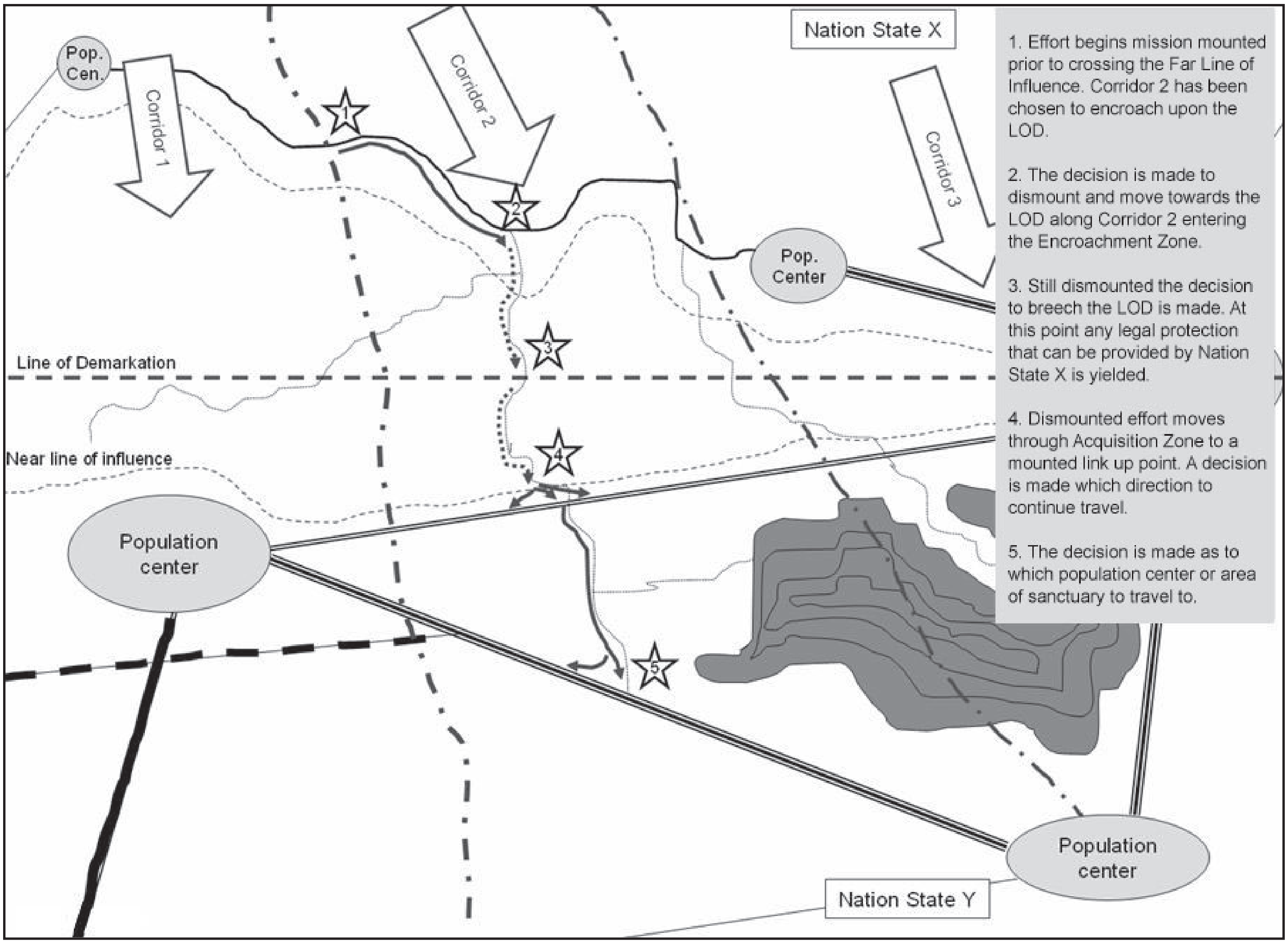
Non-participants (Category IV) unknowingly lend a hand to the effort and end up as potential targets for capture from friendly forces. Whether lending out a phone or picking up a hitch hiker, they can become unwilling participants. A strong information operations campaign helps to ensure that the local population is educated on the effort, thereby avoiding inadvertent support and limiting the ability of a true Category III facilitator from claiming non-involvement.

Processing Intelligence into Actionable Objectives

The objective COA is developed through the enabler's mission cycle which, when analyzed, predicts the time and space of future potential LOD breaches (see Figure 2.) The **mission cycle** model is merely a predictive tool that attempts to predict the timing of future breaches of the LOD by delineating the days between the effort's missions. If predictive analysis proves successful, deviation from historical movement patterns can be expected and thus a new mission cycle is created. Deviation is the effect that causes the effort to adjust corridors in response to an unsuccessful breach or infiltration along one corridor. Friendly forces can expect deviation to occur after each successful apprehension. The mission cycle is developed by identifying the catalyst which initiates the cycle. Several if not hundreds of different events or actions can serve as catalysts to include:

- A safe house on the far side of the LOD reaches maximum capacity and the package must be moved.
- Specific goods arrive on the far side of the LOD. This can be an indicator of a lack of a specific good or package on the near side, i.e., special weapons.
- An action occurs on the near side which requires new resources from the far side (i.e., a successful offensive against the effort that depletes its resources.)

- A shift in the numbers and location of available corridors causes a need for resources from the far side.
- The lunar cycle.
- Weather patterns create a cycle that allows for movement (i.e., winter in the desert versus summer.)
- Religious celebrations or annual harvests.



1. Effort begins mission mounted prior to crossing the Far Line of Influence. Corridor 2 has been chosen to encroach upon the LOD.

2. The decision is made to dismount and move towards the LOD along Corridor 2 entering the Encroachment Zone.

3. Still dismounted the decision to breech the LOD is made. At this point any legal protection that can be provided by Nation State X is yielded.

4. Dismounted effort moves through Acquisition Zone to a mounted link up point. A decision is made which direction to continue travel.

5. The decision is made as to which population center or area of sanctuary to travel to.

Figure 2. COA Decision Points.

Once a catalyst is defined, it is set to a chronological baseline. The baseline is built backwards by planning the time it takes the effort to move from the far line of influence into the encroachment zone, through the breach at the LOD and beyond the acquisition zone to the near line of influence. Backwards planning allows for the delineation of the complete mission cycle. The chronological baseline is anchored off the timing from the far line of influence to the near line of influence coupled with critical events and decision points (thus creating the event template.)

Once the mean mission cycle baseline (time) is established and friendly forces meet success from the analysis, the effort will most likely deviate from the routine and attempt to change corridors and movement patterns. In order to anticipate the effort's decision to deviate, several activities can effect the effort's decision cycle:

- Use of deception along inactive corridors in order to make it appear as if friendly forces are present.
- Limited to zero apprehensions across or near the LOD in the acquisition zone so as not to reveal sensor locations.

- Presence along lines of intervention, which forces the effort into lateral lines of separation with apprehension occurring in an adjacent corridor.

Use of apprehension zones allows for freedom of maneuver in which detection occurs without the effort correlating cause and effect between movement through one corridor and the resulting apprehension. Lines of intervention allow for progressive movement away from, and towards, the LOD. Friendly presence along lines of intervention forces the effort into a decision, and more often than not forces him into a lateral line of separation towards another corridor.

Analysis of areas of sanctuary and ports of entry requires the use of urban IPB tools which allow for the realization of how the effort will move mounted and dismounted, and the amount of time the effort can remain in the area. Some tools that can assist with this IPB: areas, structures, capabilities, organization, people, events (ASCOPE) analysis (see Figure 3), city structure and design analysis, and analysis of street patterns.

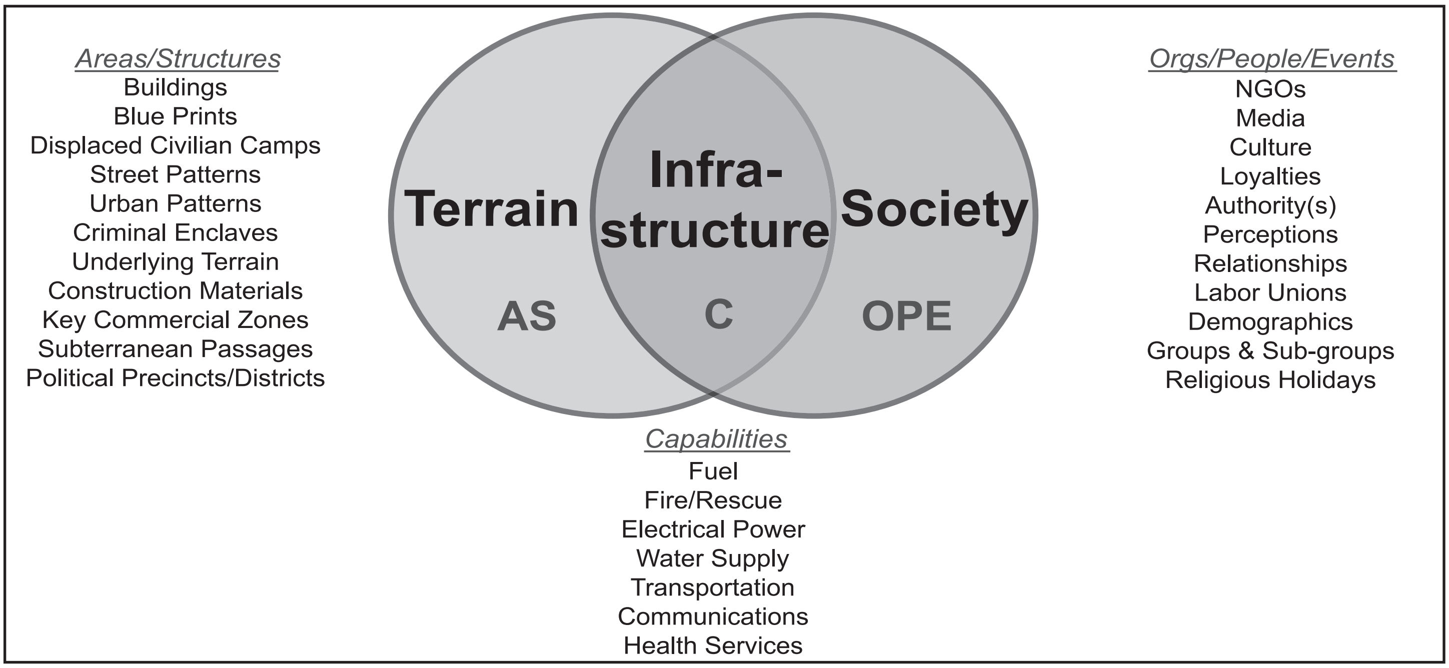


Figure 3. Key Elements of Urban Environment.

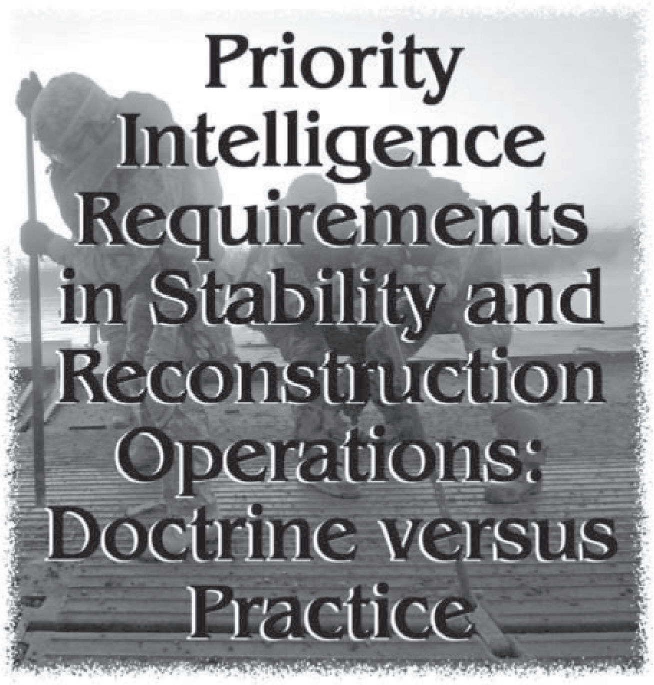
Some of the considerations for ISR operations in border areas include:

- Named areas of interest (NAIs) focusing on mounted and dismounted decision points across the LOD in the largest border zone areas.
- Secondary NAIs focusing on the first points at which lines of intervention meet lateral lines of separation.
- Use of passive sensors monitored from a distance and focused along the LOD (terrain considered and emplaced during hours of darkness).
- Areas along the corridor where mounted and dismounted efforts will occur, making NAIs on or near those locations.

Conclusion

Borders create an intelligence curtain in which analysts must rely heavily on cause and effect analysis, coupled with patterns and predictions analysis. Using the methodical approach outlined is this primer, the analyst can effectively discover and analyze those factors which influence the decisions that cross border efforts make. By analyzing how geometrics (geographic combined with geopolitical factors), terrain, and

(Continued on page 43)



Priority Intelligence Requirements in Stability and Reconstruction Operations: Doctrine versus Practice

by David S. Pierson

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.

As a G2 in Kosovo, I remember an uncomfortable situation when I had to defend the Task Force's priority intelligence requirements (PIRs) to the USAREUR Commander, General Montgomery Meigs. He criticized them for not being related to time or even decision making. With the luxury of time, hindsight, and some wisdom I have had to begrudgingly admit that he was onto something. Our PIRs could not accomplish what they were supposed to do. Strangely enough, as I have looked at the PIRs in use in Iraq I have seen requirements that look hauntingly familiar and I wonder why.

PIRs are those intelligence requirements—the information about the enemy or environment—for which a commander has an anticipated and stated priority in his task of planning and decision making.[1] PIRs are usually crafted by the G2 or S2 and approved by the commander. A PIR answers a single question, supports a decision, and is linked to time. However, PIRs employed in current Stability and Reconstruction Operations (SRO) usually fail to meet these doctrinal standards. Is the doctrine inadequate? Are commanders and G2s misutilizing their PIRs? Or is there another cause? To get at this answer one must understand Commander's Critical Information Requirements (CCIR), the nature of Stability and Reconstruction Operations (SRO), and the doctrinal application of PIRs within Army operations.

PIRs and Friendly Forces Information Requirements (FFIRs) are the components of CCIR–that information required by the commander that directly affects decision making and dictates the successful execution of military operations. The purpose of CCIR is to let the staff and subordinates know what information the commander deems necessary for decision making. Decision making is the determination of a course of action (COA) as the most favorable for accomplishing the mission. It may also be a determination to initiate critical events during an operation such as committing the reserve.[2]

Properly identifying PIRs is critical to efficient operations. **FM 2-0, Intelligence**, provides our most current doctrine regarding the elements of good PIRs which it lists as:

- Asking only one question.
- Supporting a decision.
- Focusing on a specific fact, event, or activity.
- Generally indicative of an enemy course of action.
- Linked to a latest time the information is of value (LTIOV).[3]

The "Priority" part of PIRs is what distinguishes these requirements from the myriad other requirements out there. We understand that we cannot collect and analyze everything, so we prioritize to organize our effort. The priority collection and analysis goes toward answering PIRs. The rest of what we collect, and perhaps analyze, falls into the category of information requirement (IR). An IR is an information element required for planning and executing operations. It is not necessarily linked with a decision or to mission accomplishment.[4] The main distinction between a PIR and an IR is the linkage of the former to a decision.

It is important to understand that a decision requires a choice. If information received will result in the same action or response in all anticipated circumstances or COAs, then there is no choice and this information should not form the basis of CCIR. For instance, the discovery of a specified High Payoff Target (HPT) will result in automatic engagement if it meets target selection standards. Engaging the HPT is automatic, a matter of standard procedure. This process does not involve decision making. Therefore the HPT's location may be an information requirement (IR) but it is not a PIR.

Planned Operations Drive Intelligence

SRO are more complex and more difficult to understand than conventional operations. Our inability to understand the complexities has led to the catchy phrase, "intelligence drives operations." That is doctrinally backwards. The intelligence process is driven by PIRs, emphasis on the 'P'. Commanders, based upon anticipated decisions in planned operations, set the priorities and determine PIRs. Therefore, planned operations drive intelligence. While intelligence may drive current operations, it is most likely intelligence derived from IRs and is reactionary in nature. This is the point where you are fighting the enemy rather than the plan. While often necessary, this method of fighting yields the initiative. In an ideal world—and our doctrinal world—we gain and maintain the initiative while our plans drive intelligence gathering to address key, anticipated decisions.

Our ability to plan is about half right in SRO. FM 1, The Army, defines SROs as operations that "sustain and exploit security and control over areas, populations, and resources.[5] They employ military capabilities to reconstruct or establish services and support civilian agencies." We get the first half—*security*—about right. The military readily accepts its overarching role as that of the primary function of any state, establishing the monopoly on violence.[6] This is a habitual requirement; it does not have a life cycle. Addressing this mission means affecting those non-state organizations and people who desire a franchise on violence; it is all about eliminating the competition. This can take the form of direct action against or influencing of our adversaries. Either way this process is mostly targeting which is principally supported by IRs rather than PIRs. Thus, we tend to dumb down SRO into just security operations that are defined as, "those operations undertaken by a commander to provide early and accurate warning of enemy operations, to provide the force being protected (agencies and Iraqis) with time and maneuver space within which to react to the enemy (insurgents and public perceptions), and develop the situation to allow the commander (provisional government) to effectively use the protected force. . . .Security operations are shaping, not decisive."[7]

The Battle Command Training Program observations at mission rehearsal exercises for units going to Iraq found two principal issues with division level PIRs: most commands maintained a set of static, "steady state" PIR which remained the same for their entire rotation and the PIR were too vague to ever be answered.[8] FM 3-07, Stability Operations and Support Operations acknowledges that PIRs in stability operations differ from those in offensive or defensive operations. In two short paragraphs it talks about the incorporation of people and culture into PIRs as well as the PIR cycle that exists in conventional operations.[9] This conventional cycle results in PIR satisfaction followed by actions that lead to enemy destruction. In stability operations, the same PIR may remain in effect as long as the mission requires and the actions that result rarely appear decisive. Rather, they are part of a long line of disruptive, shaping operations.

By examining the PIR in use in Iraq one can see their permanent nature. During the first three years in Iraq, the U.S. division level commands had four generic PIRs in common:

1. When, where, and how will insurgents conduct attacks against Coalition or government forces.

2. When, where, and how will insurgents conduct attacks against critical infrastructure?

3. Who are the emerging threats to government and religious leaders?

4. Who is conducting improvised explosive devices attacks and where will they occur?

When we compare these PIR to the standards listed earlier, they miss the mark. Most of these PIRs ask several questions, are not associated with specific events, are not tied to LTIOV, and do not support a specific decision based upon current COAs. Simply put, they fail to meet the standards set forth in our doctrine.

We don't fare better at brigade level. The Center for Army Lessons Learned (CALL) concluded the following concerning Stryker Brigade PIR in Iraq:

"The nature of the commander's Priority Intelligence Requirements (PIR) in stability operations often do not lend themselves to ever being more then partially answered. Static PIR and other information requirements for current operations are valid but distinctly different information requirements. Doctrine should recognize and distinguish the simultaneous existence of short term and long term (permanent) PIR in a stability operation and support operation environment."[10]

"Steady State" Versus "Operational" PIR

Some units in Iraq are using two sets of PIRs, "steady state" or permanent PIR and "operational PIR" focused on discrete events or operations. The "steady state" PIR provide broad indicators that something is out of the ordinary.[11] This is akin to the Department of Department indications and warning methodology which combines vast numbers of indicators to provide early warning about enemy actions. Such a methodology is useful in Iraq in keeping the commander aware of imminent hostilities but does little to facilitate decision making. The "operational PIR" focus on specific events and predicted enemy actions. Thus they lose their value once the event is over and a decision is no longer required. These facilitate decision making and are true PIR.

Our doctrine doesn't support permanent PIR, or even permanent operations. Our planning is based upon a sequence of actions—COA that lead to accomplishment of a mission. Decision making is the selection of the best course of action to accomplish that mission. Mission success is defined by the criteria laid out by the commander in his intent with respect to enemy, terrain, and desired end state. The mission is nested with the missions of higher, lower, and adjacent units. Actions between these units are coordinated and synchronized with options, accounting for variables, expressed as COAs. PIR support the decisions about courses of action throughout the sequence. Sequence, actions, enemy, terrain, and endstate with decisions throughout, these imply that we have the initiative and are moving toward conditions that we have defined. It is easy to see these things—they are almost intuitive—in the mechanized drive to Baghdad. They are hazy or even non-existent on the streets of Tikrit a year later. Our doctrine is based upon an underlying assumption that decision making is fleeting—that a plan has a short life cycle. That isn't usually the case in SRO in which the mission may remain constant during the entire rotation. SRO do not have an obvious life cycle. The endstate may be very ambiguous or may not even be known. The endstate may be ambiguous by design so as to not marginalize or disenfranchise any of the parties involved. Change of mission often means redeployment, not mission accomplishment.

Should our decision making doctrine specifically focus on permanent operations, particularly in SRO? An easy reaction would be to call for a rewrite of doctrine. However, our doctrine is robust and flexible enough already to address any required permanency. We have to be savvy enough to recognize the true problems we are facing rather than just reacting to the symptoms that are more readily apparent. The Army cultural view of stability operations has been so narrow as to inhibit our analysis and planning. The term stability implies a temporary fix, a bandage. The military stabilizes a society much like an emergency medical technician (EMT) stabilizes a patient with punctured artery. The technician keeps the patient viable by stopping the bleeding until a surgeon can repair the artery; the military stabilizes the environment until governmental and non-governmental agencies and organizations can treat the society. Neither the technician nor the military are the decisive part of the operation; they shape for the decisive follow on effort performed by the surgeon and agencies.

We are generally comfortable playing this role. However, unlike a conventional EMT who leaves his patient at the emergency room door, the stability EMT must assist the surgeon throughout the operation and even the recovery period. This is because we are doing more than the just stabilizing; we are also reconstructing. The military is not an EMT, it is more than that. It is a nurse or physician's assistant who can take the patient from stabilization through the operation and onto physical therapy while being prepared to perform minor surgery along the way. A failure to accept this supporting but unglamorous role has resulted in a concentration on stability operations at the expense of reconstruction operations—and our operations reflect this from insufficient tasks to inadequate PIR. To overcome this myopia we have deliberately renamed stability operations as stability and reconstruction operations. It will take more than a name change to get this right but we are moving in the correct direction.

Decisive Operations

We have to change our planning to properly address the decisive portion of reconstruction operation. Our current planning efforts often fail to identify the decisive operation which results in PIRs focused on shaping efforts and a plan that lacks decisions. What is decisive in Iraq? Units at battalion and below levels may actually have a decisive operation that is solely security. However, if we truly examine the complexities of the mission, the decisive operation is probably something greater than security at brigade and higher levels. The decisive operation is probably the establishment of local governance which means that the decisive element in a brigade formation may be the Civil Affairs element with all other units shaping and supporting. That's a bitter pill to swallow in a warrior culture.

Understanding what is decisive in SRO is no small matter. If we don't properly identify the problem then solving it will be serendipitous. That's not the way we plan operations. We develop a plan by receiving a task from higher, determining the nature of the problem, determining the essential task to solve the problem (or tasks in a phased operation), crafting a mission statement around that task, identifying the decisive operation that will accomplish the mission, and developing shaping operations that enable the decisive operation to be successful. We then develop options–COA–that describe the actions and resources needed to achieve the decisive operation in a variety of different manners. The rub in this process comes when we have to translate operational art in tactical operations.

At the operational level we develop lines of operation aimed at accomplishing an endstate. The general lines of operation in SRO are establishment of civil security, host nation security, establishment of government, the promotion of economy, and establishment of essential services.[12] Of these, the establishment of government is arguably the most important; the center of gravity supporting this is popular political support. This is operational art, but divisions, normally thought of as a tactical echelon, are having to develop campaign plans rather than tactical plans. In turn they must translate the objectives along these lines of operation into tactical mission tasks. This works fine for the security aspects of the operation, but what are the tactical mission tasks associated with infrastructure rebuilding or controlling populaces? FM 3-90, Tactics is not very helpful here. One of the most prevalent tasks conducted, Cordon and Search, is not even listed in FM 3-90. We have to go to battalion level Training Circulars to find this task spelled out.[13] The task of influencing is spelled out in information operations doctrine but not in FM 3-90. Without adequate task terms, we end up working with what we have, developing only security-related tasks supporting the lines of operation. If you look back at some of the PIR referenced earlier you will see that the divisions in Iraq recognize the importance of these lines of operation by making the protection of infrastructure and governmental entities a priority. However, the associated PIRs are aimed at protecting, not creating these endeavors or measuring the effectiveness of actions creating these endeavors.

Let's look at establishment of governance in a stability operation. In this example we will assume that local elections are set in June. We will have some objective in our plan related to these elections. Should that objective be the election of viable local government or only that we set the conditions for a successful election to take place? If we choose the latter, then the actual outcome of elections is irrelevant. However, if the elections don't produce a viable government they are a failure and we ultimately end up redoing them, or somehow modifying the results, until we achieve success. Therefore, whether we choose to admit it or not, the objective is the election of viable local government. The basic PIR used in Iraq covering this objective is, "Who are the emerging threats to government and religious leaders?" This causes us to build a set of indicators and requirements aimed at predicting attacks against key buildings and leaders. This is a prudent measure but not one that supports the true scope of the mission which involves not only protecting the existing government but, more importantly, rebuilding it. As part of this mission we will conduct security operations which are an inherent part of every operation. Security operations are also shaping operations by our doctrine. So why do we have to have a PIR supporting a shaping operation? How about a PIR that supports the decisive operation, "Will local elections in B'aqubah in June result in the establishment of an effective city government?" This forces us to look at likely scenarios and COAs that will disrupt or defeat the elections as well as election results that may nullify the new government's ability to govern. In the process we identify the primary adversaries, their capabilities and methods of influence or attack, and indicators that these activities are taking place. These become the basis for the Specific Information Requirements (SIRs) that we need collected and analyzed. Some of these indicators, or groups of them, may result in different actions being taken by our force to remain on plan–decisions. Embedded in the SIRs will be potential targets for influence or attack; they are part of the question but not the focus of the question. In this process we also identify critical components that require protection like political figures or polling places. Security isn't left out, rather it's built into the fabric of a larger tapestry.

Failure to focus on the most important aspect of the operation, the reconstruction part and all that entails, causes the plan to be devoid of decisions. It becomes a series of rapid targeting operations reacting to enemy actions in the nick of time. We deceive ourselves into believing we are on plan and have the initiative because we are often reacting faster than the enemy can carry out his planned operations. He's got the drop on us; he has the initiative, but we still shoot, move, and communicate faster. We are that good, but we could be better. If you are off plan you have probably lost the initiative. To be on plan you need to first have a plan and that plan needs to be more than looking for bad guys. It needs sequenced actions and objectives. It considers enemy actions that will block those objectives or cause us to draw off necessary resources to react to him. These key events drive decisions with PIRs associated with them. We should be forcing the enemy to constantly adjust his plan based upon the objectives toward which we are driving.

The good news is that we are getting better. Within the last year the focus of PIRs has shifted from the object of attacks to the effects of these attacks. No longer do most of the divisions ask about attacks directed against Coalition and police forces; rather they ask about attacks designed to upset the ability of forces to control a given area or conduct transfer of authority at a given time. They are beginning to focus on the effects that the enemy is trying to achieve and their impact on our long term operations. In this manner, we are beginning to make the linkage between our objectives and the decisions we need to make–between what is decisive and what is shaping.

Conclusion

PIRs facilitate decision making. That's what our doctrine tells us and our doctrine is sound. The problem occurs in the application of that doctrine in SRO because we consistently select security as decisive instead of the less glamorous mission of establishing governance or other aspects of reconstruction. Since we are security centric, with long term plans that are repetitive and largely devoid of decisions, we end up operating from a list of "steady state" PIR which are actually IR. This is further compounded by the doctrinal shortcoming of few tactical mission tasks associated with SRO. We need to identify and codify these tasks in order to make the leap from operational art to tactical operations understand and achievable. Once we have properly identified the decisive operation we will be able to identify the decisions along the way and the PIRs required to answer the key questions associated with those decisions. The doctrine requires a few modifications but is pretty sound in principle. We need to put PIRs and decision making back into our operations.

Endnotes

1. Dictionary of Military and Associated Terms, Department of Defense (Washington D.C: amended 2005), 425.

2. FM 6-0, Mission Command: Command and Control of Army Forces, Department of the Army (Washington D.C: 11 August 2003), B-14.

3. FM 2-0, Intelligence, 1-12.

4. FM 2-0, Intelligence, 1-11.

5. FM 1, The Army, Department of the Army (Washington D.C: 14 June 2005), 3-7.

6. *Maximillian Weber, The Theory of Social and Economic Organization,* Translated by A.M. Henderson and Talcott Parsons (Oxford University Press: 1947), 156.

7. FM 3-90, Tactics, Department of the Army (Washington D.C: July 2001), 12-0 and 12-1.

8. U.S. Army Battle Command Training Center Presentation to Center for Army Tactics, November 2004.

9. FM 3-07, Stability Operations and Support Operations, Department of the Army (Washington D.C: February 2003), 2-4 and 2-5.

10. Center for Army Lessons Learned, *Initial Impressions Report, Operations in Mosul, Iraq, 3rd Brigade, 2nd Infantry*, 21 December 2004, 67.

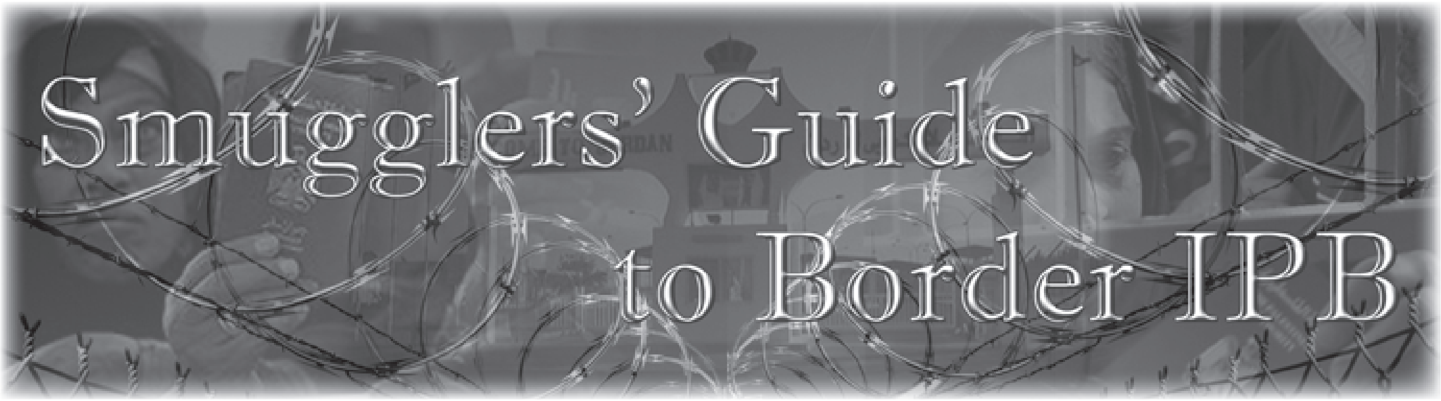
11. Major Joe Nelson, *"Do Steady State PIR work in Stability Operations and Support Operations?"* CTC Bulletin 05-15, 1st Quarter FY2005.

12. FM 3-24, Counterinsurgency (Final Electronic File), Department of the Army (Washington D.C:, Date Pending), 5-3.

13. TC 7-98-1, Stability and Support Operations Training Support Package, Department of the Army (Washington D.C: June 1997) Appendix B.

David Pierson is a retired Military Intelligence Officer currently teaching tactics at the U.S. Army Command and General Staff College. He served in a variety of tactical assignments including armor battalion S2 in Desert Storm, G2 Planner in Kosovo for KFOR 1A, and G2, Multi-National Brigade East in KFOR 4A. He also served as Company Commander, A Company, 124th MI Battalion; Executive Officer, 165th MI Battalion, and G2, 1st Infantry Division.

(Continued from page 37)



Smugglers' Guide to Border IPB

enablers combine with facilitators to allow successful breach and movement through the LOD, intelligence analysts can identify the critical decision points of the enemy in time and space, in turn setting the conditions for maneuver forces to effectively mitigate the threat. Applied as a continual process, border IPB allows for the continued influence along border areas of operations effectively denying the effort the critical advantages that borders traditionally pose.

References

FM 2-0, *Intelligence*, May 2004.

FM 3-06, *Urban Operations*, June 2003.

FM 3-06.11, *Combined Arms Operations In Urban Terrain*, February 2002.

FM 34-130, *Intelligence Preparation of the Battlefield*, July 1994.

FM 41-10 (3-05.40), *Civil Affairs Operations*, February 2000.

JP 2-01.3, *Joint TTPs for JIPB*, May 2000.

Captain Goth is currently serving as the 3-160th Special Operations Aviation Regiment (Airborne) S2, at Hunter Army Airfield, Fort Stewart, Georgia. He previously served as Chief of Operations, Joint Intelligence-Combat Training Center and as Commander, Bravo Company, 304th Military Intelligence (MI) Battalion, 111th MI Brigade at Fort Huachuca, Arizona. Captain Goth holds a BS in Political Science from Austin Peay State University and an MPA from the University of Alaska. Readers may reach Captain Goth at DSN 315-7921 or tedd.goth@us.army.mil.

Headquarters Combined Arms Center
U.S. Army Combined Arms Center
The Intellectual Center of the Army

CAC Commander's Counterinsurgency Reading List

*Indicates DC's recommendations for a "first read".
Call numbers for the books in the Combined Arms Research Library (CARL) are in bold print.

O'Neill, Bard E. **Insurgency & Terrorism: From Revolution to Apocalypse.**
Washington, D.C: Potomac Books, 2005. **CARL: 355.0218 o58i 2005**
A framework for analyzing insurgency operations and a good first book in insurgency studies.

*Galula, David. **Counterinsurgency Warfare: Theory and Practice.**
New York: Praeger, 1964. **CARL: 355.425 G181cw**
Classic summary of lessons derived form Galula's experience of insurgency and counterinsurgency in Greece, China, and Algeria.

Fall, Bernard B. **Last Reflections On a War.**
Garden City, New York: Doubleday, 1967. 428 pp. **CARL: 959.7 F194L**
Consists of Dr. Fall's unpublished materials. His analysis of Vietnam is still considered accurate.

*Kepel, Gilles. **The War for Muslim Minds: Islam and the West.**
Cambridge, Massachusetts: Belknap Press of Harvard University Press, 2004. **CARL: 297.272 K38w**
An excellent overview of the broader radical Islamic insurgency.

*Lawrence, T. E., U.S. Army Command and General Staff College, and Combat Studies Institute.
The Evolution of a Revolt. Fort Leavenworth, Kansas: Combat Studies Institute, 1989.
URL: http://cgsc.leavenworth.army.mil/carl/download/csipubs/lawrence.pdf
Lawrence's key observations on the difference between conventional and insurgency warfare.

CAC HQ, Fort Leavenworth, Kansas

Tripp, Charles. **A History of Iraq.**
Cambridge: Cambridge University Press, 2000. **CARL: 956.704 T836h 2002**
A solid single volume history of modern Iraq prior to Operation Iraqi Freedom.

West, Bing. **The Village.**
New York, New York: Pocket Books, 2003. **Carl: 959.704 W516v**
A first-person account of military advisors embedded with Vietnamese units.

Additional Resources

Asprey, Robert B. **War in the Shadows: The Guerrilla in History.**
Lincoln, Nebraska: IUniverse, 2002. **CARL: 355.02184 A843wsh** (two volumes)

An updated version of the 1975 classic that covers the history of guerrilla war from ancient Persia to modern Afghanistan.

Callwell, C. E. **Small Wars: Their Principles and Practice.**
Lincoln, Nebraska: University of Nebraska Press, 1996. **CARL: 355.0218 C163s**
A classic study of colonial warfare and small wars.

Gunaratna, Rohan. **Inside Al Qaeda: Global Network of Terror.**
New York: Columbia University Press, 2002. **CARL: 303.625 G1975i** (CARL also has 2003 paperback: **303.625 G1975ia**)
The story behind the rise of the global insurgency.

Hammes, Thomas X. **The Sling and the Stone: On War in the 21st Century.**
St. Paul, Minnesota: Zenith Press, 2004. **CARL: 355.0218 H224s 2004**
An excellent overview of what the author describes as "fourth generation warfare".

Kitson, Frank. **Low-intensity Operations: Subversion, Insurgency, Peace-keeping.**
Harrisburg: Pennsylvania: Stackpole Books, 1971. **CARL: 355.02184 K62L**
Classic explanation of the British school of counterinsurgency.

Krepinevich, Andrew F. **The Army and Vietnam.**
Baltimore: Johns Hopkins University Press, 1986. **CARL: 959.7043373 K92a**
The best volume on the U.S. Army's challenges in coming to terms with insurgency in Vietnam.

Lawrence, T. E. **Seven Pillars of Wisdom, A Triumph.**
Garden City, New York: Doubleday, Doran & Co., 1935. **CARL: 940.415 L423sp**
Autobiographical account of Lawrence's attempts to organize Arab nationalism during WW I.

Lewis, Bernard. **The Crisis of Islam: Holy War and Unholy Terror.**
New York: Modern Library, 2003. **CARL: 297.72 L673c 2003**
A controversial but important analysis of the philosophical origins of the global insurgency.

Linn, Brian M. **The Philippine War, 1899-1902.**
Lawrence: University Press of Kansas, 2000. **CARL: 959.9031 L758p**
The definitive treatment of military operations in the Philippines.

Nagl, John A. **Counterinsurgency Lessons from Malaya and Vietnam: Learning to Eat Soup with a Knife.**
Westport, Connecticut: Praeger, 2002. **CARL: 355.0218 N149c 2002**
How to learn to defeat an insurgency. Forward by CSA.

Solinas, Franco, et al. **Battle of Algiers.**
Santa Monica, California; New York, New York: Rhino; Axon Video, 1993. **CARL: H000706**
A dramatization of the conflict between Algerian nationalists and French colonialists that culminated in Algeria's independence in 1962.

Articles and Other Documents

Barnard, Daniel. **"The Great Iraqi Revolt: The 1919–20 Insurrections Against the British in Mesopotamia."**
Paper presented at the Harvard Graduate Student Conference in International History, April 23, 2004.

Cassidy, Robert M. **“Back to the Street Without Joy: Counterinsurgency Lessons from Vietnam and Other Small Wars.”**
Parameters 34 (Summer 2004): 73-83.
URL: http://carlisle-www.army.mil/usawc/Parameters/04summer/cassidy.pdf
Central Intelligence Agency. **“Iraq.”**
The World Factbook, 2006.
URL: https://www.cia.gov/cia/publications/factbook/geos/iz.html

*Chiarelli, Peter W., Patrick R. Michaelis. **“Winning the Peace: The Requirement for Full-Spectrum Operations.”** Military Review 85 (July-August 2005): 4-17.
URL: http://www.army.mil/professionalwriting/volumes/volume3/october_2005/10_05_2.html

Cockburn, Andrew. **“Iraq's Oppressed Majority.”**
Smithsonian (December 2003): 98-105.
URL: http://www.smithsonianmag.com/issues/2003/december/oppressed.php
Hashim, Ahmed S. **“The Insurgency in Iraq.”**
Small Wars & Insurgencies. 14 (Autumn 2003): 1-22. **CARL: Journals, 1st Floor**

Hoffman, Bruce. **Insurgency and Counterinsurgency in Iraq.**
Santa Monica, California: RAND, National Security Research Division, 2004.
URL: http://www.rand.org/pubs/occasional_papers/OP127/index.html

Kandell, Jonathan. **“Iraq's Unruly Century.”**Smithsonian 34 (May 2003): 44-51.
URL: http://www.smithsonianmag.com/issues/2003/may/unruly.php

Maass, Peter. **“The Salvadorization of Iraq?”**
The New York Times Magazine. May 1, 2005.
URL: http://www.petermaass.com/core.cfm?p=1&mag=123&magtype=1

Maass, Peter. **“The Counterinsurgent.”**
The New York Times Magazine. January 11, 2004.
URL: http://www.petermaass.com/core.cfm?p=1&mag=120&magtype=1

McFate, Montgomery. **“Iraq: The Social Context of IEDs.”**
Military Review 85, no. 3.
URL: http://www.au.af.mil/au/awc/awcgate/milreview/mcfate3.pdf

Metz, Steven. **“Insurgency and Counterinsurgency in Iraq.”**
Washington Quarterly 27 (Winter 2004): 25-36. **CARL: Journals, 1st Floor**
URL: http://www.twq.com/04winter/docs/04winter_metz.pdf

Milton-Edwards, Beverley. **“Iraq, Past, Present and Future: A Thoroughly-Modern Mandate?”**
History & Policy, (MAY 2003).
URL: http://www.historyandpolicy.org/archive/policy-paper-13.html

Nasr, Vali. **“Regional Implications of Shi'a Revival in Iraq”**
Washington Quarterly 27 (Summer 2004): 7-24. **CARL: Journals, 1st Floor**
URL: http://www.twq.com/04summer/docs/04summer_nasr.pdf

Record, Jeffrey and W. A. Terrill. **Iraq and Vietnam: Differences, Similarities, and Insights**
Carlisle Barracks, Pennsylvania: Strategic Studies Institute, U.S. Army War College, 2004. **CARL: 355.033573 R311i**
URL: http://handle.dtic.mil/100.2/ADA423779

*Sepp, Kalev I. **"Best Practices in Counterinsurgency."**
Military Review 85 (May-June 2005): 8-12.
URL: http://www.au.af.mil/au/awc/awcgate/milreview/sepp.pdf

Tomes, Robert R. **"Relearning Counterinsurgency Warfare."**
Parameters 34 (Spring 2004): 16-28.
URL: http://carlisle-www.army.mil/usawc/Parameters/04spring/tomes.pdf

Military References

Army publications that are assigned a Marine Corps number are indicated with an asterisk.

*FM 1-02/MCRP 5-12A. *Operational Terms and Graphics.* 21 Sep 2004.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 4 Dec 2001. (DOD Dictionary of Military Terms Web site < http://www.dtic.mil/doctrine/jel/doddict/ >)

CJCSI 3121.01B. *Standing Rules of Engagement for U.S. Forces*. 15 Jan 2000.

DODD 2310.01E. *The Department of Defense Detainee Program*. 5 Sep 2006.

DODD 5105.38M. *Security Assistance Management Manual.* 3 Oct 2003. (Published by the Defense Security Cooperation Agency. Chapter 8 addresses end-use monitoring. AR 12-1 implements for the Army.)

JP 1. *Joint Warfare of the Armed Forces of the United States.* 14 Nov 2000.

JP 3-0. *Joint Operations.* 17 Sep 2006.

JP 3-07.1. *Joint Tactics, Techniques, and Procedures for Foreign Internal Defense.* 30 Apr 2004.

JP 3-08. *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations.* 2 vols. 17 Mar 2006.

JP 3-60. *Joint Doctrine for Targeting*. 17 Jan 2002.

JP 3-13. *Information Operations.* 13 Feb 2006.

JP 3-61. *Public Affairs.* 9 May 2005.

AR 12-1. *Security Assistance, International Logistics, Training, and Technical Assistance Support Policy and Responsibilities.* 24 Jan 2000. (Marine Corps follows DODD 5105.38M.)

*AR 190-8/MCO 3461.1. *Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees.* 1 Oct 1997.

FM 2-0 (34-1). *Intelligence*. 17 May 2004.

FM 2-22.3 (34-52). *Human Intelligence Collector Operations.* 6 Sep 2006. (See MarAdmin 458.06 for Marine Corps policy and guidance on intelligence interrogations.)

FM 3-0. *Operations.* 14 Jun 2001. (Under revision. Projected for republication during fiscal year 2007.)

FM 3-05 (100-25), *Army Special Operations Forces*. 20 Sep 2006.

FM 3-05.40 (41-10). *Civil Affairs Operations.* 29 Sep 2006. (MCRP 3-33.1 contains Marine Corps civil affairs doctrine.)

*FM 3-05.301/MCRP 3-40.6A. *Psychological Operations Tactics, Techniques, and Procedures*. 31 Dec 2003. (Distribution limited to government agencies only.)

*FM 3-05.401/MCRP 3-33.1A. *Civil Affairs Tactics, Techniques, and Procedures.* 23 Sep 2003.

*FM 3-09.31 (6-71)/MCRP 3-16C. *Tactics, Techniques, and Procedures for Fire Support for the Combined Arms Commander.* 1 Oct 2002.

FM 3-13 (100-6). *Information Operations: Doctrine, Tactics, Techniques, and Procedures.* 28 Nov 2003. (Appendix E addresses information operations targeting.)

FM 3-61.1. *Public Affairs Tactics, Techniques, and Procedures.* 1 Oct 2000.

FM 3-90. *Tactics*. 4 Jul 2001.

FM 4-0 (100-10). *Combat Service Support.* 29 Aug 2003.

FM 4-02 (8-10). *Force Health Protection in a Global Environment.* 13 Feb 2003. (NAVMED P-117, chapter 19, contains corresponding Marine Corps doctrine.)

FM 5-0 (101-5). *Army Planning and Orders Production.* 20 Jan 2005. (MCDP 5 contains Marine Corps planning doctrine.)

FM 5-104. *General Engineering.* 12 Nov 1986. (Will be republished as FM 3-34.300.)

FM 5-250. *Explosives and Demolitions. 30 Jul 1998.* (Will be republished as FM 3-34.214.)

FM 6-0. *Mission Command: Command and Control of Army Forces.* 11 Aug 2003.

FM 6-20-10. *Tactics, Techniques, and Procedures for the Targeting Process.* 8 May 1996.

FM 6-22 (22-100). *Army Leadership*.12 Oct 2006.

*FM 6-22.5 (22-9)/MCRP 6-11C. *Combat Stress.* 23 Jun 2000.

FM 7-98. *Operations in a Low-Intensity Conflict*. 19 Oct 1992. (Contains tactical-level guidance for brigade and battalion operations in an irregular warfare and peace operations environment.)

FM 20-32. *Mine/Countermine Operations.* 29 May 1998. (Will be republished as FM 3-34.210, *Explosive Hazards Operations*.)

FM 27-10. *The Law of Land Warfare.* 18 Jul 1956.

FM 31-20-3. *Foreign Internal Defense: Tactics, Techniques, and Procedures for Special Forces*. 20 Sep 1994. (Will be republished as FM 3-05.202.)

*FM 34-130/FMFRP 3-23-2. *Intelligence Preparation of the Battlefield.* 8 Jul 1994. (Will be republished as FM 2-01.3/MRCP 2-3A.)

FM 46-1. *Public Affairs Operations.* 30 May 1997.

FM 90-8. *Counterguerrilla Operations*. 29 Aug 1986.

FMI 2-91.4. *Intelligence Support to Operations in the Urban Environment.* 30 Jun 2005. (Expires 30 Jun 2007. Distribution limited to government agencies only. Available in electronic media only. Army Doctrine and Training Digital Library Web site < www.adtdl.army.mil >).

*FMI 3-34.119/MCIP 3-17.01. *Improved Explosive Device Defeat.* 21 Sep 2005. (Expires 21 Sep 2007. Distribution limited to government agencies only. Available in electronic media only. Army Doctrine and Training Digital Library Web site < www.adtdl.army.mil >.)

FMI 5-0.1. *The Operations Process.* 31 Mar 2006. (Expires 31 Mar 2008. When FM 3-0 is republished, it will address the material in FMI 5-0.1 that is relevant to this publication.)

MarAdmin (Marine Administrative Message) 458/06. "USMC Interim Policy and Guidance for Intelligence Interrogations." 22 Sep 2006. (States that FM 2-22.3 provides DOD-wide doctrine on intelligence interrogations. Lists sections of FM 2-22.33 that apply. Marine Corps Publications Web site < http://www.usmc.mil/maradmins/ >.)

MCDP 1. *Warfighting.* 20 Jun 1997.

MCDP 4. *Logistics.* 21 Feb 1997.

MCDP 5. *Planning.* 21 July 1997.

MCDP 6. *Command and Control.* 4 Oct 1996.

MCRP 3-33.1A. *Civil Affairs Operations.* 14 Feb 2000. (FM 3-05.40 contains Army civil affairs doctrine.)

MCWP 4-12. *Operational-Level Logistics.* 30 Jan 2002.

NAVMED P-117. *Manual of the Medical Department, U.S. Navy. Chapter 19, "Fleet Marine Force," change 117. 21 Jun 2001. (Article 19-24 discusses levels of care. FM 4-02 contains the corresponding Army doctrine. When published, MCRP 4-11.1G will supersede this publication.)*

Intelligence and Electronic Warfare
Tactical Proficiency Trainer (IEWTPT)

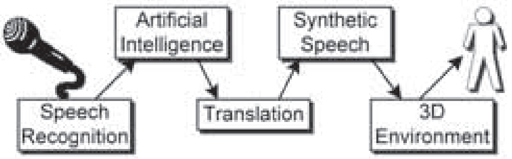
HUMINT Control Cell

The IEWTPT Human Intelligence (HUMINT) Control Cell (HCC) is the Army's latest sustainment trainer for HUMINT Collectors.

The HCC provides additional HUMINT training tools that are hard to replicate with the current training capabilities.

- Scenarios address current HUMINT issues that are specific to the regions they are based in.
- The immersive environment allows the Soldier to engage in a realistic setting with virtual humans that have appearances and mannerisms accurate to the culture in the scenario.
- The use of an interpreter and specific language translations allows the HUMINT Soldier to train using the languages that are used in the real world environment.

The HCC is comprised of the latest technological advancements in speech recognition, speech synthesis, and artificial intelligence.

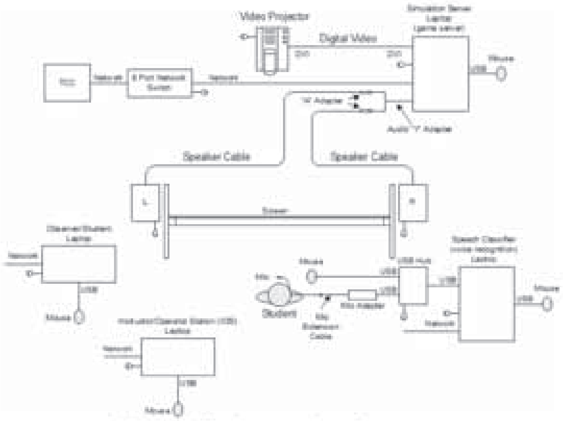


The HUMINT Collector interacts with a life size 3D character avatar (Virtual Human) rendered by a Commercial Off the Shelf (COTS) Video Game Engine. The Collector engages in free flowing conversation with the Virtual Human which is converted to text using speech recognition. The Virtual Interpreter translates the statement to the Virtual Human. The artificial intelligence component analyzes the statement and determines a response, which is then outputted from the Virtual Human. The Virtual Interpreter translates the response to English and relays it to the HUMINT Collector.

IEWTPT Enables Embedded Training

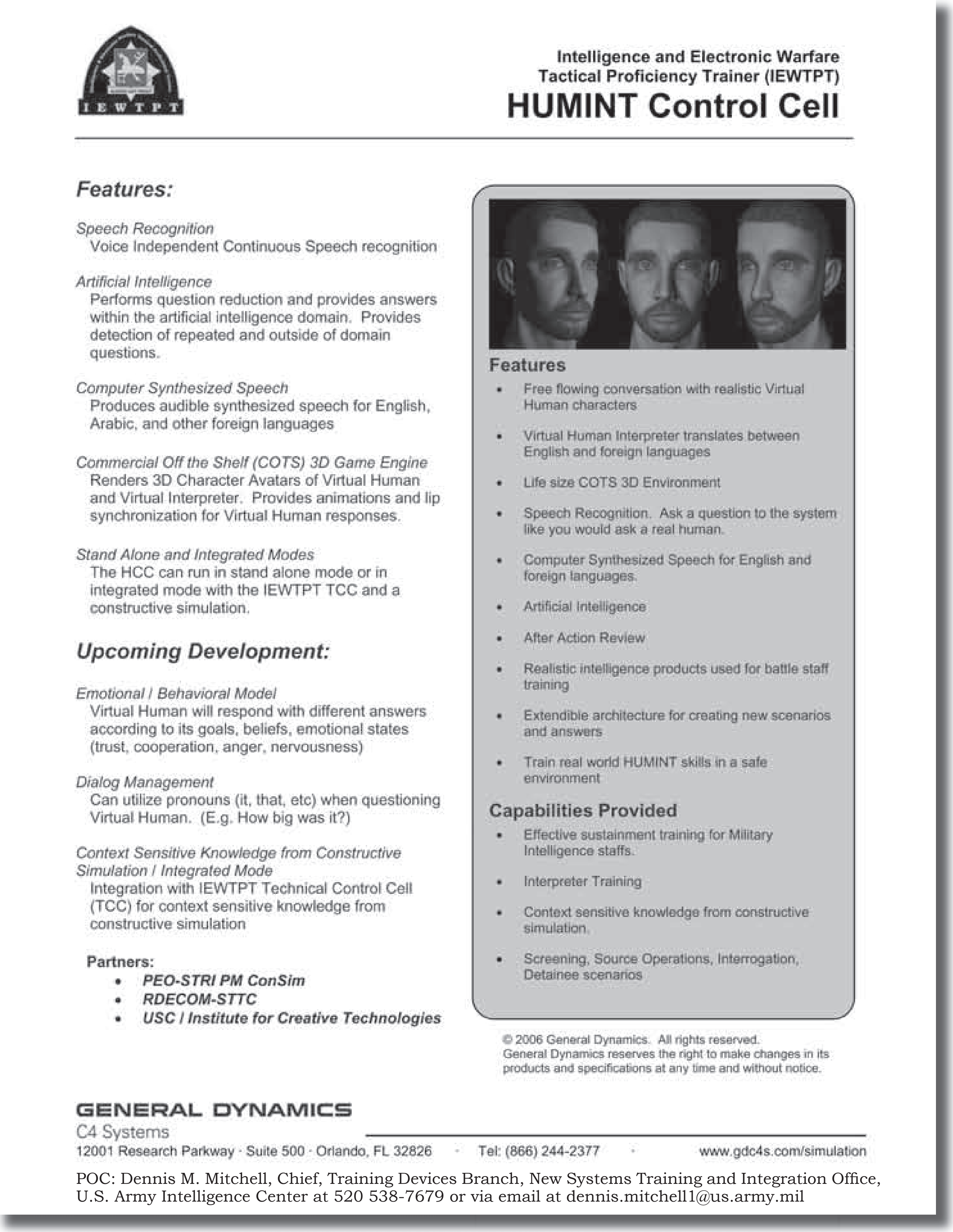
Virtual Human and Virtual Arabic Interpreter

The HUMINT Collector gathers intelligence information from the Virtual Human, while a HUMINT Instructor monitors the student's performance. At the end of the tactical questioning, the HUMINT Collector reviews After Action Review Statistics as well as HUMINT Instructor comments.



HCC Fully Immersive System

GENERAL DYNAMICS
C4 Systems
12001 Research Parkway · Suite 500 · Orlando, FL 32826 · Tel: (866) 244-2377 · www.gdc4s.com/simulation



Intelligence and Electronic Warfare
Tactical Proficiency Trainer (IEWTPT)

HUMINT Control Cell

Features:

Speech Recognition
Voice Independent Continuous Speech recognition

Artificial Intelligence
Performs question reduction and provides answers within the artificial intelligence domain. Provides detection of repeated and outside of domain questions.

Computer Synthesized Speech
Produces audible synthesized speech for English, Arabic, and other foreign languages

Commercial Off the Shelf (COTS) 3D Game Engine
Renders 3D Character Avatars of Virtual Human and Virtual Interpreter. Provides animations and lip synchronization for Virtual Human responses.

Stand Alone and Integrated Modes
The HCC can run in stand alone mode or in integrated mode with the IEWTPT TCC and a constructive simulation.

Upcoming Development:

Emotional / Behavioral Model
Virtual Human will respond with different answers according to its goals, beliefs, emotional states (trust, cooperation, anger, nervousness)

Dialog Management
Can utilize pronouns (it, that, etc) when questioning Virtual Human. (E.g. How big was it?)

Context Sensitive Knowledge from Constructive Simulation / Integrated Mode
Integration with IEWTPT Technical Control Cell (TCC) for context sensitive knowledge from constructive simulation

Partners:
- ***PEO-STRI PM ConSim***
- ***RDECOM-STTC***
- ***USC / Institute for Creative Technologies***

Features
- Free flowing conversation with realistic Virtual Human characters
- Virtual Human Interpreter translates between English and foreign languages
- Life size COTS 3D Environment
- Speech Recognition. Ask a question to the system like you would ask a real human.
- Computer Synthesized Speech for English and foreign languages.
- Artificial Intelligence
- After Action Review
- Realistic intelligence products used for battle staff training
- Extendible architecture for creating new scenarios and answers
- Train real world HUMINT skills in a safe environment

Capabilities Provided
- Effective sustainment training for Military Intelligence staffs.
- Interpreter Training
- Context sensitive knowledge from constructive simulation.
- Screening, Source Operations, Interrogation, Detainee scenarios

GENERAL DYNAMICS
C4 Systems
12001 Research Parkway · Suite 500 · Orlando, FL 32826 · Tel: (866) 244-2377 · www.gdc4s.com/simulation

POC: Dennis M. Mitchell, Chief, Training Devices Branch, New Systems Training and Integration Office, U.S. Army Intelligence Center at 520 538-7679 or via email at dennis.mitchell1@us.army.mil

ARMY G2 IT

Note to the Field—December 2006

Lynn Schnurr, Army G2 IC CIO

Introduction

Hello Army G2s–The Phantom Corps has successfully transitioned with V Corps as the Multi-National Corps-Iraq C2 element and in Afghanistan, 82nd Abn Div is getting ready to transition with 10th Mnt Div. We wish all the incoming units a safe and productive year and thank the departing units for their significant contributions to the war effort.

This month's note to the field will cover a couple of important subjects. The first, Multi-Level Security, is written by Dr. Randy Garrett, Science Advisor for Army G2 and INSCOM. In it, Dr. Garrett addresses the current state of cross domain security and a project undertaken by INSCOM with the support of USD(I), NSA, DIA, and the Army G2 to prototype a true multi-level security environment over the next year—this is exciting work and has the potential for huge benefits to the Warfighter.

A second article is from the schoolhouse and focuses on master analyst training. This is extremely important if your unit is slated to deploy in FY08 or beyond or is in the works to get a DCGS-A garrison training set. The "embedded mentor" program, while highly successful, was a temporary program to ease the DCGS-A Quick Reaction Capability formerly known as JIOC-I into operations while Soldiers were fighting a War. Mentors will be phased out in FY07 and replaced by unit Soldiers trained on DCGS-A. We strongly encourage G2s, S2s, ACE Chiefs, and their Commanders to get at least one high-speed NCO or Warrant Officer per unit into this training over the coming year.

Lastly, this month's note provides an update on a handheld biometric device, aka HIIDE, and an article on new linguist contracts.

Sincerest regards. Lynn Schnurr, Army G2 Intel CIO.

Multi-Level Security

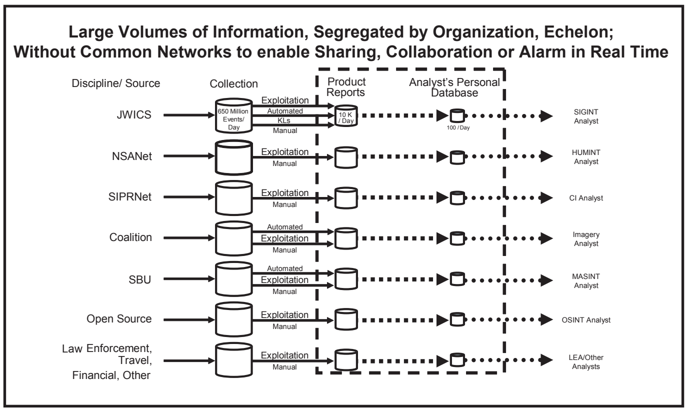
by Dr. Randy Garrett, Senior Science Advisor, Army Intelligence

Providing multi-level security on a single system has proven to be a decades long challenge. (Multi-level security means that the same computer system contains unclassified, secret, top secret, and SCI data, but maintains accredited access control so that users of the system are only able to access data for which they are authorized). As far back as mid-1960's, the Multics project was created to provide multiple security levels. Although Multics was not widely adopted, a smaller descendant has enjoyed some success. In a play on words, the successor was named Unix. Although widely used, Unix does NOT provide multi-level security.

The current state-of-the-practice is to have multiple LEVELS of security. The distinction is that each security level has its own physically discrete and separate computer system with some form of tightly controlled gateway between the levels.

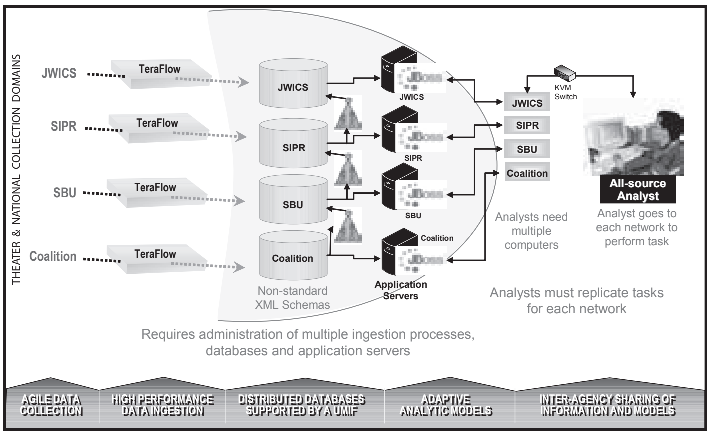
For example, many people have separate NIPR, SIPR, and JWICS computers with a device to switch the keyboard, mouse, and monitor between them. The only "gateway" between these security levels is an approved physical medium, such as a CD-ROM.

A more sophisticated system has different security levels on the same monitor, at the same time, but each level is isolated to a different window. It may or may not be possible to "cut and paste" between windows at different security levels. The DoDIIS Trusted Workstation (DTW) is an example. The graphic below illustrates the way most analysts currently operate.



Pre-JIOC-I (Plus most of the IC community today).

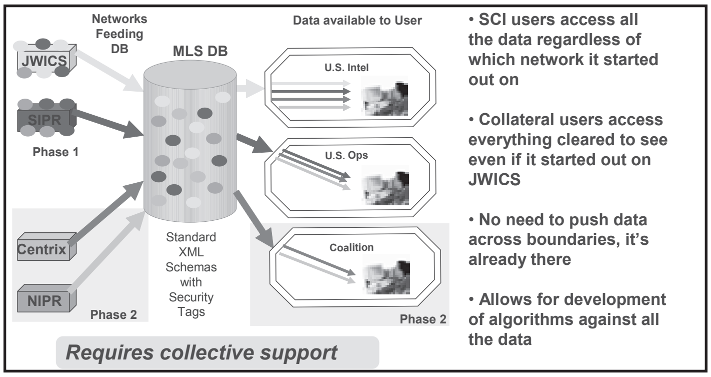
Each of the previous forms of multiple levels of security was intended for use by human beings. Cross Domain Solutions (CDS), colloquially called "guards," provide a means for bridging security levels for computer-to-computer. Some guards guarantee security by using one-way links. In these systems, it is physically impossible for the data to flow in more than one direction across the link (typically from low systems to high, such as SIPR to JWICS). An example is the TRUCE. Other guards tightly control the interface, only allowing the transfer of strictly formatted data that is carefully checked. Examples of this type of guard are ISSE and RADIANT MERCURY. The JIOC-I, now DCGS-A, system employs all three of these guards to allow data to move, in a very controlled and accredited fashion, between the differing security levels, facilitating a flat analytic network.


THEATER & NATIONAL COLLECTION DOMAINS
JWICS
SIPR
SBU
Coalition
TeraFlow
TeraFlow
TeraFlow
TeraFlow
JWICS
SIPR
SBU
Coalition
Non-standard XML Schemas
JWICS
SIPR
SBU
Coalition
Application Servers
KVM Switch
JWICS
SIPR
SBU
Coalition
Analysts need multiple computers
All-source Analyst
Analyst goes to each network to perform task
Analysts must replicate tasks for each network
Requires administration of multiple ingestion processes, databases and application servers
AGILE DATA COLLECTION
HIGH PERFORMANCE DATA INGESTION
DISTRIBUTED DATABASES SUPPORTED BY A UMIF
ADAPTIVE ANALYTIC MODELS
INTER-AGENCY SHARING OF INFORMATION AND MODELS

JIOC-I Today.

We have recently begun a project, in conjunction with DIA and DNI, to create a true multi-level secure database. Different networks would no longer have completely separate computer systems. Instead, one database would be connected to multiple networks (for example, SIPR and JWICS) simultaneously. The operational benefit, in addition to a smaller physical footprint and reduced maintenance, is that SIPR users would not only see Secret and Unclassified information that came from SIPR, they would also see Secret and Unclassified information that came from JWICS.

The ultimate goal would be supporting Coalition. In this case, appropriately authorized foreign users would get all data that was not marked NOFORN or that was explicitly marked as releasable, regardless of which network it originated on. For now, Coalition support is only in the earliest conceptual stages.



- SCI users access all the data regardless of which network it started out on
- Collateral users access everything cleared to see even if it started out on JWICS
- No need to push data across boundaries, it's already there
- Allows for development of algorithms against all the data

Future: Flatten the Network–MLS.

We will spend the next year developing a prototype database, ingesting all levels of classified data, and enabling computers from multiple networks to connect to the database in the test environment. This is more than a science project though. If successful, we hope to instantiate this in CY08 as a flat network DCGS-A brain in an operational environment.

Master Analyst Training

by SFC Wayne Voss, USAIC

The All Source Analysis System (ASAS) Master Analyst Course (AMAC), 3A-F71/232-ASI1F has been replaced with the Intelligence Master Analyst Course (IMAC). The course number will remain the same for the foreseeable future. Even though AMAC had a long run and served the intelligence community well, it was time to update it to embrace the newest automation systems. The IMAC is structured similar to the old AMAC, but with emphasis on analytical skills and exploiting the Distributed Common Ground System-Army (DCGS-A).

The goal of the IMAC is to produce a network savvy Master Analyst that embodies the virtues of being an Analyst, Trainer, and Troubleshooter. The IMAC is currently nine weeks long, taught three times a year at the United States Army Intelligence Center (USAIC) at Fort Huachuca, AZ. IMAC provides extensive training on the multiple facets and methodologies of intelligence analysis and critical thinking. Systems training is not ignored within the IMAC; over five weeks are dedicated to integrating and leveraging the many layers and applications of the DCGS-A. The IMAC is available for all Military Intelligence Analysts, grades E5 through E7 and W01 through CW3. Personnel in the grade of E4(P) will be granted a waiver based on operational need and a memorandum of endorsement signed by the first O5 in their chain of command.

The Intelligence Workstation Certification Course (IWCC), 3A-F86/243-F33 is designed to continue where Instructor and Key Personnel Training (IKPT) or New Equipment Training (NET) have left off. The IWCC provides a basic/intermediate training alternative to meet the commander's immediate training needs. IWCC is three weeks long and is taught eight times a year at the USAIC. The goal of IWCC is to train analysts to leverage DCGS-A in a meaningful manner. Main threads of DCGS-A training includes ARC-GIS/CJMTK, Pathfinder/Analyst Notebook, and Query Tree NG.

The IMAC and IWCC are managed by the Intelligence Master Analyst Branch (IMAB). The IMAB is responsible for developing all pertinent course training materials, supports sustainable training for Master Analysts, manages the Master Analyst tracking program, and provides mobile training teams as appropriate. Additional information about IMAC and IWCC can be accessed through the USAIC ICON portal at icon.army.mil, or by contacting SFC (P) Wayne J. Voss, wayne.voss@us.army.mil, or Mr. Matthew J. Nunn, matthew.nunn@us.army.mil.

COURSE SCHEDULES FOR FY07

IMAC (3A-F71/232-ASI1F)

✦ IMAC 07-001	—	16 Oct–18 Dec 06
✦ IMAC 07-002	—	26 Mar–24 May 07
✦ IMAC 07-003	—	09 Jul–07 Sep 07

IWCC (3A-F86/243-F33)

✦ IWCC 07-001	—	30 Oct–20 Nov 06
✦ IWCC 07-002	—	08 Jan–29 Jan 07
✦ IWCC 07-003	—	05 Feb–26 Feb 07
✦ IWCC 07-004	—	05 Mar–23 Mar 07
✦ IWCC 07-005	—	09 Apr–27 Apr 07
✦ IWCC 07-006	—	11 Jun–29 Jun 07
✦ IWCC 07-007	—	23 Jul–10 Aug 07
✦ IWCC 07-008	—	10 Sep–28 Sep 07

Handheld Interagency Identity Detection Equipment (HIIDE) CONOPs, Fielding and Training

by Mr. Jerry Jackson, EIT, Principal Senior Systems Analyst, DCS G2

Providing identification of individuals encountered during the course of tactical operations has taken on an entirely new meaning in the Counterinsurgency operations of OIF and OEF. While US forces once had the latitude to detain large numbers of individuals in the vicinity of IED, sniper or other incidents and take any time necessary to determine their identity, the current operational and political environment does not allows such flexibility. Compounded by the enemy's progressive learning curve at concealing their true identities, the need for a fast yet reliable method of ascertaining the true identity of individuals encountered has become critical to successfully removing known insurgents from the battlefield.

In response to the Mosul Dining Facility bombing, the U.S. Department of Defense fielded the Biometric Identification System for Access (BISA) to ten primary sites throughout Iraq. Utilizing VSAT communications links, these systems provide a method for collecting the biometrics (fingerprints, iris images, face photo, personal data, etc) from individuals who request base access to US and coalition facilities and transmit that data back to a single authorized DoD repository in West Virginia where it is vetted against all collected DoD data and then vetted against the extensive FBI fingerprint database. Prior to the BISA fielding, the Army G2 recognized that the ability to tie an individual to his true biometric identity and link all available intelligence products and analysis related to that individual through that identity, would be critical in streamlining interrogation and intelligence analysis activities. Without a system to build knowledge records and tie that information to a specific individual, multiple analysts could be working to compile information on the same individual based on RFIs or incidents that occur at different times and locations with each piece of analysis perhaps being stored in a different database for each. To solve this problem, the Army G2 through the efforts of the Language Technology Office (LTO) at Ft Huachuca, became an advocate for the Biometric Automated Toolset or "BAT." The BAT system provides users with the ability to positively identify individuals based on the immutable biometrics they present (Fingerprints, iris and face). With now more than 850 systems deployed, BAT was the first multimodal system that can identify individuals with greater certainty based on the combination of multiple biometric signatures. Rather than the simple "fact of a match" afforded by other biometric systems, the BAT provides any relevant "so what" information that could assist the user to better determine the disposition of the encountered individual.

The HIIDE

The BAT system, while considered a portable system, is not conducive to use in mobile tactical operations. It includes a Panasonic Toughbook Laptop computer paired with a Canon face camera, optical rolled or slap fingerprint sensor and a Pier 2.3 Iris collection device each connected to the laptop by various cables. The BAT systems require several minutes for set up and tear down, a limitation that caused Soldiers to detain individuals and bring them back to where a BAT or other biometric system was already set up so they could be positively identified. This effort would require significant extra time and personnel resources often resulting in all the individuals detained being released once identified as non-hostiles. The answer to this problem, as advocated by the Army G2, is the Handheld Interagency Identity Detection Equipment or "HIIDE".

The HIIDE is a powerful for biometric identification and represents a true tactical extension of the BAT system. Users can enroll, match or verify with the three primary biometrics: iris, finger and face. The intuitive user interface also allows the entry of biographic data to create a comprehensive database on the enrolled subjects. The HIIDE has an onboard processor and data storage capacity and is the only device that allows complete functionality while connected to a host PC or when operating in the field untethered.

The HIIDE is a Microsoft XP embedded device that includes state of the art lens technology for both iris and facial image capture and an FBI standards compliant 500 DPI capacitive fingerprint sensor. Capture of an individual's biometrics on the HIIDE is accomplished through an easy to use step by step wizard process starting off with capturing a subject's left and right iris images. The HIIDE then can capture all ten fingerprints and finally a facial image is acquired. The user can choose to skip any or all of the biometric captures for maximum flexibility. Once the biometric capture is completed, the user can input a fully customizable biographic information file and save the enrollment. Recognition of a subject can be performed using either the iris or fingerprint biometric for 1:n searches or a 1:1 verification using facial recognition.

The HIIDE can store up to 10,000 full biometric portfolios (2 iris templates, 10 flat fingerprints, a facial image and selected contextual data) and identify a subject in stand-alone mode (i.e., un-tethered to a host PC). The biometric and contextual data is fully compliant with the FBI's Electronic Fingerprint Transmission Standard (EFTS) which is focused on fingerprints, and the newer DoD Electronic Biometric Transmission Specification (EBTS), which accounts for multiple modes of biometrics. The device can be expanded to include USB enabled peripheral devices such as passport or card readers, and an external keyboard and mouse. Current development efforts include completion of full compatibility with the Tactical Computer (TactiComp) fielded by the Army Space Program Office (ASPO). Through this interoperability, the HIIDE will gain the wireless reach back to the biometric enterprise "inside the wire" via the TactiComp's self healing "Mesh Net" capability.

Concept of HIIDE Operations

Designed from the ground up as a cooperative interagency effort, the HIIDE is fully compatible with the BAT V4.0 with Service Pack 4 installed. Through this GUI level interoperability, the HIIDE device provides connectivity to the DoD Biometric Enterprise but frees the Soldiers/Marines who use it from wired connectivity to the biometric data source. Utilizing the internal storage and matching capabilities of the device, the user gains truly tactical biometrics or "biometrics outside the wire." The method of utilization of the HIIDE device as part of a unit's operations first requires the unit to conduct a mission analysis. The intended functionality of the device as part of those operations will guide the process of integration. Some examples include, but are not limited to, population and resource control, cordon and sweep operations, check points, contracting, or verification of the identity of targeted individuals on an objective.

Population and Resource Control

The ability to not only identify personnel wanted by coalition forces but to identify persons of interest while conducting normal patrols has already proven of value to US Forces. U.S. Forces utilize biometric identification to confirm that individuals they encounter are authorized to be in the area. By conducting biometric screening and collection of all individuals in a town as part of counterinsurgency efforts, it is possible to later identify individuals that don't belong to the previously enrolled local population (such as mobile insurgents). Such a policy has proved so successful at limiting insurgent freedom of movement that some local leaders have approached US forces to have their towns biometrically enrolled. They realize that biometric enrollment will help to identify those that don't belong in the area (such as foreign insurgents) without the local leaders risking reprisal by reporting insurgents to the coalition.

In this usage, the HIIDE could be loaded with a subset of the full biometrics collected from the referenced population. Utilizing the Device Manager software that comes with the HIIDEs or through the BAT V4.0 SP4 GUI, the user can select which biometrics they choose to download. For example, if the unit chose to use iris images as primary identification and finger prints as backup, the unit could select to down load two iris images, two thumbs and two forefingers for each individual and use those biometrics to positively identify any individuals they encounter as actually being from a said neighborhood. As part of the normal download of identification records the HIIDE always downloads a face image for all selected files if one is in the database. That permits the user to visually confirm the identified individual is in fact the person standing in front of him/her. Using this method, any individuals not from the neighborhood could be identified and further screened for identification as a possible outsider or insurgent.

Cordon and Sweep Operations

Viewed as a tactical extension of the BAT system for "biometrics outside the wire", units can utilize the HIIDE during cordon or sweep operations. Prior to deploying with the HIIDEs, the unit would utilize a BAT system to conduct reduction queries to narrow the listed of "wanted" individuals down to manageable levels. depending on the size of the files to be downloaded (rolled fingerprint templates are at least 40 percent larger than flat fingerprint templates) and the number of biometrics chosen for download as discussed above, the HIIDE can hold between 3800 and 10,000 biometric identities. The files chosen could be combined lists of all of the individuals on the NGIC national watch list combined with successive higher headquarters lists or the individuals that the local intelligence section have identified as being in the area and as having previously participated in actions against coalition forces. (The exact make up and selection process for this list is a subject of ongoing discussions and subject to unit TTPs.) Once downloaded to one or more HIIDEs taken with forces on the operation, the HIIDE can be used to "biometrically triage" the individuals rounded up in a cordon or sweep and to identify known wanted individuals or those who have the exceptionally bad luck of constantly being in the vicinity of IEDs, snipers, etc. Even if not detained, the HIIDE can be used to create a tracking report on the details of that biometric encounter. Multiple instances of such reports on the same individual downloaded to BAT can provide an analyst with a pattern to analyze movements and proximity to events that may warrant putting the individual on alert/detain status. Those with no reason to be detained and cleared by HIIDE screening could be released immediately to avoid building animosity in the otherwise neutral population. Those not previously in the database and not to be detained would have their biometrics collected by the HIIDE user prior to release. Upon returning from the operation, the collected files and tracking reports can be downloaded to the BAT system for addition to existing analysis. For those individuals to be detained due to anti coalition activity, positive swipe for residue etc., the tactical force should not waste effort to collect biometrics with the HIIDE if the individual is not in the limited HIIDE database. The using unit should wait until the individual is brought back to a BAT or other more capable biometric enrollment system so that the highest quality biometric possible is entered into the system.

Checkpoints

Whether operated at Entry Control or Traffic Checkpoints, the HIIDE can be utilized to search for wanted or alert individuals that may pass through the points. This will help limit cross compartment movement of insurgent elements and restrict entry to authorized personnel only. The HIIDE could also be utilized on bases to validate the identity of local employed personnel who a security force may encounter away from an entrance. By loading the entire approved employee list for a base on the HIIDE, the identity and employment information of the individual can be determined quickly (4 seconds using iris match) and an assessment done by Force Protection personnel of whether the person should be where he or she is found.

Contracting

U.S. Forces make millions of dollars in payments to individuals and company representative on a daily basis. The ability to properly document and store an irrefutable record of those transactions could prove invaluable. In this role, the HIIDE or BAT could be used to collect the biometrics of local contractors or employees at the outset of the business relationship. As part of the process of contract initiation or for payment during or at the end of a contract the identity of the individual is verified using a HIIDE and a tracking report is created annotating the circumstances of the biometric identification such as "Biometrically identified as part of payment #17 in the amount of $110,000 on DTG as part of Contract XXX". These Tracking Reports could form the basis of ensuring that later accusations of non payment of "you didn't pay me" are not encountered.

Verification of the Identity of Targeted Individuals

In instances where specific individuals are the subject of operations, the HIIDE can provide a rapid method of identifying individuals with certitude. Whether it is for verifying the correct individual is in custody on an objective, or logging all those killed on an objective, the HIIDE offers a lightweight tactical alternative to other systems. In this usage, the biometrics of the targeted individual along with any other wanted individuals are downloaded from BAT to HIIDE prior to conducting the operation. Once secured on the objective, the HIIDE offers a handheld method for validating the individual is the intended target of the operation.

In some instances, due to the blast physics of suicide vests or other explosives, the head of subject is left relatively intact when the rest of the body is destroyed. Barring significant damage to the face and eyes it would still be possible to identify the individual from data-based iris images for between two to twelve hours maximum (depending of ambient, temperature and other conditions) after death. Additionally, there is an operational advantage to collecting the biometrics of all individuals captured or killed on an objective should the tactical situation permit. Individuals killed on an objective might include unrealized successes against insurgents that US or coalition forces may continue to expend resources searching for if not changed to deceased in the reference database. The motto for all cases should be "If you can take a biometric, take a biometric, but take the highest quality biometric the tactical situation allows."

HIIDE Fielding

The Army G2 is currently fielding 1250 HIIDE devices. Of an original procurement of 1500 devices, 250 HIIDEs were issued to the United States Marine Corps for use by the Marine Expeditionary Forces, counterintelligence elements and the Marine training centers, MARFORSYSCOM and Mojave Viper. The Army plans to field these first 1250 devices by operational priority following consultation with USCENTCOM and MNC-I. Currently the majority of the existing HIIDEs are to be fielded to support operations in Afghanistan and Iraq with additional HIIDEs going to support the Multi-Functional Teams being formed under the 525 MI Bde, Joint Special Operations Command, the International Security Assistance Force (ISAF) and a small number to support the Combat Training Centers at Ft Polk and the National Training Center. Initial HIIDE fielding is already underway with devices to be fielded in Iraq and Afghanistan in Jan/Feb 07 in conjunction with the fielding of the BAT Service Pack 4 software.

HIIDE Training

As part of the comprehensive fielding plan for HIIDE, the devices will only be issued to units once training on the devices has been accomplished. Already executed training events with the 525 MI Bde and the USMC have demonstrated that the two levels of training available to users provides users with all required skills. The two levels of training include Field Operator and Administrator level training.

Field Operator training is intended for those users who will simply be tasked with collecting biometrics from individuals and using the HIIDE to identify individuals. Introduction to biometrics, the specifics of the device, basic device operation and an orientation to the mandatory fields that must be collected to create a valid Electronic Fingerprint Transmission or EFT (the FBI standard) file are covered. Field Operator training taught by a HIIDE instructor or an individual who has completed the Administrator level training should take approximately one hour.

The second level of training available is the Administrator level. Administrator training is intended for those individuals who will be required to perform device configuration and management, upload and download of files for BAT or in the case where there is no BAT system, via the HIIDE Portfolio Browser software, and who will be required to train Field Operators. Administrator training requires approximately 12 hours of training. During this twelve hours the students are given a detailed run-through including practical exercises of the HIIDE Device Manager Software. The HIIDE Device Manager is license free software that is used to configure all aspects of the HIIDE Device including authorized users, biometric wizard prompt selection, internal database management, power configurations, etc. This training is vital because improper alterations of the device settings, as with any computer, can render the device useless to other users or can permit the Field operators to collect biometrics that fail to create FBI compliant EFT files. Since some units may utilize the HIIDE under conditions where a BAT system is not present to support upload and download, the G2 purchased a limited number of HIIDE Portfolio Browser software sets. The Portfolio Browser permits a user to export a HIIDE collected biometric in either the native HIIDE Portfolio format, an FBI compliant EFT file or in the native BAT format known as a BAT Data File (BDF). Once exported to a file folder in the BDF format, the data can be transported by any normal means (CD ROM, thumb drive, etc) to a location where a BAT system resides and imported directly into BAT. The Portfolio Browser software also permits download of a watchlist to a drive from BAT and once received at the computer with the HIIDE Portfolio Browser, that new identification list can be uploaded to HIIDE. **It is important to note that to export or import BDFs or an EFT, the HIIDE Portfolio Browser software requires the installation of the Aware NIST Pack software on whatever computer the Portfolio Browser software is running on. BAT has the NIST software as part of its basic install but non BAT users will require the NIST software prior to Portfolio Browser usage.**

Conclusion

The world of biometrics has moved from solutions involving single biometric modalities to ones of increasing complexity such as national identification projects. These projects often involve two or three biometric modalities. Layering biometric technology allows users to maximize the benefits of each of the modalities while effectively minimizing the limitations. The HIIDE device utilizes the speed and accuracy of iris identification, the ability to access large fingerprint databases, and the user comfort that comes with facial recognition. Combined in a single device, this offers a powerful and flexible tool that can be customized to fit almost any identification scenario and will truly be the first major step towards the operationalization of biometrics.

New Linguist Contracts

by Sylvia Dunn, DCS G-2, DAMI-OP

On 15 Dec 06, re-competition of the Army's Linguist Contract resulted in the award of three new contracts, with a fourth contract award expected in 2nd Quarter FY07. Global Linguist Solutions (GLS) won the Iraq portion of the original contract and the Afghanistan portion of the contract went to Thomas Computer Solutions (TCS). CALNET won the Guantanamo Bay linguist contract award. The new contracts are cost plus, award-fee based and contract for linguists against identified vacancies in specific locations.

The contract transition should be transparent for the Warfighter. Theater Linguist Management teams will facilitate contract transition through the execution of select routine activities in each affected region, i.e., Common Access Card (CAC) re-issue, uniform waivers, and requirements revalidation. New CAC cards and company identification badges will be issued for linguists that transition to the new contracts.

Some issues remain to be resolved prior to contract transition. An announcement is expected in 2d Quarter FY07 that gives additional details concerning the transition period. The transition period for the Iraq and the Afghanistan contracts will extend for approximately 90 days and the Guantanamo Bay contract has a transition period of 30 days. During the transition process all routine policies and procedures will remain in effect.

Army G2 Information Management Directorate R&S Division
Technical Points of Contact

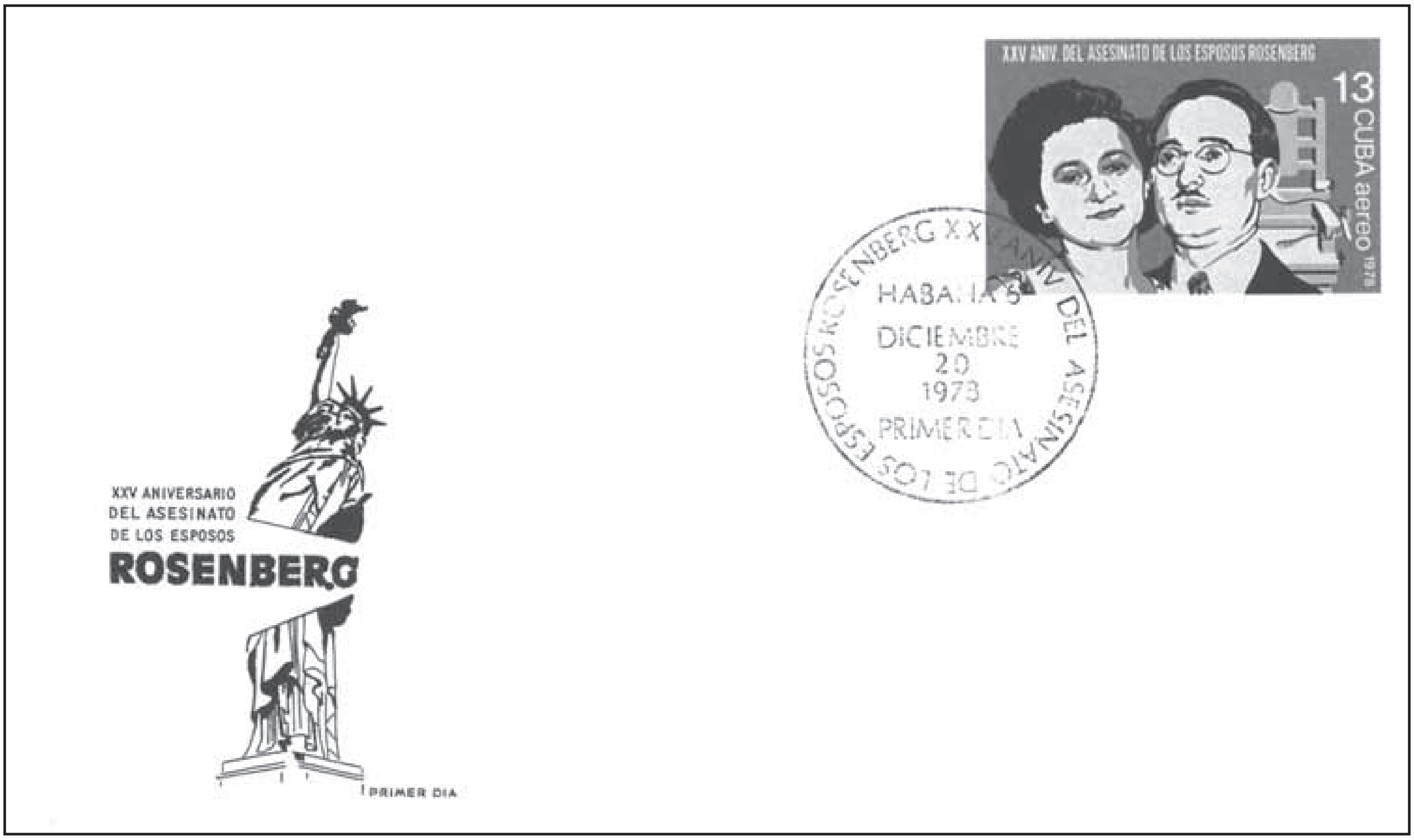
Vince McCarron (DCGS-A): vincent.j.mccarron@us.army.mil
Kristen O'Keefe (DCGS-A): kristin.okeefe@us.army.mil
Ed Tower (DCGS-A/ASAS-L/Tacticomp): ed.tower@us.army.mil
Jeff Dunn (Holographic Imaging): dunnjg@us.army.mil
Jim Fenton (Biometrics): james.fenton@us.army.mil
Jerry Jackson (HIIDE): jerry.jackson@us.army.mil
Bob Plimpton (Pathfinder): robert.plimpton@us.army.mil
Tom Langenfeld (DOCEX): thomas.langenfeld@us.army.mil
Patty Guitard (DCGS-A): patricia.guitard1@us.army.mil
LTC Bill Turmel (Battle Command): william.turmel@us.army.mil
Mike Callawaert (JIOC): michael.callewaert@us.army.mil

Intelligence Philatelic Vignettes

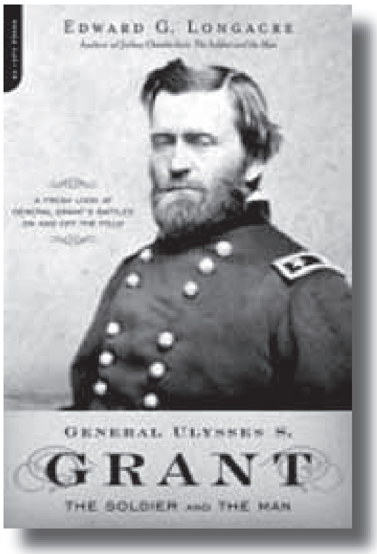
Fidel's Philatelic Follies

by Mark Sommer

In a blatant "thumb in the eye" propaganda move, the government of Cuba issued this stamp and accompanying first day cover (the philatelic term for an envelope) of Soviet spies Julius and Ethel Rosenberg who were executed for their crimes. Carried out on June 19, 1953 at the infamous Sing Sing prison in Ossining, New York, the Spanish inscription reads "The 25th Anniversary of the Assassination of the Rosenbergs" with the Statue of Liberty cut in half. The stamp is also significant as it is the only stamp issue in the world which pictures the electric chair (nicknamed "Old Sparky" by those at the prison.)



*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 published works in the intelligence field include: "Getting the Message Through: Clandestine Mail and Postage Stamps", **MIPB**, October–December, 1992 and "Undercover Addresses of World War II", **International Journal of Intelligence and Counterintelligence**, Fall 1993.*



General Ulysses S. Grant: The Soldier and the Man
by Edward G. Longacre

(Cambridge, MA: Da Capo Press, June, 2006),
338 pages, $34.95, ISBN: 9780306812699.

Reviewed by
Chief Warrant Officer Two Kevin S. Gould

Edward Longacre's biography of Ulysses S. Grant follows him from West Point cadet to the end of the 1865 siege of Petersburg, Virginia. Longacre deliberately avoids a comprehensive biography of Grant, focusing on how Grant's values, relationships, struggle with mediocrity, and alcoholism shaped his personality and leadership style. He presents Grant as a struggling alcoholic who was concurrently a devoted husband and father dismayed when remote assignments cut him off from his family. Longacre attributes Grant's early alcohol abuse to boredom and misery as a frontier staff officer. Following his relief in 1857, Grant worked as a farmer, real estate broker, and clerk in his brother's tannery. Despite supporting a family on limited income, Grant paid fifteen hundred dollars to purchase one of his father-in-law's slaves only to immediately release him.

Longacre covers Grant's campaigns from his command of a volunteer regiment capturing Fort Donelson through the Battle of Shiloh, the siege of Vicksburg, Battle of Chattanooga, the Second Wilderness Campaign of 1864, and the siege of Petersburg. He provides a general overview of each campaign focused on Grant's relationships with his subordinate commanders and political and military superiors. Longacre focuses closely on Grant's relationships with Benjamin Butler, George Meade, William F. Smith, and Henry Halleck. He treats Grant's relationship with Lincoln with less detail, although Lincoln's high regard for Grant's fighting qualities led to Grant's promotion to lieutenant general. Grant proved to be Lincoln's most loyal general who shared Lincoln's vision for victory. Grant was focused on his goals, preferring to always move forward. Longacre contrasts Grant's willingness to aggressively carry the fight to the enemy at the cost of tens of thousands of Union casualties with his emotional reactions to the deaths of his friends and his retreat from field hospitals and other scenes of post-combat carnage.

Longacre succeeds in portraying Grant as a triumphant individual who mastered his personal faults and overcame obstacles in his personal and professional life. The narrative is clear and the action quick. He does not bog the reader down in the minute details of Grant's campaigns. His bibliography points the reader to other information on both Grant and his lieutenants. It includes both published and unpublished personal papers and memoirs—the standard and latest scholarship to provide a balanced view of his strengths and weaknesses. Some readers may disagree with Longacre's focus on Grant's alcoholism; however, contemporaries raised it throughout Grant's public life and it has commanded scholars' attention ever since. Longacre argues that the struggles Grant faced from his family, his education, and early military career prepared him for his role as Commanding General of the Union and as President. Students of leadership in the American Civil War or of the psychology of leadership will find Longacre's book an important addition to their professional reading.

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 MIPB@hua.army.mil or by mail on disk to:

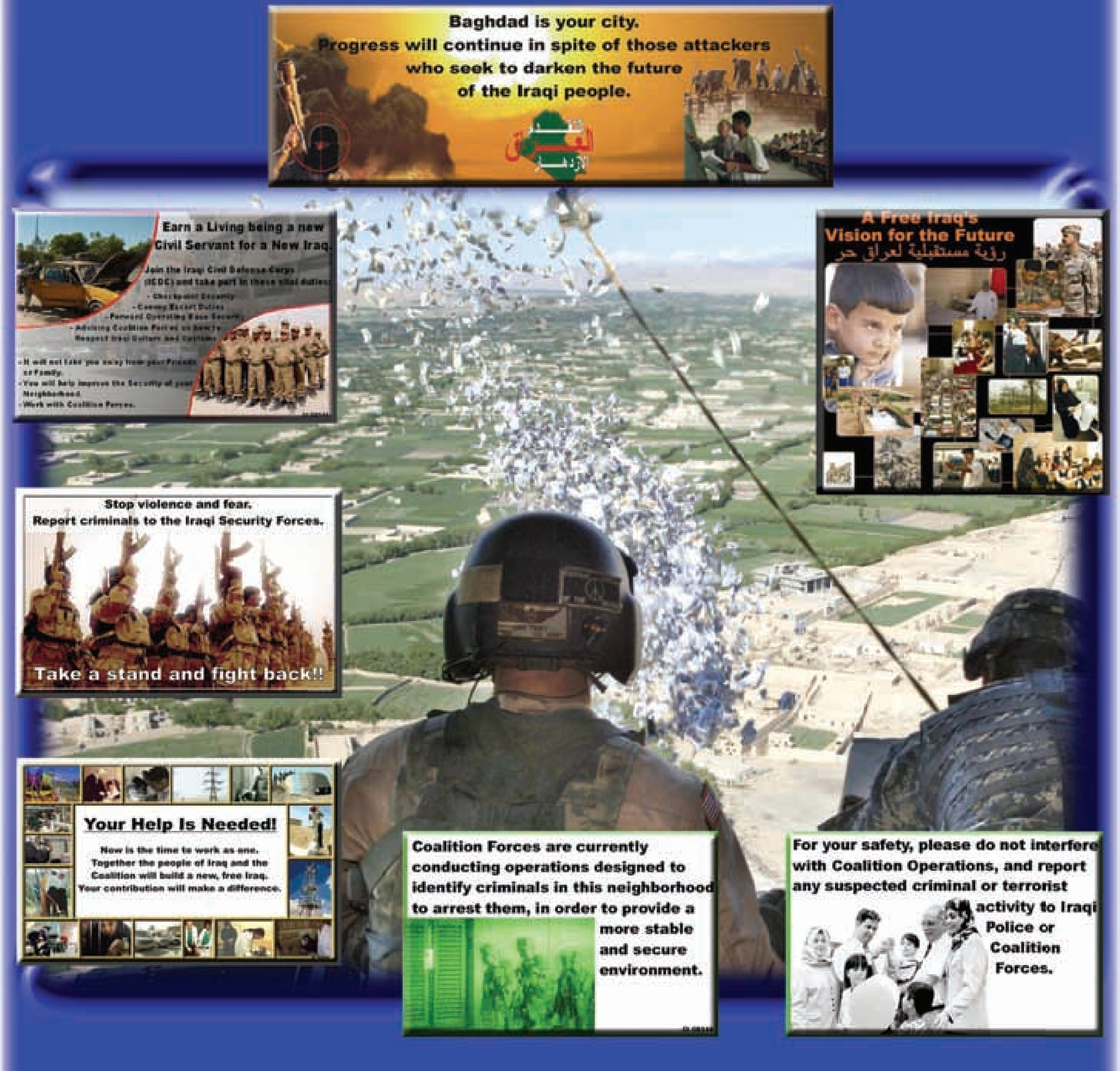
ATTN ATZS-CDI-DM (Smith)
U.S. Army Intelligence Center and Fort Huachuca
550 Cibeque Street
Bldg. 61730, Room 124
Fort Huachuca, AZ 85613-7017

If you have any questions, please email us at MIPB@hua.army.mil or call 520.538.0956/DSN 879.0956. Our fax is 520.533.9971.

Upcoming Themes and Deadlines

Issue	Theme	Deadline
Apr-Jun 07	Transformation	30 Apr 07
Jul-Sep 07	GEOINT	31 Jul 07
Oct-Dec 07	Biometrics	30 Oct 07

Products in Support of Counterinsurgency Operations



Baghdad is your city.
Progress will continue in spite of those attackers
who seek to darken the future
of the Iraqi people.

Earn a Living being a new Civil Servant for a New Iraq.

Join the Iraqi Civil Defense Corps (ICDC) and take part in these vital duties:

- Checkpoint Security
- Convoy Escort Duties
- Forward Operating Base Security
- Advising Coalition Forces on how to Respect Iraqi Culture and Customs

- It will not take you away from your Friends or Family.
- You will help improve the Security of your Neighborhood.
- Work with Coalition Forces.

A Free Iraq's Vision for the Future
رؤية مستقبلية لعراق حر

Stop violence and fear.
Report criminals to the Iraqi Security Forces.

Take a stand and fight back!!

Your Help Is Needed!

Now is the time to work as one.
Together the people of Iraq and the Coalition will build a new, free Iraq.
Your contribution will make a difference.

Coalition Forces are currently conducting operations designed to identify criminals in this neighborhood to arrest them, in order to provide a more stable and secure environment.

For your safety, please do not interfere with Coalition Operations, and report any suspected criminal or terrorist activity to Iraqi Police or Coalition Forces.

All products produced by USACAPOC (original in Arabic) as found on Psywar.org

ATTN ATZS-CDI-DM
USAIC AND FORT HUACHUCA
550 CIBEQUE STREET
FORT HUACHUCA AZ 85613-7017

"With good intelligence, counterinsurgents are like surgeons cutting out cancerous tissue while keeping other vital organs intact."

FM 3-24
December 2006

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

PIN: 083844-000