MIPB

Military Intelligence Professional Bulletin
April-June 2011 PB 34-11-2

INTELLIGENCE

in the Current Environment

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2011		**00-04-2011 to 00-06-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Military Intelligence Professional Bulletin (MIPB). PB 34-111-2, April-June 2011	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Intelligence Center and Fort Huachuca,ATTN: MIPB (ATZS-CDI-DM),Box 2001, Bldg. 51005,Fort Huachuca,AZ,85613-7002**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**88**	

Purpose: The U.S. Army Intelligence Center of Excellence 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:

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

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1107511

FROM THE EDITOR

In addition to all the great articles and book reviews, the Joint Readiness Training Center (JRTC) contributed its lessons learned on intelligence operations during Rotation 11-01 for this issue. The 3rd BCT, 82nd Airborne "Panthers" paratroopers deployed to the JRTC at Fort Polk and conducted the first full spectrum operation rotation in eight years.

We continue to receive excellent articles from the field on the current operating environments for intelligence as well as suggestions for improving training. Please continue sending MIPB your ideas and thoughts. Please note that we have a new department, Culture Corner, which will provide insights on cultural competency on a regular basis.

Throughout 2012, the Military Intelligence (MI) community (USAICoE, INSCOM, DA G2, and FORSCOM) will be commemorating the 50th anniversary of the establishment of the MI Branch and the 25th anniversary of the MI Corps. Activities are being planned to educate as well as build professional interest in the history and heritage of Army Intelligence starting with the American Revolution through experiences and events throughout the year.

MIPB is proud to participate in this celebration by publishing a July September 2012 50th anniversary commemorative issue in collaboration with Lori Tagg, USAICoE Command Historian and Michael Bigelow, INSCOM Command Historian. While content for this issue will be supplied by Lori and Mike, I would like to invite you to submit historical Army Intelligence related articles for publication in issues leading up to the July September 2012 publication. Suspenses for these issues are:

July September 2011	S: 30 May 2011
October December 2011	S: 30 August 2011
January March 2012	S: 30 November 2011
April June 2012	S: 30 January 2012

Sterilla A. Smith
Editor

MILITARY INTELLIGENCE

April - June 2011 Volume 37 Number 2 PB 34-11-2

FEATURES

JRTC

Departments

ALWAYS OUT FRONT

by Brigadier General Gregg C. Potter
Commanding General
U.S. Army Intelligence Center of Excellence

Leading Change[1]

Two-plus decades ago, when I attended the U.S. Army Intelligence Officer Basic Course at Fort Huachuca, Arizona, training was not on a computer and our Nation knew its threat, the Soviets. Since then, our Army has drastically changed force structure and how it operates. We have moved from a corps and division-centric army to a brigade-centric army. Our Army has modified how it equips and trains our Soldiers to perform the intelligence mission in light of the changing operational environment and our Army's structural changes.

Change is constant in our business, whether it is the security environment or fielding new equipment or instituting new training models. Acclimating people to change and encouraging them to embrace it and move forward is challenging. Since taking command of the U.S. Army Intelligence Center of Excellence (USAICoE) and Fort Huachuca, I have stated that our mission is to train, develop, and educate our Army's Intelligence Soldiers and leaders, military and civilian. Our mission is also to design, develop and integrate intelligence capabilities through concepts, doctrine, requirements, and materiel development that support expeditionary full-spectrum operations in a joint, interagency, intergovernmental, and multi-national environment.

I have identified several critical tasks to accomplish this mission. First, we must provide to our operational force the best trained Soldier to support operations in Iraq and Afghanistan. To do this, we must attract the best and the brightest talent from our officers, warrant officers, noncommissioned officers, Department of the Army civilians, and contractors to train the next generation of intelligence Soldiers and leaders. We will provide relevant training to transform Soldiers into agile and adaptive combat leaders and intelligence professionals, preparing them to meet current and future challenges. Leader development must build leaders who can handle the complexities they face now and in the future.

Second, we must identify innovative and relevant intelligence capabilities for the current and future force. We must focus resources on where risk is greatest so that we can maximize emerging Military Intelligence (MI) capabilities. Then we must integrate those capabilities into the operational force, building an Intelligence force that wins the "fight for knowledge" in all terrain and across the full spectrum of military operations to achieve decisive victory. To guide our Soldiers, we must provide them the doctrine needed to operate in the field. Where we previously used 40 to 50 intelligence Field Manuals we now have four. The rest are Training Circulars and Army Tactics, Techniques, and Procedures publications that we will rapidly update in a rapidly changing security and technology environment.[2]

USAICoE will execute our mission as good stewards of natural and national resources. One means by which we will accomplish this task is by implementing training guided by principles of the U.S. Army Learning Concept for 2015 (ALC 2015). ALC 2015 is our Army's vision of how we will train and educate our Soldiers and leaders and develop the skills, attributes, and abilities to execute full spectrum operations in an era of persistent conflict. One of our biggest challenges is to deliver quality training, doctrine, new concepts, and equipment to our Soldiers and leaders. This training must be delivered through relevant, tailored, and engaging experiences throughout a career-long continuum of learning that is location independent and accessed when needed. We will adjust our training, examining what needs to be trained at Fort Huachuca and

what should be trained in the operational units.

USAICoE will focus on two core competencies of MI–Intelligence, Surveillance, and Reconnaissance (ISR) Synchronization[3] and leading edge analytic training and education. From Initial Military Training through our Pre-Command Course, we must devote the requisite time and effort to the training of the very difficult and most important skill of ISR Synchronization. Our intent is to ensure that every intelligence Soldier knows how to direct and leverage our ISR collection systems and our analytical processing, exploitation and dissemination systems. Our intelligence force must excel at the fundamentals and techniques for both manual and digitally assisted multi-disciplined analytic processes to convert sensor-collected data, information, and combat information into intelligence that answers the Commander's priority intelligence requirements.

USAICoE must produce an adaptive, knowledgeable warrior who can think by leveraging data, information, and intelligence to accomplish any mission. We will emphasize human cognition, cognitive analytics, critical thinking, problem solving, and knowledge management. Additionally, we will tie these topics to foundational doctrinal concepts such as the military decision making process, intelligence preparation of the battlefield, targeting, and ISR Synchronization. Our intent is to enable Soldiers to understand the value of analysis, to excel at the fundamentals, and to perform analysis using any tool set, manual or digital.

Our goals are to:

- Create a culture that promotes a passion in people for our Army Values and the intelligence business, innovation, accountability, and teamwork.
- Manage complexity.
- Focus on precise decision making.
- Simplify organizational processes without overly simplifying the picture of the operational environment.
- Build a unified partnership across the intelligence community and promote a unified effort to support the force with the most effective intelligence solutions.

As USAICoE undertakes this new focus, we need your involvement, ideas, and feedback to ensure that we develop team solutions. We here at USAICoE develop the concepts that will influence our Army and the doctrine that you will execute. We participate in materiel development for those systems that you will operate. We train those Soldiers who you will lead and serve with through the years. These are the challenges that excite me and they should excite you as the primary stakeholder.

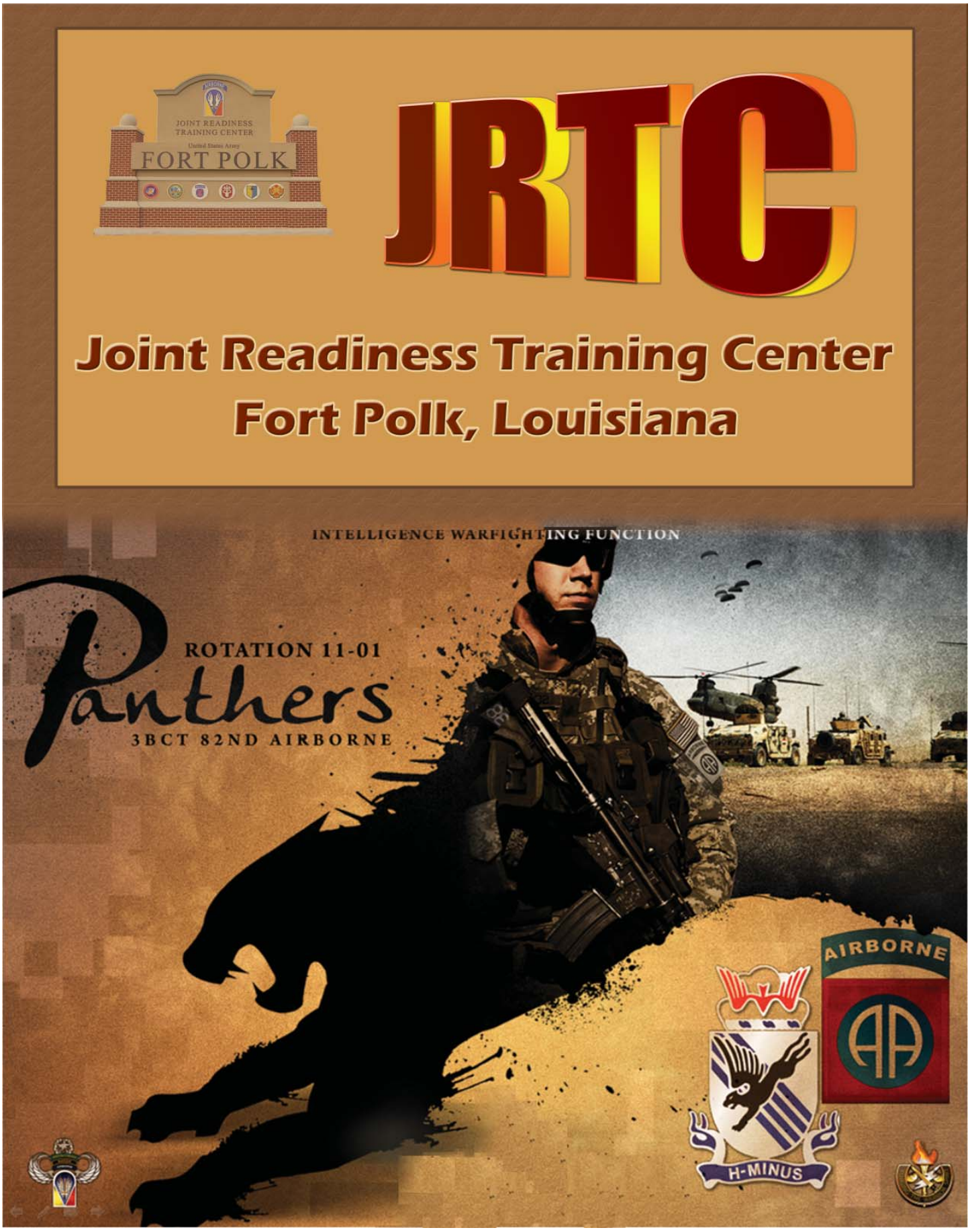
Endnotes

1. I highly recommend for your professional reading, "*Leading Change*" by John P. Kotter, Harvard Business Press, 1966.

2. Currently the Army is drastically restructuring the Army doctrinal hierarchy and changing the way doctrine will be developed and maintained in the future. We will provide more information in a separate article about these significant Army doctrinal changes in the near future.

3. Recently the Army senior leadership decided to eliminate the term and acronym for intelligence, surveillance, and reconnaissance (ISR) as a part of the development of the new draft of FM 3-0, Operations. Therefore, the U.S. Army Training and Doctrine Command will develop new constructs and terminology for FM 3-0 and subsequent Army doctrine. These changes will include replacing the term ISR synchronization.

Always Out Front!


JOINT READINESS TRAINING CENTER
United States Army
FORT POLK
JRTC
Joint Readiness Training Center
Fort Polk, Louisiana
INTELLIGENCE WARFIGHTING FUNCTION
ROTATION 11-01
Panthers
3BCT 82ND AIRBORNE
AIRBORNE
H-MINUS

Joint Readiness Training Center: Full Spectrum Operations Overview

by Lieutenant Colonel (P) John Haynicz, Senior Intelligence Trainer

"Our Army will embrace FSO with the best leaders and Soldiers we've ever had–and because of their acute ability to rapidly absorb and apply warfighting skills, we'll be stronger and much more capable than we've ever been."

–Brigadier General James Yarbrough, Commanding General, JRTC

In October 2010, the Joint Readiness Training Center (JRTC) conducted its first full spectrum operations (FSO) rotation in eight years. The 3rd Brigade Combat Team (BCT), 82nd Airborne "Panthers" deployed to Fort Polk, Louisiana and conducted the rotation with the augmentation of an engineer battalion, aviation battalion, air defense artillery (ADA) company, and a chemical, biological, radiological, and nuclear (CBRN) platoon. The rotation spanned 21 days and consisted of five days of situational training exercises (STX), three days of command post exercises (CPX), and eight days of force-on-force (FoF), while simultaneously conducting 15 days of live fires. This article provides the general overview of the rotation and general observations from the Task Force Leaders and Intelligence Trainer/Mentors of JRTC. What follows are more in-depth articles focusing on specific topics and single-source discipline observations.

It is important to mention that none of the observations made during this rotation could have been collected without the hard work and determination of the Panther Brigade. They were the "men in the arena" and it was an honor to partner with these great Soldiers and Paratroopers as they took any challenge or obstacle head on. The 3rd Brigade, 82nd Airborne continually internalized any lesson or observation and immediately implemented "fixes." Their energy, professionalism, and technical and tactical competence ensured that the lessons observed from this rotation could be applied throughout the Army.

FSO is defined in FM 3-0, Operations, 27 February 2008, as "Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action–lethal and nonlethal–proportional to the mission and informed by a thorough understanding of all variables of the operational environment." The FoF portion of the rotational scenario involved a country that was experiencing a border dispute and required the Panther Brigade to conduct a forced entry operation through parachute assault to seize an airfield, conduct a defense of the lodgment, and finally conduct an attack to defeat enemy forces. This design allowed the Brigade to work all three aspects of FSO in different proportions.

As stated earlier, the rotation spanned 21 days consisting of five days of STX, three days of CPX, and eight days of FoF. The STX lanes ran concurrently to CPX, allowing all company/troop/batteries to hone battle skills while their battalion (BN) and BCT staffs were conducting the CPX. The infantry companies conducted an attack to seize an objective (terrain oriented), a raid to seize a high value target (enemy oriented), and a 36-hour defense which was conducted against a conventional force that possessed unmanned aircraft systems (UAS), indirect and direct fire weapons (to include BMPs/T-80 tanks.) The cavalry troops conducted a screen mission against a mechanized force, a reconnaissance of an infantry battalion objective, and finally a combined arms live fire exercise. The forward support companies conducted combat convoys that included replenishment operations and establishment and security of a logistic resupply point against a determined conventional threat.

All the STX lanes included time for planning, rehearsals, and execution. Intelligence Pre-Rotational Training consisted of a daylong Intelligence Seminar reviewing intelligence, surveillance, and reconnaissance (ISR), Fusion, and the multiple enablers available at JRTC, followed by three days of Distributed Common Ground System (DCGS) refresher and One System Remote Video Terminal (OSRVT), unattended ground sensors (UGS) and Biometrics Automated Toolset/Handheld Interagency Identity Detections training. The Soldiers of the MI Company (MICO) conducted 9 days of Military Source Operations and Interrogations training (both instruction and STX), low level voice intercept (LLVI) training (integrated into the cavalry troop STX), and a UAS validation STX.

The CPX was a computer simulation of the attack phase of the operation that lasted three days and ran concurrent with the STX portion of the exercise. It allowed the BCT and BN/Squadron (SQDN) staffs to work current operations as well as planning for future operations. Tactical operation centers were set up in distributed distances and stressed the digital battle tracking and planning systems. The Brigade planned, synchronized, and executed a battalion level air assault as part of their attack to secure objectives.

The FoF portion of the exercise lasted eight days and included a forced entry operation to seize an airfield, a non-combatant evacuation exercise (NEO), a deliberate defense, and a deliberate attack. The Brigade conducted a parachute assault to seize a lodgment and secure an airhead line. Air-Land operations began as the unit started to build combat power while interacting with the civilian population, conducting NEO operations, and fighting a Level III insurgency in the immediate area. Two days into the exercise, the Brigade was informed that a conventional threat force was moving toward the lodgment in order to deny the use of the field landing trip (FLS) to friendly forces. The BCT conducted a deliberate defense to retain the airhead line. The enemy did not secure the FLS during the attack and had to withdraw to defensive positions in order to regroup. The BCT then planned, synchronized, and attacked prepared enemy positions in zone, culminating the exercise.

The threat faced by the Brigade was a Hybrid Threat. It was a combination of a Level III insurgency and a near peer conventional force (Regiment(-), that had defected from the legitimate government of the host nation. The Level III insurgents were the only opposing force (OPFOR) in play when the BCT conducted forced entry operations. The insurgents were equipped with small arms, mortars, 107mm MRLs, limited shoulder fired surface-to-air missiles and employed various forms of improvised explosive devices/vehicle borne explosive devices. Additionally, the insurgents were supported by a neighboring threat nation with rotary wing support, logistics and intelligence information that included UAS surveillance. These insurgents were present in and around the towns as well as in the surrounding area and remained operational during the entirety of FoF, eventually conducting operations in coordination with the conventional force in a combined purpose.

As the Brigade was conducting initial entry operations, they received intelligence from the joint task force (JTF) that a conventional force was moving in their direction, most likely to attack in order to deny the use of the lodgment by U.S. forces. The Brigade conducted a defense of the air-head and after repelling the enemy attack, conducted a counterattack against a hastily prepared defense position. The rogue conventional force threat contained many of the capabilities that the U.S. Army possesses to include attack and lift rotary wing support, CBRN, Armor, UAS, and ADA assets, as well as limited C4ISR capabilities such as UAS with OSRVT. Out of all the capabilities that were given to the enemy conventional forces, the UAS turned out to be the game changer. The enemy had two types of UAS, one replicating Shadow's capabilities and one replicating a Raven's capabilities. The enemy's ability to obtain real time video allowed them to concentrate their effects efficiently and effectively on the BCT. This is but one of the major intelligence observations to come from this rotation.

Major Observations

Intelligence Preparation of the Battlefield (IPB). Detailed terrain analysis was missing at all levels and all Warfighting Functions (WFF). There appeared to be an overreliance on Terrain Team products and PowerPoint map reconnaissance (unfortunately, this is not limited to FSO, JRTC observes this during Operations Enduring Freedom and New Dawn rotations as well.) Additionally,

units did not confirm/deny planning assumptions of the terrain once on the ground and learned to include this requirement in collection plans. This was particularly important in determining enemy courses of action (ECOA) using restricted or severely restricted terrain, and for the emplacement of obstacles. Unit S2s understood the enemy composition and range of capabilities, but struggled to fully develop Situational and Event Templates that incorporated all the enemy enablers. The S2s were also challenged with how to depict enemy actions and visualize the fight for their commanders.

This challenge was not only in the medium used (analog or digital), but in symbology and ECOA statements necessary to depict and describe enemy actions across each WFFs in time and space. PowerPoint depictions were generally used in the planning phase and once digital systems were established, but for the beginning portion of FoF, all the S2s utilized mapboards with acetate overlays to battle track and develop ECOAs. Lastly, young S2s were challenged in their ability to fight the full range of OPFOR capabilities during wargaming, when conducted. Enemy objectives and schemes of maneuver, synchronized with OPFOR enablers by task and purpose were seldom fully developed. This had compounding negative effects in attempting to synchronize decisions points (DPs) to priority intelligence requirements (PIR) to named areas of interest (NAIs) to a specific collection plan.

Intelligence at the Company Level. The lesson observed is that intelligence support at the company level is as valid in FSO as in counterinsurgency (COIN). FSO is not entirely a top down Intel fight. Bottom up assessments and refinement are still required for the complete picture of the operational environment. The Panthers did not formally establish a Company Intelligence Support Team (CoIST) program. Like many units, Fire Support Soldiers made up the bulk of their CoIST efforts, and the BCT chose to employ these Soldiers in their traditional Artillery role. However, company commanders quickly learned the need to employ small teams (FSO, FSNCO, XO, RTO) to conduct Intel analysis and reporting.

The lesson observed is that a small, dedicated team that understands the IPB process and how each patrol can answer PIR will provide much needed situational awareness to the company commander. Prebriefings and debriefings of patrols, with the analysis occurring in the command post are still critical to mission success. What was difficult, and impacted company Intelligence operations the most was loss of robust communications and the inability to data record/mine. The primary reporting method was FM, followed by Blue Force Tracker and in some instances, Global Rapid Response Information Package (GRRIP). One reason for the success of CoIST in COIN is routine access to SIPR and intelligence databases. The fluid fight of FSO should give us pause to rethink how we use these tools to provide Intel and improve communications access at company level.

C4ISR and the Analog to Digital Challenge. Developing the Intel Architecture in an immature environment is a monumental task considering all the communications systems, tools and sources available to a BCT. This was compounded for the BCT by having to operate in both an analog and digital environment. The deliberate process of transitioning from analog systems (mapboards and FM) to digital systems (DCGS, Command Post of the Future) was a challenge. Additionally, units must determine a method to capture data in analog form for entry into digital at a later time. The Panther architecture was structured to allow all DCGS users

access to a higher echelon tactical exploitation database (TED). As capability grew, only select BALS accessed higher DBs to reduce bandwidth usage. The BCT Fusion Warrant Officer was able to access JTF TED via GRRIP within hours of insertion; however the BNs did not utilize TED and share information with the BCT as much as they could have.

This environment also challenged the BCT staff in planning future ISR operations. The S2 was reliant on CHAT and tactical satellite to request and synchronize future ISR support, until additional digital capability was established. An additional lesson observed was one of processing, exploitation and dissemination of EAD assets. The BCT has limited capacity to exploit beyond its organic capability. During initial entry with limited communications, considerations and planning must occur between the JTF and the BCT for the exploitation and dissemination of EAD collections in support of BCT operations. Lastly, the decision point to transition ISR from a JTF fight to a BCT fight was not based on a geographic control measure. The decision to transition to the BCT was determined by the BCT's capability to monitor, communicate, and control that asset. Transitions were based on full motion video, Signals Intelligence, Human Intelligence (HUMINT), and Measurement and Signature Intelligence. Once BCT systems (OSRVT, CHAT, Trojan Spirit II, CI and HUMINT Automated Reporting and Collection Systems, and Common Ground Station) were established and operational, Intel handover from JTF occurred.

Unity of Intelligence. The Intelligence effort of the BCT must be unified in its task of answering the commander's PIRs. ISR operations must be planned and synchronized in detail to support the commander's DPs. The BCT commander remarked that decisions come faster in FSO. This requires wargaming to determine DPs with associated PIR, and developing the collection tasks in terms of time and space (NAIs). One method to ensure the unity of effort is through rehearsals. The Panthers conducted an ISR and Fires rehearsals prior to every major BCT operation, to synchronize sensor to shooter and ensure subordinate units understood their task and purpose for ISR taskings.

This unity also includes synchronizing all internal assets and includes the employment concept of the Reconnaissance Squadron. Is this unit the BCT commander's "eyes and ears on the battlefield" or is it employed as another maneuver force? Do we support the Recon SQDN with MICO assets in answering the BCT CDRs PIR or do we employ them separately? Is the Squadron commander (SCO) the Chief of Reconnaissance, tasked to execute the BCT collection plan across the breadth of the BCT area of operations, or just another maneuver force tasked with specific ISR tasks?

The Panther's concept of the operation was to employ the SCO and the Recon SQDN as the Chief of Reconnaissance; task organized with HUMINT and LLVI enablers. The SQDN was partially successful in this role, leveraging an entire staff and command group to synchronize ISR across the BCT. The lesson observed is to ensure the Recon SQDN is fully integrated into the overall BCT collection plan, that organic and higher ISR assets are task organized or synchronized to support the SQDN collection tasks, and that they are prepared to act as the SQDN identifies the enemy and answers PIR.

OPFOR UAS Capabilities. As stated earlier, "Red UAS" was a game changer. This capability added a new dynamic to the battlefield and required units to consider operational security and deception in their planning and execution. Additionally, it required predictions from the S2 on when the OPFOR was most likely to employ UAS, so as to coordinate ADA assets to counter. Lastly, the OPFOR is capable of viewing friendly UAS feeds with like capabilities, requiring adjustments to our tactics, techniques, and procedures.

In conclusion, JRTC would like to again acknowledge the commitment and determination of the Soldiers of the 3rd BCT, 82nd Airborne "Panthers". They are to be proud of their performance and we thank them for allowing us to be their partners in testing the evolving FSO concepts. It was evident to us that the foundations of intelligence operations and analysis are well known from 10 years of persistent COIN conflict. It's the environment that has the potential to change and we must be prepared to adapt to overcome it, just as the Panthers did in October 2010.

Lieutenant Colonel Haynicz is currently the Senior Intelligence Trainer/Mentor at the Joint Readiness Training Center. He has served as an S2 and S3 at the battalion and brigade level in addition to commanding a MICO and the 441st MI Battalion in Japan.

Intelligence, Surveillance, and Reconnaissance in Full Spectrum Operations

by Kirk Drennan and Heather Greaves

Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment. Mission command that conveys intent and an appreciation of all aspects of the situation guides the adaptive use of Army forces. (Field Manual 3-0 Operations)

Introduction

As a community, the Intelligence Corps` faces certain challenges in planning intelligence, surveillance, and reconnaissance (ISR) to support full spectrum operations (FSO) at the tactical level. Many changes have occurred in capabilities, doctrine, and organization. Prior to 9/11, the ISR capabilities and assets available at the division and brigade were much less than tactical commanders enjoy today. Doctrinal changes call for modifications in the way tactical forces–including tactical intelligence units–operate. Through the 1990s the intelligence community still looked at the battlefield as a linear array and arrived at echeloned solutions to meet its challenges.

That began to change with the promulgation of the contemporary operational environment (COE) around the change of the century. The COE was formally established as a training model in 2003 with FM 7-100, Opposing Force Doctrinal Framework and Strategy, which laid out how an opposing force should fight in the COE. Nevertheless the intelligence community still tended to think in linear terms in respect to intelligence coverage by echelon. Meanwhile organizational changes wrought by modularity shifted many divisional ISR capabilities to the brigade combat team (BCT).

Changes Kept On Coming

If anything, the wars in Afghanistan and Iraq have accelerated changes within the force and have left some persistent "hanging chad" when it comes to doctrinal issues. One of particular relevance to the tactical intelligence community was the question of battlefield design. The 2001 version of FM 3-0 laid out the ideas of FSO along with contiguous and non-contiguous areas of operations (AO). It retained the use of close, deep, and rear areas in describing contiguous, linear operations. The January 2005 version of FM 5-0, Army Planning and Orders Production, (replacing the standard FM 101-5) continued to use the close, deep, and rear construct to describe planning. FMI 5-0.1, The Operations Process, published in 2006, reinforced concepts from FM 3-0 and 5-0; although it dropped and adjusted some terms, it did not address the battlefield construct of close, deep, and rear.

Meanwhile FM 3-90.6, The Brigade Combat Team, was published in August 2006 to reflect the changes of modularity. It superseded FM 7-30, The Infantry Brigade (as well as FM 3-21.31, FM 3-90.3, and FMI 3-90.6). Because it addressed a modular BCT that could fight as part of a division or independently, the 2006 FM carefully laid out the concepts of FSO as well as contiguous and non-contiguous AOs. We offer what it said regarding deep, close, and rear operations:

Deep, Close, and Rear areas

2-9. The commander may use deep, close, and rear areas to describe his area of operations. In such situations, the commander directs and focuses operations in these areas of his AO. He describes his AO in terms of deep, close, and rear areas when the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC) require the use of a spatial reference.

We should also note that the 2006 FM 3-90.6 offered graphics using deep, close, and rear for contiguous and non-contiguous battlefields.

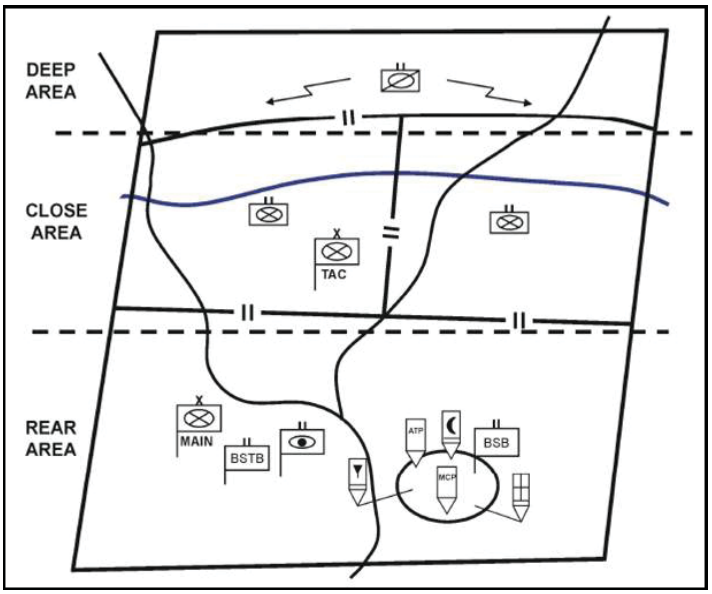


Figure 2-2. Deep, close, and rear areas in a contiguous battlefield.

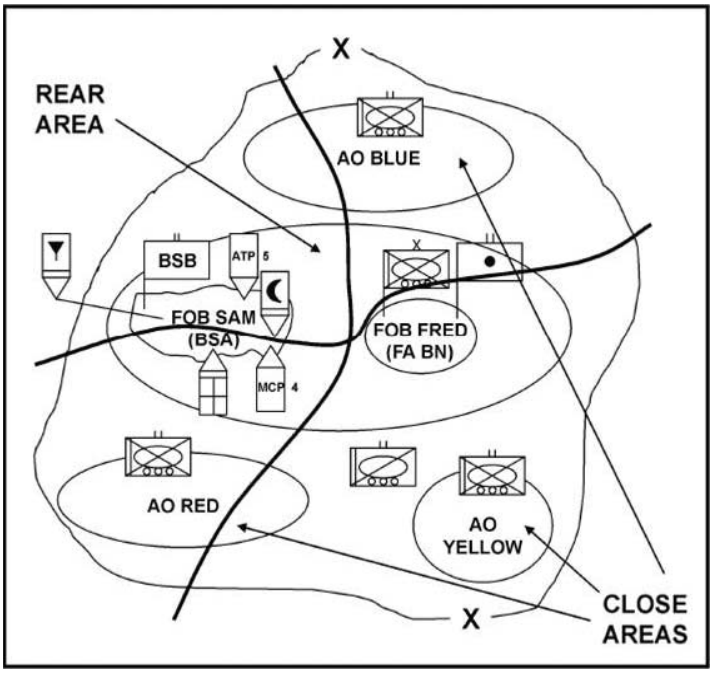


Figure 2-3. Deep, close, and rear areas in a non-contiguous battlefield.

The description of the deep area was–and still is–especially relevant to ISR: "***The BCT commander's improved ability to see in depth is one of the characteristics of the modular brigade.***" That statement reflected the reality of the modular BCT and the intent of FM 3-0 in 2001. It highlighted the increased capabilities of the modular BCT in FSO, regardless of the battlefield.

The 2008 version of FM 3-0 rescinded the terms deep, close, and rear. While it offered close combat as a replacement for "close," there were no substitutes for deep or rear. The process was similar when it came to FM 2-0, Intelligence. The 2004 version retained the concepts of deep, close, and rear just like the 2005 version of FM 5-0. But the 2004 FM 2-0 was written with a divisional G2 perspective and retained concepts such as battlefield operating systems. The 2010 version of FM 2-0 eliminated discussion of deep, close, and rear and took more of a generalist view of intelligence. The same can be said for the 2010 version of FM 3-90.6 the BCT, it offers a stripped down version of BCT operations, one without the close, deep, and rear framework. The best source for examining ISR support and planning for a BCT in FSO was–and still is–the 2006 version of FM 3-90.6, The BCT.

The BCT commander's ability to see deep became a doctrinal gap for the ISR community. He could look deep and he needed to plan for it, he just could not talk about it. FSO has again raised that issue.

FSO and the JRTC

We began this article with the official definition of FSO as it set the stage for our discussion of ISR in support of the recent FSO training rotation at the Joint Readiness Training Center. Discussions about Rotation 11-01 began in 2008. Many of those discussions centered around the idea that the rotation would involve major combat operations rather than concentrating on counterinsurgency as part of mission rehearsals for operations in Iraq and Afghanistan. For a while, the proposed rotation was commonly–and erroneously–referred to as an major combat operation (MCO) training event. Rotation 11-01 incorporated offense, defense, and stability operations as part of the rotational design.

> ***Full spectrum operations require continuous, simultaneous combinations of offensive, defensive, and stability or civil support tasks. FM 3-0***

FSO is deceptively complex. In addressing ISR support to FSO, the current (2010) FM 2-0 discusses intelligence support to the elements of FSO. The current FM 3-90.6 does the same. That is an artificial convention because it allows one to examine offensive, defensive, and stability operations or civil support separately. FSO dictates those forms of

combat operations will occur within a unit's operating environment (OE).

A battlefield today could include some or all of the following:

- Special operations forces and paramilitaries still scattered throughout the battlefield.
- Political entities in hiding.
- Weapons of mass destruction unaccounted for.
- Massive refugee situation, in the cities and on the roads, affecting our ability to move.
- Emergence of an insurgency (led by the paramilitaries.)
- Famine and disease outbreaks.
- Collapse of rule of law, and civil capacity.
- Possible foreign MCO intervention.
- Collapsing infrastructure to include deteriorating roads, bridges, and dam breaches, all of which affected our freedom of movement, and our own sustainment operations.

Rotation 11-01 encompassed many of those requirements and in doing so challenged BCT ISR planners. As stated earlier many changes had taken place within the Army. An entire generation of MI officers had entered the Army who had never considered ISR to support an offensive or defensive operation, much less FSO in its totality.

Synchronizing the ISR Fight in FSO

ISR synchronization remains critical in providing battlefield commanders the intelligence required to make decisive decisions at critical times. FSO, if anything, heightens that need because even with the increased ISR capabilities resident in the modular BCT, the ISR planner has only so many tools in the ISR kitbag. The ISR plan cannot focus entirely on one element of the operation. In rotation 11-01, the BCT conducted security and stability operations across its rear as it mounted a shaping attack on a secondary objective to set the conditions for its decisive attack beyond. In all of this, the BCT maintained a defensive posture around its initial airhead. It was in all regards a near perfect display of the concepts of FSO.

The basics of ISR did not change in meeting these challenges. What did change was the degree of ISR integration across the entire staff. The ISR plan was no longer "the S2's plan." The ISR plan was integral to the commander's concept; synchronization of the ISR plan was a command priority. While the S3 was doctrinally responsible, development of the ISR plan routinely fell on the brigade S2 since he or she normally coordinated ISR assets and was the primary user of ISR products. The complexity of the FSO rotation meant that the S3, S2, and other staff elements were required to work together to develop the ISR plan. In order to drive the staff planning process, FM 2-01 identifies the commander's role in providing guidance to his or her staff in planning for ISR:

The Role of the Commander in ISR Operations

The following list was developed by General William W. Hartzog and used by the Army's Battle Command Training Program in teaching ISR operations. It concisely details the commander's role in ISR operations:

- To defeat the enemy, you must tell your intelligence officer what you must know and when you must know it.
- You must tell your Operations officer that every plan must be coordinated with your intelligence officer.
- You must know what intelligence systems are available to support you and what their capabilities are.
- You and your staff must participate in the IPB process. Do not let your Intelligence officer do IPB by himself/herself.
- You must decide who is responsible for controlling your recon effort and assign them the assets and mission.

Additionally, these additional steps support successful ISR operations:

- Limit PIR and constantly check to be sure they are being collected on. Ensure your Intelligence and Operations officers are not diffusing the collection effort. A unit generally will not have enough assets to cover all intelligence gaps.
- Synchronize ISR operations with higher headquarters and make sure subordinate commanders have synchronized their plans with yours.

Relooking Close, Deep, and Rear

The first step in synchronization is establishing a common framework to facilitate understanding of the OE. As Rotation 11-01 demonstrated, the ISR fight is the BCT commander's fight. As such, it should be framed in the same terms as the decisive, shaping, and sustaining operations against which the BCT commander commits the BCT. Ultimately, ISR operations must be nested from division to company level to ensure integration of all available assets towards a single purpose that results in increased security and flexibility to gain and maintain the initiative. This is critical when commanders plan combat operations within their area of responsibility (AOR). In a widespread battlefield with multiple ongoing operations, allocation of combat and ISR assets should and must share common control measures.

We believe that the terms close, deep, and rear, as discussed in the 2006 version of FM 3-90.6, are of great value in describing the battlefield during FSO.

BCTs will face a more sophisticated as well as more powerful adversary in the future that can fight as a cohesive unit but still decentralize its efforts. As BCTs prepare the OE for defensive and offensive operations they will have to contend with security issues in their rear as well as providing situational awareness and target acquisition in their close and deep fight. Certainly that was the case in Rotation 11-01.

Using close, deep, and rear allow us to better define each echelon's AOR in ISR planning. In the past, these areas took on certain characteristics in order to coordinate responsibility for collection requirements based on organic ISR capabilities and availability. Intelligence coordination lines were established on the battlefield in order to define those responsibilities. These lines could be based geographically or time phased depending on the circumstances.

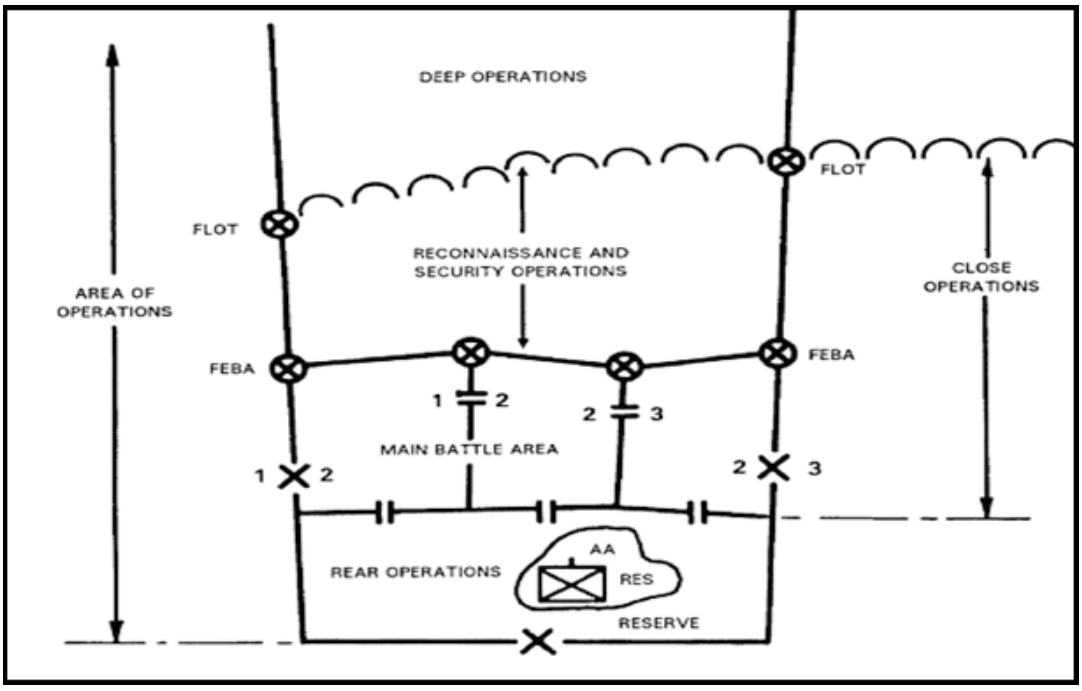


Figure 5-1. Defensive framework. (From FM 3-90.6)

For today's battlefield it may be more useful to define close, deep, and rear in terms of combat power. The demarcation between close and deep then becomes the distance from the forward edge of the battle area (FEBA) into enemy held terrain that the commander's weapon system with maximum range can "reach out and touch" the enemy. The close and rear fight are demarcated by the distance from the FEBA into friendly held terrain that the enemy's weapon system with the greatest range can "reach out and touch" friendly forces.

Regardless of definition, effective ISR utilization, triggers, and handovers must fall under the commander's concept of the deep, close, and rear fight. Unless directed by higher, the commander is the only one who can define these fights whether through timing, geography, or mission completion. He must ensure that his staff understands them. In cases where he uses a definition different than that used by his higher headquarters, he must give his staff guidance on how he expects them to nest their criteria with those of their counterparts in higher headquarters. Commanders must also realize that their defined deep fight will often surpass that of their subordinate commanders due to more robust assets, larger staffs and greater planning windows.

The question becomes at what distance from the FEBA is the commander able to register credible effects on the enemy and at what distance is the enemy able to register credible effects on him. In terms of ISR, this depends on the organic assets the commander possesses because each asset's capability differs impacting its ability to collect. The ability to plan for the close, rear, and deep fight depends on the capabilities the organization possesses.

Commanders at all echelons can nominate targets outside of their defined close fight. If the asset used to observe the target is pushed into the tactical control (TACON) of the lower level commander, the lower level tactical commander's close fight is effectively increased. In this case there must be a clearly defined point in time and space at which the observing asset transitions from TACON Higher to TACON Subordinate.

The 2006 version of FM 3-90.6 offers a useful discussion of reconnaissance handover. In part it states:

4-63. Reconnaissance handover (RHO) is the process of transferring information and/or responsibility for observation, or surveillance of potential enemy contact, or an assigned area from one element to another. It may cover a sector/zone, NAI, TAI, and/or threat contact. RHO can involve visual, electronic, or digital observation and information sources in any number of combinations. RHO is usually associated with a designated reconnaissance handover coordination point, or a PL designated as a reconnaissance handover line.

4-64. RHO shares many critical tasks with battle handover, including relief in place, linkup, and passage of lines. Unlike battle handover, however, RHO can take place without being in combat or being within threat direct fire range. Instead, it focuses on planning, preparing, and executing the seamless passage of information, threat contact, or an assigned NAI—and the related responsibility for it—from one element to another without loss of contact.

It's All About Framing Transitions

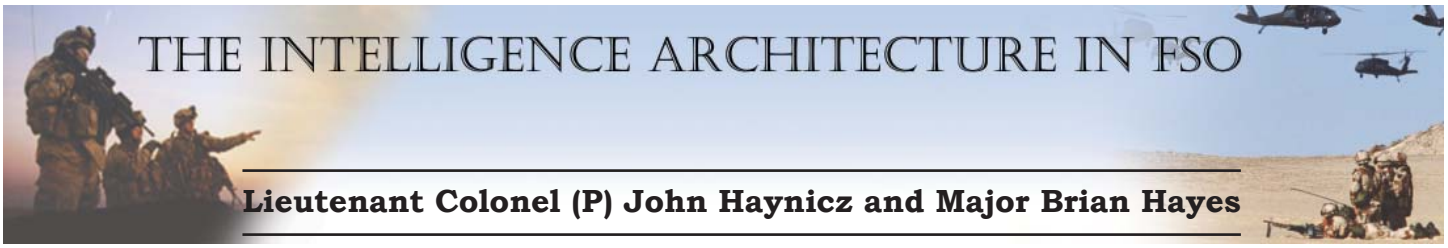
Using close, deep, and rear allows a higher headquarters to develop the common operational picture outside a subordinate unit's AO and identify targets that may impact them as they try to achieve tactical and operational objectives. Subordinate units must be aware of the overall objectives of their higher headquarters because this will dictate what ISR assets can be allocated for their own use. It is the responsibility of the higher headquarters to provide intelligence that may impact the subordinates close fight whether they are expanding their AOR, defending, or conducting offensive operations.

The deep fight requires coordination between higher and lower echelons to provide situational awareness and target development as units transition from one type of operation to another. Those transitions–just like the definition of close, deep, and rear–can depend on geographic, timing, or operational considerations. A BCT could, for example, shift from a defensive posture into an offense, even as it maintains a defense around a key feature like an airfield. That is exactly what happened in Rotation 11-01. In that case, the defense of the airfield, formerly the close/close combat area, became the rear fight for the BCT and the deep area shifted west to encompass the area of interest and influence beyond the objective for the offensive.

The essence of FSO is the fluid battlefield, regardless of the OE. Doctrine helps frame that battlefield to facilitate situational awareness and synchronized operations, driven by effective ISR. We submit that resurrecting the concepts of close, deep, and rear in framing that battlefield is necessary to synchronizing the ISR fight in FSO.

Mr. Drennan has been an ISR contractor/instructor for TRADOC G2 in support of the ISR TOPOFF program. He currently supports JRTC rotations as the JRTC OPS GRP G2 Division Collection Manager providing ISR training and mentoring during each rotation. He retired in 2010 after serving for 24 years in the U.S. Army as an Intelligence Officer and has multiple deployments in support of Operation Iraqi Freedom. His most recent positions prior to retirement were the Corps Analysis and Control Element Chief and the Corps Deputy G2 for the XVIII Airborne Corps.

Ms. Greaves is a contractor with the 505th Operations Squadron Joint Integration Team. She served in the U.S. Navy as an Intelligence Officer for six years with assignments in Japan, Afghanistan, and CONUS. She has worked in the fields of Strike Intelligence, Collections, and Special Warfare. She holds an MA in Anthropology from California State University, Fullerton.



THE INTELLIGENCE ARCHITECTURE IN FSO

Lieutenant Colonel (P) John Haynicz and Major Brian Hayes

"Harder to Do Than I Thought"

Developing, implementing, and sustaining an Intelligence Architecture is a monumental task for any brigade combat team (BCT) S2. Considering all the communication and collaboration systems, analytical tools and databases available, a BCT S2 shop can quickly become overwhelmed. Extended operations in Operations Enduring Freedom/ Iraqi Freedom/New Dawn have afforded Intel Architectures to mature and grow overtime, allowing in some cases for stable and robust communications, rapid access to intelligence databases, and uninterrupted connectivity to intelligence, surveillance, reconnaissance (ISR) systems and platforms.

During Joint Readiness Training Center (JRTC) rotation 11-01, the 3/82nd ABN was presented with the challenge of developing an Intelligence Architecture in an immature environment. Establishing the Intel Architecture was the "harder to do than I thought" event for the BCT S2. This article will discuss three challenges as noted by the BCT S2 and the trainer/ mentors of the JRTC:

- Establishing a communications plan.
- The digital-analog-digital transition.
- The reconnaissance handover (RHO) from the joint task force (JTF) to the BCT.

Communications

In establishing a communications plan, JRTC coaches a method using the acronym PACE (Primary, Alternate, Contingency, and Emergency) communications methods. This is to emphasize the development of multiple redundant methods to communicate during operations. In our current digital age, units must consider PACE not only for voice communications, but for data transfer as well. The BCT S2 had to establish an Intelligence information PACE for each phase of the operation (Intermediate Staging Base (ISB), In-Flight, Initial Entry, Follow On Operations) and adjust the PACE as communication capabilities improved with the JTF and with subordinate units. Considerations for PACE development included JTF communication systems, airflow of assets and availability of unit equipment, and coordination/communication with the BCT S6, or signal officer. The discussion in this article will focus on the In-Flight and Initial Entry phases of the operation. Due to rotational design, the ISB portion of the exercise was condensed and consisted only of a Green Ramp Intelligence update provided by the JTF.

The In-Flight phase of the operation planned for the use of JACC/CP (Joint Airborne Communications Center/Command Post) and Secure En-route Communications Package-Improved platforms The key information to communicate was a six line Intelligence update, sent 20 minutes before commencing airborne operations. The PACE for all BCT communications during this phase consisted of the following:

P: mIRC Chat.

A: TACSAT (The primary communication method between aircraft).

C: UHF (U.S. Air Force communications).

E: FM (limited).

Unfortunately, the JACC/CP was ultimately removed as a communication platform for the operation, forcing the BCT S2 to revert to the alternate method of TACSAT. Having established and communicated a working PACE with the JTF prior to operations allowed for a rapid transition. The six line Intel update was successfully communicated from the JTF to the BCT, providing critical intelligence information on the condition of the field landing strip and enemy disposition. For initial entry operations the BCT S2 PACE plan was as shown below:

Airborne Insertion (On DZ)			
Voice		Data	
P:	FM	P:	GRRIP
A:	mIRC	A:	
C:	TACSAT	C:	
E:	IRIDIUM	E:	

The unit employed an organic, air-droppable tactical command and control HMMWV (named the SHARC) uploaded with multiple communication and analysis systems for rapidly establishing command and control immediately following the airborne insertion. For the Intelligence section, communication systems for initial entry included GRRIP (Global Rapid Response Information Package) for primary digital communications loaded with "mIRC chat" capability and a stand-alone Distributed Common Ground Station-Army (DCGS-A) to process data. For communication with Battalions, the PACE was primarily the same, replacing the Iridiums with Blue Force Tracker/Force XXI Battle Command Brigade and Below (BFT/FBCB2), and as a last resort, runners.

This plan was effective in communicating with subordinate battalions during the initial insertion. As operations continued and the BCT footprint increased, FM communications were strained due to distance, necessitating the use of digital systems. For communication with the JTF HQ, FM communications never materialized and the BCT S2 exercised their alternate plan, immediately switching to mIRC Chat over GRRIP. This was very successful in communicating and passing data. However, had the GRRIP system failed, there was no redundant method for data exchange and therefore would have severely limited intelligence support and coordination during the initial phase of operations.

As stated earlier, the past decade of persistent conflict has afforded units the ability to fight digitally, using assured communications and access to data. The rotational unit employed all of their digital systems in the planning and preparation phase prior to operations. The unit then shifted to analog systems for Initial Entry operations, requiring those units without connectivity, particularly at company and battalion level, to fight from analog systems, mainly FM radios and mapboards. BFT was included in the PACE plan, but use was limited. The plan for the employment of the DCGS-A called for all pre-deployment Intelligence products and extracted data to be copied to all operator laptops prior to departure in anticipation of the period of limited to no digital communications inherent in initial entry operations.

This concept of operations (CONOP) was intended to allow operators at all echelons to continue to produce mapping, link diagramming, spatial, and temporal analytical products digitally using data current as of departure from the ISB as long as there was power available. Collaboration across all elements, as well as current data updates from higher headquarters (HHQ), was intended to be accomplished using DCGS-A Offline Case files and ARC Shape files transferred via the unit's PACE plan. Once full Army Battle Command Systems (ABCS) capability and digital connectivity was established, the intent was to shift collaboration and data update functions to the BCT and HHQ ABCS Publish and Subscribe Servers as designed.

The BCT HQ established partial digital connectivity within four hours after initial entry and full digital connectivity on D+2. The Battalions followed with full connectivity by D+3. The unit's plan for employment of DCGS was successful and facilitated limited situational awareness at the BCT level. GRRIP was also successful as an initial connectivity platform. The Brigade Support Element (BISE) Chief was able to communicate with JTF counterparts (via GRRIP mIRC Chat) within hours of Initial Entry and was able to access data resident on HHQ systems, receive data updates via Offline Case files, and disseminate data to subordinate elements via Offline Case files shortly thereafter.

The Digital-Analog-Digital Transition

The unit learned that the transition from digital-analog-digital must be a deliberate, planned process. As discussed above, the PACE plan must be identified by specific system with redundant methods. The plan for DCGS connectivity must be developed and understood by all operators. Additionally, the BCT should not wait on battalions to establish digital capability, but should direct a set date-time-group for subordinates to establish connectivity by a specific system. This needs to be wargamed, synchronized and resourced, as with any operation. To ensure success, future units should employ plans similar to 3/82nd for initial operations considering redundant communication systems whereby all analysts have access to data until more mature communications and servers are established. As such, 3/82 ABN chose not to employ their organic DCGS-A Intelligence Fusion System (IFS) server sets at the maneuver Battalions after considering the following issues:

1. A qualified field support engineer (FSE) is required to administer and set up the IFS. The current maintenance CONOP for DCGS-A prohibits administrator level access by anyone other than a qualified DCGS-A FSE except by specific authorization from the system Program Manager's office. While the BCT had negotiated this authorization, the four designated Soldiers were all assigned to the BISE which left no one at the three IFS owning maneuver Battalions with the level of access required to either power-on or power-off the DCGS-A IFS server sets. Given the dynamic nature of FSO, the probability that a Battalion would be forced to displace in reaction to enemy activity without the time or security required to transport someone authorized to properly bring the IFS down from the BCT made it impractical to establish the Battalion IFS. This issue must be part of the unit's Intelligence Architecture planning process and the necessary coordination, authorization, and training must be in place well in advance of deployment.

2. IFS-to-IFS synchronization requires robust, stable communication. While DCGS-A remains a powerful weapon in the Intelligence Analyst's arsenal even without access to an IFS, the ability to collaborate effectively and efficiently with other analysts, as well as the operators from other Warfighting Functions, and access to near-realtime data for ongoing product development is significantly impacted by the lack of connectivity. Achieving these effects however, comes at a significant price in terms of the amount of communications bandwidth potentially consumed in the process. The next step in collaborative efficiency beyond the use of offline case files mentioned above calls for the synchronization of the operator's Tactical Entity Database (TED). This process consists of transmitting copies of the battalion TEDs to the brigade IFS where they are imported, compared to eliminate duplication, and merged into a single master database which is then transmitted back down to the battalion IFSs. The potential negative impact on bandwidth is significant and only increases as the operational environment evolves.

Lastly, a significant challenge faced by the unit was the capture, tracking, and transfer of data from analog to digital systems. Rough estimates concluded approximately 50 percent of the information gathered during the first three days of operations was lost and never digitally captured. Intelligence sections at all levels must take steps to properly capture data during this analog period and transfer via data entry at a later time. Again, this must be a deliberate process. Additionally, Soldiers can still use their DCGS-A systems without connectivity. Data can still be entered for pattern analysis and the use of tools without being connected to the network.

RHO to the BCT

The planning for and executing of the RHO from JTF control to the BCT fight is another critical consideration when planning the architecture for FSO. The ISR capabilities for a BCT have grown exponentially with the transition to the modular brigade. Both physical control of unit assets and capabilities to access the data and temporarily control theater assets have allowed BCTs to "see" and detect as far as a division. In the past, "fights" were classified as the deep, close, and rear, where the HHQ was responsible for the deep fight and would pass Intelligence assets and the threat formations off to subordinate units at predetermined geographic control measures. Now, we fight in contiguous or non-contiguous environments and utilize a multitude of organic systems or request access to theater sensors.

For this operation, a conditions-based approach was used wherein the RHO was determined based on the BCTs capability to monitor, communicate, and control specific assets. Initially, the JTF was responsible for providing all the intelligence support the BCT required as it transitioned from ISB to Initial Entry.

As the BCT established systems and built capacity, transitions for ISR such as database access, full motion video, Signals Intelligence, and Measurement and Signature Intelligence occurred. Key to implementing this operation is communication between JTF and BCT, including understanding BCT PACE plan and Digital Transition plan. Additionally, the HHQ must fully understand the BCT collection plan, priority intelligence requirements, and Intelligence operations for the Initial Entry phase in detail to support BCT efforts. Lastly, RHO includes not only passing control of assets from one HQ to another, but the transfer of data and intelligence collected by those assets in support of the BCT fight, requiring digital capability at the BCT level.

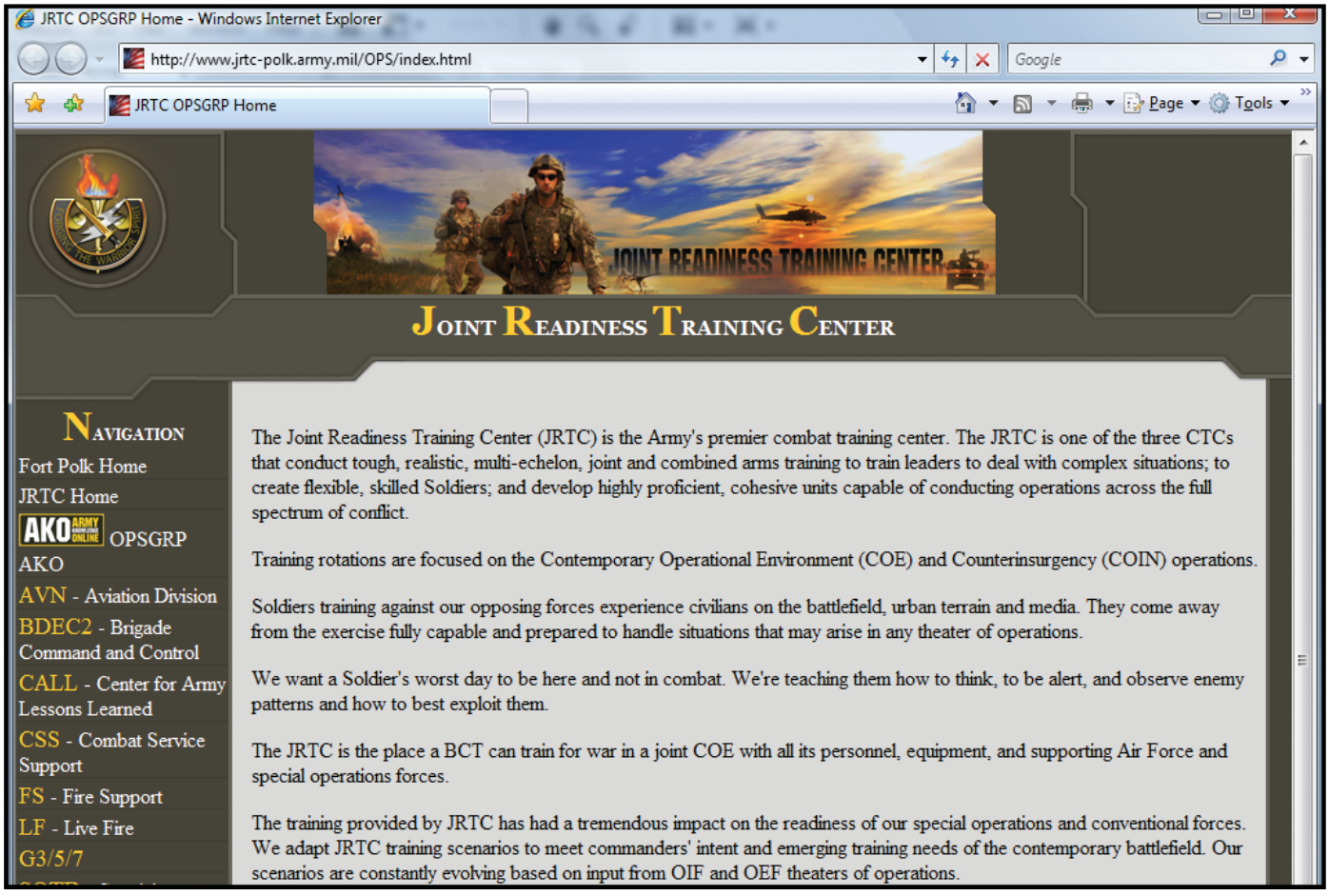
Conclusion

A functional Intelligence Architecture is paramount to collecting, analyzing, and disseminating intelligence in order to drive operations in any environment. Having to develop and sustain an intelligence architecture in an immature environment is a daunting task at any level. The three identified observations from this rotation of establishing a functioning PACE, preparing and executing a digital/analog transition, and coordinating a detailed RHO can assist in successful accomplishment of this mission.

Lieutenant Colonel Haynicz is currently the Senior Intelligence Trainer/Mentor at the JRTC. He has served as an S2 and S3 at the battalion and brigade level in addition to commanding a MICO and the 441st MI Battalion in Japan.

Major Hayes has over 10 years experience in the Army as an Intelligence Officer. He has served as the MI Company Senior Trainer/Mentor and currently serves as a scenario planner at the JRTC. He has deployed three times to Iraq where he served as an assistant Brigade S2/Collection Manager, Brigade S2X, Battalion S2, and MI Company Commander.

Check out the JRTC website at
http://www.jrtc-polk.army.mil/OPS/index.html



The Role of the Company Intelligence Support Team in Full Spectrum Operations

by Thomas Tomes and Christopher Maxwell

Introduction

In the usual theater mission rehearsal exercises (MRE) at the Joint Readiness Training Center (JRTC), the Company Intelligence Support Team (CoIST) in each maneuver battalion (BN) is pivotal in supporting company commanders (CO Cdrs) and BN S2s. Rotation 11-01 with the 3rd Brigade Combat Team (BCT), 82nd Airborne Division was the first full spectrum operations (FSO) rotation at JRTC in eight years. Recognizing that CoISTs should play a role in FSO, 3/82 ABN elected to use a modified CoIST concept with CO command posts (CPs) serving this critical requirement among all of its other requirements.

What was discovered during the BCT's rotation is that FSO does not lessen the need for CoISTs at the maneuver company; it modifies the mission's priorities and adds to them. During this rotation, both the 3/82 ABN and JRTC observed several CoIST challenges. This article will discuss three of those challenges:

- Manning a CoIST for FSO.
- Resourcing a CoIST with appropriate automation and communication resources.
- Establishing standing operating procedures (SOP) for CoISTs during FSO.

Building the CoIST

The initial challenge for the BCT was to select the right Soldiers to build these CoIST cells and provide those Soldiers with the necessary tools and training. CoISTs may not be the three to five man elements normally seen in a counterinsurgency (COIN) rotation because of manning constraints and priorities but they need to have the same functionality. They must be properly configured and properly trained. The Army has become much more technologically advanced in the last 10 years and is able to process much more data as compared to previous decades when we last trained for FSO. Analytical and battle tracking cells (CoISTs) at the lowest level help process this data in a near real-time environment. The Army must continue to allocate resources such as Soldiers, equipment, and time to "train" on critical CoIST tasks such as intelligence preparation of the battlefield, CoIST system technology, battle tracking, report writing, and other skills to be successful.

"CoIST-like" duties were assigned to the CO CPs as opposed to identifying an independent element to perform these functions. These CPs used SOPs specifically designating responsibilities, processes, and formats as well as a primary, alternate, contingency, and emergency (PACE) plan for communications. No two CP SOPs were the same for 3/82 ABN with respect to CoIST duties. This caused much confusion across the BCT and never allowed the Intel War Fighting Function to effectively connect from CO to BCT. Having an independent CoIST, resourced with personnel and equipment, and clearly assigning that intelligence functions would have significantly enabled 3/82 ABN to make the intelligence connection. Additionally, CoISTs would have assisted BCT CO Cdrs understanding of the threat and assisted BN S2s with threat analysis at the company level.

Soldiers manning a CoIST do not have to be intelligence analysts. In most cases, a BCT will likely not have the MOS 35F, Intelligence Analyst Soldiers available to man each maneuver company CoIST.[1] The BCTs will continue to have to train other Soldiers already in the company on how to generate, build, and update map graphics and how to push and pull information from the BN S2 over the FM operations and intelligence (O/I) net. This is a full time requirement and cannot be effectively managed by the Soldiers manning the CO CP. The BN or BCT S2 should create an SOP with the Cdrs and S3s that specifically defines a digital and analog PACE plan along with a timeline of how information and intelligence will be passed vertically.

Automation Obstacles

The second challenge for CO CPs during this FSO rotation was the reduced communication capabilities (both digital and analog). During a JRTC MRE rotation, communication capabilities organic to the unit or JRTC issued, are shipped in on convoy logistics patrols or signed over from the outgoing unit and are setup at the CO CP with little effort or

friction. The challenge seen during the FSO rotation was that 3/82's communications systems were limited due to the forced entry airborne insertion. It had only those automation systems each paratrooper jumped in with or air-landed on follow-on aircraft after the airfield became secure. As an interim fix, 3/82 ABN elected to pass all information within the company and to higher HQ over the command net via FM. There was no designated O/I net for intelligence related information nor were there digital systems at the company level to pass intelligence information.[2]

During 3/82 ABN's rotation, BN S2s would generally pass intelligence information to the BN tactical operations center (TOC) radio operator, or a battle captain to be forwarded to companies, troops, or batteries. Subordinate companies would push intelligence information in reverse over the BN command net to the BN TOC. This process provided the BN S2 limited visibility and no direct contact with companies to assist with the Threat Common Operating Picture (T-COP). S2 situational awareness and understanding were therefore limited. Most information relayed through the BN TOC was in the size, activity, location, unit, time, and equipment (SALUTE) format. The BN S2 section would then expend a significant effort trying to analyze incomplete reporting, often resulting in an inaccurate threat assessment. If CoISTs had been formed and active, the basic analysis of enemy activity could have occurred at the company level, providing BN the beginnings of a T-COP as opposed to raw, incomplete information.

Planning for an FSO mission should incorporate CoISTs; units need to understand that these requirements still exist. Communications and processes are the basic building blocks that must be assembled to complement training Soldiers. Historically, the O/I net was the way to pass information in an analog environment and could have served 3/82 ABN well if the company CPs and BN S2s had run this net. The SOP for all units should address the use of the O/I net to pass information directly to the S2 section at BN and prevent a saturation of the BN Command net. Additionally, instead of using SALUTE reports to pass information, units should consider developing a debrief format for any patrols or key leader engagements that could be passed over FM O/I nets.

Included in 3/82 ABNs PACE plan was the Blue Force Tracker (BFT). While the BCT had the capability to communicate via BFT it lacked operator proficiency. Soldiers operating the BFT could not text other elements because of what they believed to be encryption problems. In reality, there were no encryption issues as the units were capable of observing blue force movements on the digital map, which uses the same encryption devices. BFT is a viable option for a means of communication. The system is able to send enough information, in a single or multiple messages, to interact with other elements within the patrol and send situation reports to and receive requested information from their respective CO, BN, and BDE.

3/82 ABN issued Biometric Automated Toolsets (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE) kits to some maneuver companies that had the primary mission of owning battle space and a distinct requirement to interact with the local populace. Unfortunately, the units did not plan on how to transfer collected data in the HIIDE from the company to the BN to be synched with the BAT computer, and ultimately uploaded into the BAT server. To address this issue, 3/82 ABN tried "a HIIDE for HIIDE" swap; logistical convoys from BN brought additional updated HIIDEs and swapped them with the ones the company had filled with entries. This procedure was somewhat successful, depending on having enough HIIDEs to swap and being able to reach the companies. Operational tempo and battle space restrictions meant companies often did not get new HIIDEs or send HIIDEs to be synched to the BN. This resulted in a significant lag in valuable biometric data getting to companies or getting into the larger BAT database for other companies and BNs to see.

FSO and Intelligence SOPs

Another issue identified by the trainer/mentors and 3/82 ABN was that there was no BCT or BN SOP or format to get finished or refined intelligence products from one echelon to another. Often, intelligence summaries collection requirements, target lists, requests for information, and other products developed by the BN S2s were seldom distributed down to companies as there were no independent CoISTs to receive this information. The "CoIST-like" CO CPs attempted to process this information received from BN S2s but were often overwhelmed

with operational requirements.

Patrolling is just as essential in FSO as it is in COIN, and patrol pre-briefs and debriefs are just as critical during FSO as they are in COIN. A poorly briefed patrol is placed at unnecessary risk as they do not understand the current threat, and a patrol that is not debriefed causes the loss of valuable intelligence for the commander. Without an established CoIST SOP or functioning independent CoISTs, 3/82 ABN struggled with pre-briefs and debriefs simply because no one was specifically assigned that responsibility in the CO CPs. BN S2s had developed standard formats to pre-brief and debrief patrols, but they were often not used. When companies did pre-brief or debrief, they were often incomplete and vague due to competing requirements within the CO CP.

Whether in COIN or FSO, the crucial information that patrols seek must be refined in patrol pre-briefs and collected in debriefs. This information is not only relevant to the company but can assist with further refining the BNs' and BCT's T-COP. If a standing CoIST is not resourced, a standardized or abbreviated pre-briefing/debriefing format that draws out more essential information than just a SALUTE report can be used so that anyone within the CO CP can pull and push information to patrols, conduct analysis for CO Cdrs, and provide that information to their higher headquarters.

Because of the limited communications from companies to BNs on debriefs and key leader engagements, targeting at the BN level suffered. Often, there was no identified plan for personality targeting or a formalized process to identify potential targets to the BN. For the company to contribute to targeting, the CoIST must understand the BN's lines of effort or concept of operations, priority intelligence requirements (PIR) and high value targets. The company can then nominate targets nested within the BN's concept of operation. With targets identified, it would be beneficial to conduct predictive analysis at the company level to fully understand the second and third order effects of any targeting effort. Predictive analysis is critical for companies to successfully nest within any BN effort.

Conclusion

With the significant amount of reporting to navigate through, not enough man power, automation issues, and dissemination issues, CO CPs were often overwhelmed and unable to perform the necessary requirements that a CoIST is designed to address. As a result, companies did not effectively perform precise target analysis, BNs struggled with target analysis, and both companies and BNs had difficulty accurately assessing the enemy situation which left many unanswered PIR/SIR and intelligence gaps. Companies struggled with the refinement of the threat situation and BNs and the BCT were forced to often rely on reporting, specifically Human Intelligence collection teams and echelon above brigade Signals Intelligence, rather than incorporating company assessments into their T-COP.

By not fielding formalized CoISTs with specific duties and responsibilities outlined in SOPs, companies, troops, and batteries during this FSO rotation depended solely on their respective BN S2s for all intelligence information and threat analysis. In any environment, FSO or COIN, CoISTs are more than the first level of analysis of information for the CO Cdrs. If manned and trained, a CoIST can offer a more accurate and timely intelligence picture for their respective company than the BN S2 or BCT S2.

Endnotes

1. The British have been doing this for years as part of their Northern Ireland operations. U.S. BCTs have used a similar concept in manning CoISTs at the JRTC and deployments to theater. A standard fly-away training package for CoISTs and "extended" company CP operations across the FSO spectrum is needed.

2. This was part of a larger digital-to-analog transition issue that characterized the rotation.

Mr. Tomes has been a CoIST instructor for NSTID/TD at Ft. Huachuca for the past 2 years. and the JRTC CoIST Site Lead for the last 12 months. He served for 25 years as a member of the U.S. Army Chemical Corps. Mr. Tomes has served in Germany, Iraq, Saudi Arabia, Kuwait, and Korea as well as CONUS.

Mr. Maxwell has over nine years experience in the intelligence community with extensive experience in intelligence operations. He has a diverse career with strategic analytical experience in the Central Command's Information Dominance Cell and Intelligence Command's Intelligence Operations Center. He has deployed to Afghanistan supporting multiple large-scale operations and battles such as Operation Rock Avalanche and the Battle of Wanat with the 173rd Airborne BCT. He assisted in the development of the JRTC CoIST program as the JRTC CoIST Integrator. He is currently a Senior Consultant in Fort Polk's Counter Improvised Explosive Device Integration Cell, focusing on CoIST and Biometrics.

Military Intelligence Company Support to Brigade Operations:

Integrate to Synchronize

Major Gualberto J. Marrero III

In past rotations, the Military Intelligence company (MICO) of the brigade special troops battalion (BSTB) has struggled to make full use of its intelligence collection assets as part of a mission rehearsal exercise (MRE). Rotation 11-01 was not an MRE; it was the first full spectrum operations (FSO) rotation in eight years at the Joint Readiness Training Center (or any of the combat training centers). Nevertheless the MICO encountered the same difficulties that plague a MICO from effectively providing and synchronizing intelligence, surveillance, and reconnaissance (ISR) assets.

When the MICO struggles, the brigade it supports cannot see the enemy clearly or maintain an accurate picture of the battlefield. MICO commanders and brigade combat team S2s must work together to synchronize and manage MICO assets. Otherwise systemic issues will disrupt MICO efforts to provide synchronized assets. These issues beginning with poor MICO integration with the brigade (BDE) S2 shop, are exacerbated by an ineffective primary, alternate, contingency, and emergency (PACE) communications plan, and brought to full effect by a poor understanding of their collection capabilities in general. The result is a severely degraded collection effort. The BDE intelligence warfighting function does not fight as a team, cannot communicate effectively in that fight, and cannot agree on what to collect because it does not understand how. The first indicator of just such a failing collection effort is a MICO that cannot manage and track its assets for the BDE. Fixing that issue is therefore a great leap forward for the MICO in bridging the gap with the BDE Staff, thereby enabling intelligence to drive BDE operations.

The effort begins with a common understanding of collection capabilities and the requirements necessary to make full use of those capabilities. The MICO must clearly define its assets and capabilities by mission roles to the BDE Staff, not just the BDE S2. The MICO sections should analyze their capability and recommend how best to employ that capability for the BDE S3 as well as the BDE S2. Such recommendations must include operational requirements and limitations. For example, each section should analyze the terrain to identify possible locations that will allow the best emplacement for collection. This will, in turn, allow the MICO commander to clearly articulate the capabilities and limitations of the respective systems and the second and third order effects of diverting an ISR asset away from its recommend location. The MICO commander must continue to provide a clear task and purpose to every ISR asset so that effective ISR feedback is provided to the BDE. Once the assets are emplaced, the MICO command post (CP) must track all systems in a running estimate updated with specifics on:

- Current status of asset (location, personnel, and system.)
- Information the asset can provide (its intelligence collection "foot print.")
- Requirements needed to be able to provide that information.
- How the current task organization impacts collection capabilities.

Tracking must be done carefully and consistently. When more than one shop tracks the same equipment you end up with an erroneous picture of system status within the BDE. Keep it simple. The MICO owns the equipment; the MICO CP should track its status and provide it to the BDE Staff on a daily basis on trackers. Trackers allow the BDE Staff to synchronize ISR assets across the BDE. These trackers will ensure the BDE S2 has a clear picture of its intelligence collection "foot print" and identify any intelligence gaps across the BDE's lines of effort (LOE).

Targeting is another critical area where many MICO commanders miss a golden opportunity to integrate with the BDE S2 specifically and with the entire BDE staff in general. As stated above, the MICO commander is by mission and organization the subject matter expert on MI collection assets in the BDE. Yet the MICO is rarely involved in the military decision making process (MDMP) and BDE targeting process. Instead the MICO reacts to requirements coming from these processes rather than participate in them to identify intelligence gaps and recommend asset selection for all phases of the operation.

Communications and information exchange between the MICO and BDE S2 are limited by the absence of well established standard operating procedures (SOP). Failure to fully understand and implement an effective SOP leads to a lack of understanding of how the MICO supports the MDMP process. A well established SOP dictates how the MICO integrates with the BDE S2 shop and define those roles between these two elements. The SOP should include a PACE communications plan to support that integration.

Every organization struggles with where the MICO commander fits into the puzzle. Is the MICO commander a collection manager, asset manager, or an analysis and control element chief? Does the MICO commander work for the BDE S2, the BDE S3, the BSTB commander, or the BDE commander? The BDE commander who establishes roles and responsibilities for the MICO commander will help alleviate some of the frustration between the BDE S2 and the MICO. MICO commanders should be involved in every assessment and mission analysis meeting and integrated into the BDE targeting cycle so that they clearly understand the identified intelligence gaps associated with the BDEs LOE. Without MICO expertise the efforts to apply assets to confirm or deny threat courses of actions or to answer intelligence gaps will be desynchronized across the BDE. Clearly defined priorities of work and duties and responsibilities within the BDE S2 are vital to the success of the MICO's integration into the BDE.

If information is important for successful operations, its timeliness is crucial. Often, the MICO does not have effective contingency plans to get information from its own assets when digital communications go down or during movements. It is absolutely critical to maintain communication to all MICO assets. The most important question to ask in devising a PACE plan is "How does the asset report information?"

Defining the PACE in the MICO

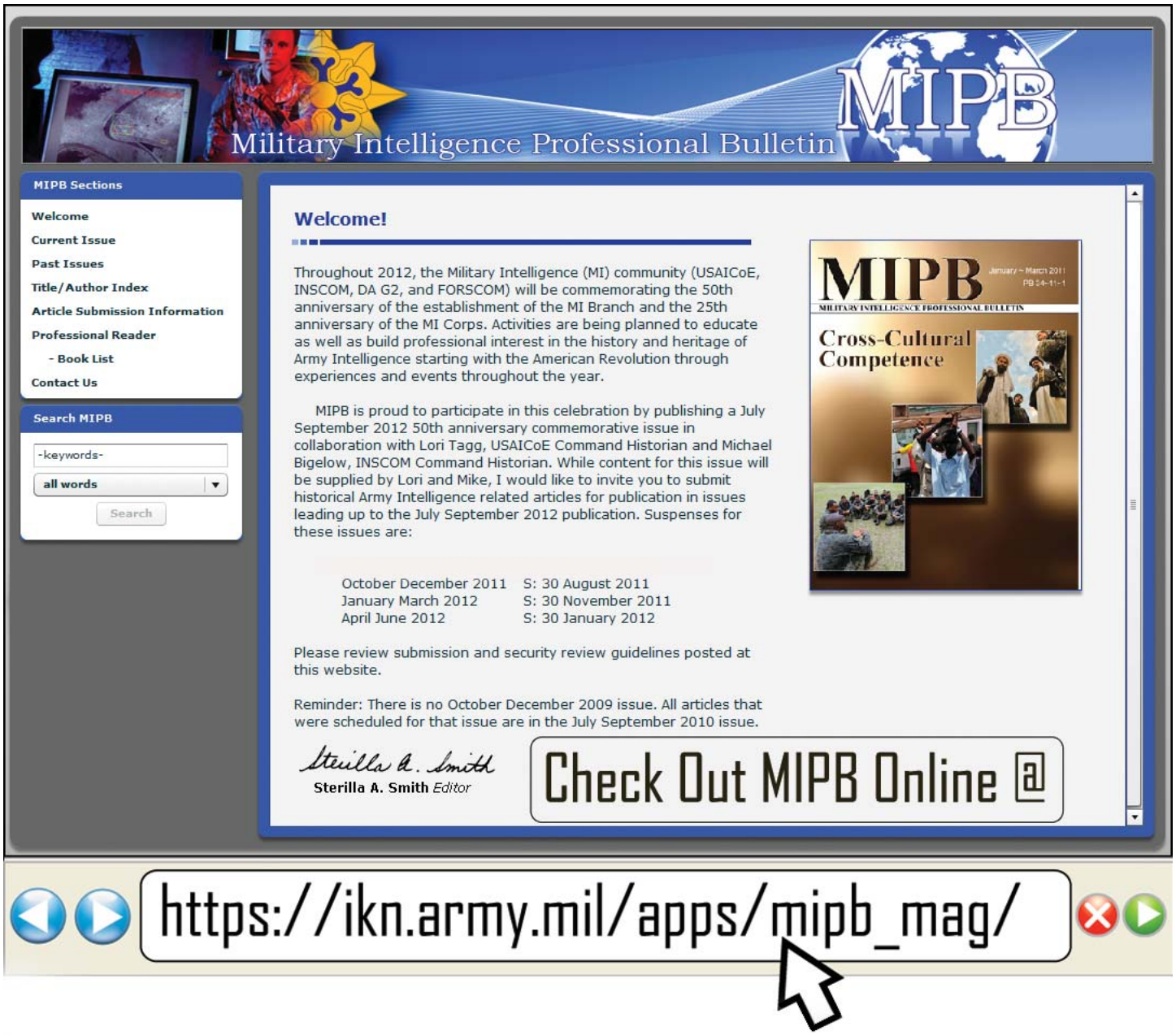
		" A WAY"				
	Current	C2	TUAS	HUMINT	PROPHET SENSOR	DRAGON
P	FM	FM/TACSAT	JABR	BCS3/Email	JWICS	FM/TACSAT
A	FACE to FACE	BFT/FBCB2/ MCS	Email	Breeze	UHF	BFT/FBCB2/ MCS
C	N/A	HF	VOIP	CPOF	NSA Net	HF
E	N/A	Cell/Iridium	FM	Cell/Iridium	Cell/Iridium	MCS/BREEZE/ JABR

Answering that question cannot be a "big hand—little map" wave toward SIPR, VoIP, FM, or courier. The answer must be specific to the type of information being passed and the asset passing it. An unmanned aerial system does not pass the same kind of information as a Human Intelligence collection team nor is the communications link the same. Similar differences imply dissimilar solutions when a PACE is devised. Establishing a separate PACE plan for all the MICO assets works as a way to cross-cue assets and share information in a timely manner which will allow for the MICO CP to maintain an accurate portrayal of asset status. Defining the PACE communications methods in advance reduces confusion when those alternate communications are needed. The MICO commander must communicate the method to everyone. The establishment of a MICO-level PACE is paramount to continued improvement in the flow of information and integration of intelligence at every echelon within the MICO.

Regardless of the shift to FSO, the MICO remained the BDE's number one collection asset. And just as in the past several years of MREs, the MICO and the BDE S2 struggled with their separate and collective challenges. The most pressing is the synchronization and the ability to maintain an accurate under-

standing of asset status. If employed correctly, the MICO is able to provide the BDE with the critical intelligence needed to maintain situational awareness and understanding of the battlefield. However, if these assets are used without a clear understanding of their tasks and purpose, they will more often than not fail to achieve their full collection potential. The MICO's integration into the BDE Staff and its ability to adequately providing accurate asset management and tracking for the BDE will alleviate these problems and ensure that the BDE will get the most out of its intelligence collectors.

Major Marrero is currently the Task Force 4 (BSTB) Senior MICO Trainer/Mentor at the JRTC. He served as the Bravo Company Commander, 201st MI Battalion, 470th MI Brigade from March 2008 to June 2009. During the Battalion's Operation Iraqi Freedom 07-08 deployment, he served as the Interrogation Control Element OIC at Camp Cropper, BIAP. His previous assignments include OIF (3), OEF (3), and Seoul, South Korea. His stateside assignments include Fort Benning, Georgia, Assistant Intelligence Officer, Joint Special Operations Task Force Intelligence Officer, 3rd Battalion, 75th Ranger Regiment, and Assistant Operations Officer, 201st MI Battalion. He holds a BS in Psychology from Sam Houston State University, Huntsville, Texas.



Chief Warrant Officer Three Conan Payne and Chief Warrant Officer Four Chad LeBoeuf

Introduction

Over the last several years the focus for both Iraq and Afghanistan has been on counterinsurgency (COIN) as opposed to full spectrum combat operations (FSO). As a result, the Army shifted its focus for Human Intelligence (HUMINT) at the brigade combat team (BCT) to emphasize Military Source Operations (MSO) over interrogation operations.

This shift affected the BCT's ability to conduct simultaneous HUMINT collection operations during FSO. First, the modified table of organization and equipment (MTOE) for the standard modular BCT is geared specifically toward MSO. It does not provide sufficient manpower to conduct simultaneous MSO and interrogation operations. Next, the emphasis on MSO within the BCT and parallel shift of interrogations to Military Intelligence (MI) brigades (BDE) has created a functional rift within HUMINT, creating Soldiers that are not proficient at both aspects of their jobs. Finally, and perhaps most importantly, the shortage of HUMINT collection capability has led to a number of tactics, techniques, and procedures (TTP) in the current operational environment that are not conducive to successful HUMINT collection in any operational setting.

Modular BCT Manning Creates False Choices

The standard modular BCT contains enough HUMINT soldiers at the MI company (MICO) to staff an operational management team (OMT) and three HUMINT collection teams (HCT), as well as a four-to-five member S2 HUMINT (S2X) element as part of the BCT S2 staff. Often this manning is insufficient to conduct MSO in a COIN environment, leading the MICO to create a fourth HCT either from HUMINT overages or by pulling HUMINT Soldiers from the three existing HCTs.

As the BCT shifts from COIN to FSO, it becomes necessary to shift resources to support interrogations as well. Interrogation requirements are typically heavier in the initial phase of FSO. This initial requirement to support interrogations forces the BCT to keep all of its HUMINT assets for interrogations at the onset and then begin to task organize them for MSO as the operation allows. However, this leaves the BCT without any organic MSO capability during the initial entry period. Moreover, maneuver elements have become accustomed in COIN to having their own HCT. FSO doctrine calls for a BCT to conduct simultaneous offensive, defensive, and stability operations (including COIN) as necessary. Commanders are therefore wisely reluctant to give up this capability.

This initial requirement was evident during 3/82 ABN's FSO rotation at the JRTC. At the onset of the rotation following the Airborne Insertion, 3/82 ABN's HCTs assembled upon predetermined locations, where they were to perform screening operations in conjunction with securing local townships. As a result of the screenings, many HCTs were able to identify potential leads of intelligence, whether for interrogation or for development under MSO, yet there were no additional HUMINT assets available to pursue these leads.

One more consideration on this point, the BCTs have become reliant on previously established networks during the last several years in both Iraq and Afghanistan. An FSO conflict includes the possibility of initial entry, whether into a theater or a region within a theater of operations, meaning that

even more time and manpower would be required in order for the HCTs to spot, assess, and develop networks to support operations. The emphasis on interrogations at the outset would make MSO completely unfeasible without additional manning. Ultimately, the BCT needs the capability to provide each maneuver battalion an HCT and an interrogation element while keeping a small cadre of HUMINT collectors to support BDE-level interrogations. This would require the doubling of the current MTOE.

A HUMINT House Divided

As mentioned previously, COIN emphasis has been on MSO almost to the complete exclusion of interrogations at the BCT. That is not to say that no interrogations are conducted in support of COIN. In the current fight that role has typically been filled by external support to the BCT, usually HUMINT assets from a separate MI BDE or Battlefield Surveillance Brigades, focused on interrogations to the exclusion of MSO. Over time this has created two separate cadres of HUMINT collector–interrogators and source operators. A collector assigned to a BCT has probably conducted few, if any, interrogations. When this Soldier returns to the U.S. he will probably attend advanced training in source operations, such as the Source Operations Course (SOC) or Advanced SOC (ASOC). He will likely receive no additional resident training on interrogations as long as he is assigned to a BCT. The opposite holds true for those assigned to the interrogation BDEs. They will likely attend courses such as the Joint Senior Interrogator Course (JSIC) or the Joint Interrogation Management Course (JIMC), and no further resident training on source operations.

Only two HUMINT collectors within 3/82 ABN possessed substantial interrogation experience to provide internal coaching and mentoring to inexperienced HUMINT collectors. These experienced Soldiers were members of the OMT. The OMT requirements precluded their ability to provide interrogation oversight and guidance to the less experienced collectors tasked with supporting interrogation operations. Additionally, 3/82 ABN HUMINT Soldiers, assigned to the HCTs, experienced difficulty switching from the mindset of exploiting information in a COIN environment to that of traditional FSO requirements, threat order of battle factors (identification of command structures, strengths, and dispositions of personnel, equipment, and units). Both their interrogation inexperience and not recognizing FSO requirements resulted in limited exploitation of detainees following capture.

When transitioning to FSO the BCTs find themselves severely lacking in interrogation capabilities with their current MTOE. Even if the BCT receives a larger contingent of HUMINT Soldiers they may not, depending on where these Soldiers served previously, receive Soldiers prepared to adequately support interrogation operations without a great deal of training. One way to mitigate this is to ensure HUMINT collectors rotate positions rather than staying an entire career in one track or another, thus ensuring balance of practical experience and training opportunity. Another way, one discussed to varying extents over the last several years, would be to make interrogation the foundation of all HUMINT collectors and then providing the option, perhaps at the first reenlistment, of training to become a source operator. A third option would be to divide the military occupational specialty (MOS) into two separate MOSs, making the interrogator distinct from the source handler. The benefit to options two and three is that slots could then be coded specifically either by additional skill identifier or MOS. Otherwise the BCT would still have to hope that its soldiers were well-rounded enough to support both the interrogation and MSO missions.

"Harry Potter" HUMINT

An issue that stands out amongst the others is one not directly connected to the distinction between COIN and FSO. Too many see HUMINT Soldiers as a sort of "Harry Potter," capable of waving a wand over all collection tasks. Tactical leaders persist in a fundamental misunderstanding of what HUMINT

provides and how HUMINT collects its information. Quite frankly, as long as this remains a problem, no changes to MTOE or HUMINT training will likely be effective. Focusing on the trends from the COIN fight, we see commanders continuing to think of HUMINT as a passive collection asset; that somehow the mere presence of a HUMINT collector in an area will cause HUMINT information to begin flowing in. It has been a common TTP to see teams broken down to the point where individual companies each have one HUMINT soldier.

The company-level is too narrow in scope for even a complete team to be effective. A lone HUMINT Soldier attached to a company cannot possibly take the necessary steps to properly maintain an existing source network, much less develop one in initial entry operations. More often than not when HUMINT Soldiers are distributed as such we then focus on tasks such as tactical questioning (TQ), document exploitation, and patrol debriefs, none of which are HUMINT tasks. As we see the BCT move into an FSO scenario, we can count on seeing this failed TTP perpetuated given the need for simultaneous MSO and interrogations and the limited number of HUMINT Soldiers available.

Several 3/82 ABN's HCTs were primarily enveloped in a traditional Scout operation of reconnaissance and were not permitted to encounter the local population in a manner conducive to source development. This restriction challenged the HCT's collection efforts and hampered their ability to develop a successful source network.

Moving forward we need to ensure there is more education for the tactical-level consumer of HUMINT with regard to how HUMINT is conducted and what missions the HUMINT Soldier is trained to conduct. Commanders need to understand the difference between TQ and an actual interrogation at the point of capture, understanding how impractical the latter truly is. Then we might see a lower incidence of source meetings being canceled for HUMINT collectors to travel with line units for possible TQ missions. They should understand that HUMINT is neither a static sensor nor a scout; simply dropping one off in a denied area will not yield immediate HUMINT information.

Face Forward, Not Backward

We must examine some of the restrictions on maneuver in the current fight. For example a four MRAP, twelve person, two crew-serve-weapon minimum for any mission can effectively shut down successful HUMINT collection operations. These are theater specific rules and must be carefully weighed rather than promulgated as an Army policy. This type of thinking effectively restricts HUMINT collectors to either sitting on the forward operating base or traveling with a platoon-sized element on a maneuver-focused mission, which generally offers little or no collection opportunity.

Consistently, the 3/82 ABN's HCTs were restricted from conducting source meets due to the imminent threat of the adversarial forces. Additionally, HCTs were prevented from travelling throughout 3/82 ABN's lodgment area, where travel was relatively secure and unrestricted. 3/82 ABN adopted restrictive policies, based on operations in current theaters, requiring teams to move in large convoys, which severely affected HCT military source operations.

As our focus changes from COIN to FSO, we must ensure that our HUMINT soldiers get the technical and tactical training they require to support both their interrogation and MSO roles on the battlefield. At the same time we must provide better training to the Army leadership to ensure this limited resource is employed to its fullest potential. We need to carefully preserve what we have learned in the past decade. Not collecting HUMINT poses far greater risk to the deployed force. Finally, we need to ensure units are staffed optimally to be able to conduct and manage both of these missions simultaneously. At present the BCT is simply not trained or organized to handle both tasks, and as such will likely fail at both.

CW3 Payne is currently the senior HUMINT Collector Technician at the JRTC. His training includes the HUMINT Collector Course, Defense Strategic Debriefing Course, ASOC, Reid Technique of Interview and Interrogation, and Modern Standard Arabic. Mr. Payne has served in a variety of operational assignments to include strategic debriefing in Europe, interrogations and source handling in Iraq and Afghanistan, and maritime interdiction operations with 6th Fleet. He holds a BA in Humanities from the University of Maryland.

CW4 LeBoeuf has over 18 years of service in the U.S. Army as a Counterintelligence Technician. He is currently assigned to JRTC as the Senior CI and S2X Trainer/Mentor. Mr LeBoeuf has a diverse background in tactical and strategic CI assignments.

Signals Intelligence in Full Spectrum Operations: "Outside the Wire? What Wire?"

Warrant Officer One Larry Jones and Sergeant First Class Timothy Rodriguez

Introduction

The tactical Signals Intelligence (SIGINT) missions and resultant observations from the 3/82 ABN full spectrum operations (FSO) rotation in October 2010 at the Joint Readiness Training Center (JRTC) were considerably different from our "normal" counterinsurgency (COIN) centric mission rehearsal exercises (MRE) missions and observations. The three major lessons learned were:

- There is a lack of a comprehensive SIGINT Intelligence Preparation of the Battlefield (IPB).
- There is too much focus on "sophisticated" communication methods.
- There is a lack of tactics, techniques, and procedures (TTP) to use SIGINT collection systems tactically.

COIN is but a small part of FSO, it is nonetheless driving how the Army is currently training SIGINT Soldiers.

There are three underlying reasons why FSO has become a lower SIGINT training priority over the last 10 years. The first major challenge involves live environment training and the Relief in Place/Transfer of Authority (RIP/TOA) process. Units focus their SIGINT platoon entirely on their future battle space where the SIGINT operational environment (OE) is fully matured. Also, traditional SIGINT IPB is not taught as part of the larger Military Decision Making Process (MDMP). The second challenge is that units experience a large personnel turnover in the tactical SIGINT platoon and do not set priorities for home station training focusing on traditional FSO requirements. As a result, units default to their experiences in Iraq and Afghanistan and train accordingly. This focus on the CENTCOM mature theater eliminates the training on much of the SIGINT spectrum necessary for FSO.

The final challenge is time (operational tempo). Leaders do not have time to prioritize the necessary SIGINT training for FSO. Time between deployments is limited and focused on their future battlespace. SIGINT platoons do not train on maneuvering and employing tactical SIGINT assets and focus instead on their next deployment. 3/82 ABN experienced all of these challenges before their rotation and experienced the effects of these challenges during their FSO rotation.

OE Tunnel Vision

In the current COIN operational environment, traditional IPB is deemed unnecessary as units RIP and "fall in on" a mature SIGINT enterprise. Tactical SIGINT platoons deploying to Afghanistan and Iraq commonly do not complete an IPB of the SIGINT environment; relying instead on products already developed by the outgoing unit. SIGINT Soldiers rotating into a COIN fight often fall into an already established SIGINT environment where enemy networks are already identified and targeting lines have already been developed and often have been worked for months, if not years.

FSO is completely different in that there is likely an immature SIGINT environment compared to that in Afghanistan and Iraq. Obviously, in a forced entry situation, there is no RIP/TOA process. 3/82 ABN was challenged by the fact that their tactical SIGINT Soldiers had limited training and experience to conduct SIGINT IPB during the MDMP preceding their forced entry operation. 3/82 ABN quickly discovered that their difficulty in defining the SIGINT OE prior to initial entry by identifying the best places for signals collection and exploitation was an absolute necessity and prevented them from effective collection until D+2.

Another challenge experienced by 3/82 ABN was not having a developed SIGINT collection plan prior to initial entry that tied back to a comprehensive collection plan focused on intelligence gaps and the commander's priority intelligence requirements (PIRs). Additionally, inconsistent communication with the fusion cell hampered the SIGINT cells collection focus.

We have the SIGINT equipment to cover every aspect of operations from initial entry collection and exploitation to follow on analysis and precision targeting. We have the doctrine and the TTPs. Preparation for an initial insertion into a country that does not have established friendly presence has not changed. We do not have FSO experienced or trained Soldiers. A generation of SIGINT Soldiers has neither the experience nor the training needed to conduct detailed MDMP, culminating in thorough SIGINT IPB and a written operations order for FSO.

Target Fixation

Secondly, as SIGINT became decisively engaged in the current COIN fight so did its training and product development. The tactical SIGINT community has, as a result, forgotten about traditional "unsophisticated" communication capabilities. The current training for Soldiers deploying to Afghanistan and Iraq is based upon the previous Operation Iraqi Freedom-mode of "sophisticated" communications being the most prevalent and therefore the priority for training.

Tactical SIGINT training moved away from more primitive communications technologies that continue to play a large role in the SIGINT environment throughout the world and are critical in FSO. Special Intelligence (SI) assets have been widely used throughout the COIN fight and will continue to be an absolute necessity within any type of FSO. These assets can quickly help determine where to place other collection assets and provide an overview of the signals environment. Imagery, in conjunction with SI assets, is a tremendous help when trying to place SIGINT assets on the battlefield. SIGINT planners can look at a location during IPB and develop employment considerations. Other ground SI assets will continue to be used for surgical targeting during FSO focusing on networks and individuals. During the 3/82 ABN rotation, SIGINT fusion with other intelligence disciplines was a challenge that ultimately lead to a collection plan that was not focused on all sources or disciplines.

Fixed Site Employment, Rediscovering Tactical SIGINT

The COIN fight in Afghanistan and Iraq has consumed the majority of SIGINT resources for the last 10 years pushing other FSO requirements to the second tier of collection. In meeting those COIN and second tier collection requirements, tactical SIGINT assets collected from sanctuary sites or from inside fortified forward operating bases (FOB) or combat outposts (COP). 3/82 ABN learned how this mindset can cause collection degradation in an FSO environment. The BCT continued to move their collection assets to sites with heavily established security as opposed to points of optimal collection or in the current fight–with maneuver units. One example during the rotation was collocating the Prophet collection system with the tactical operations center. While the asset enjoyed security, collection suffered as this was the lowest lying point in the surrounding area.

In the last 10 years, SIGINT collection assets have become locked into these massive structures in Iraq and Afghanistan. The Prophet and Low Level Voice Intercept (LLVI) teams have become fixtures on FOBs and COPs rather than being mobile tactical collection assets. Commanders do not fully understand their SIGINT capabilities and are sometimes unwilling to apply the resources necessary to ensure their security outside a fixed position. Additionally, SIGINT Soldiers lack the skills and experience necessary to provide asset employment considerations and recommendations in order to shape decisions.

The intended use of the Prophet in FSO is to follow the forward line of troops on the battlefield providing the maneuver commander with near-real time SIGINT collection. Prophet Enhanced is an upgraded multi-functional system placed on a Medium Mine Protected Vehicle capable of moving over rough terrain. The upgraded Prophet is equipped with satellite on the move capability enabling immediate analysis through database access. It increases early warning, force protection, and enhances forward collection capability while providing commanders the data to enhance their targeting efforts at every echelon.

LLVI teams are a dynamic tool that should be utilized as a forward collection asset, reconnaissance tool, and operate in conjunction with other SIGINT assets. In COIN, these teams are often in fixed sites; they are not pushed forward to fill collection gaps because of security concerns. During FSO, the LLVI teams can and should be attached to forward reconnaissance elements, like scouts, for collection and early warning force protection. Training on FSO employment and site selection of the Prophet and LLVI

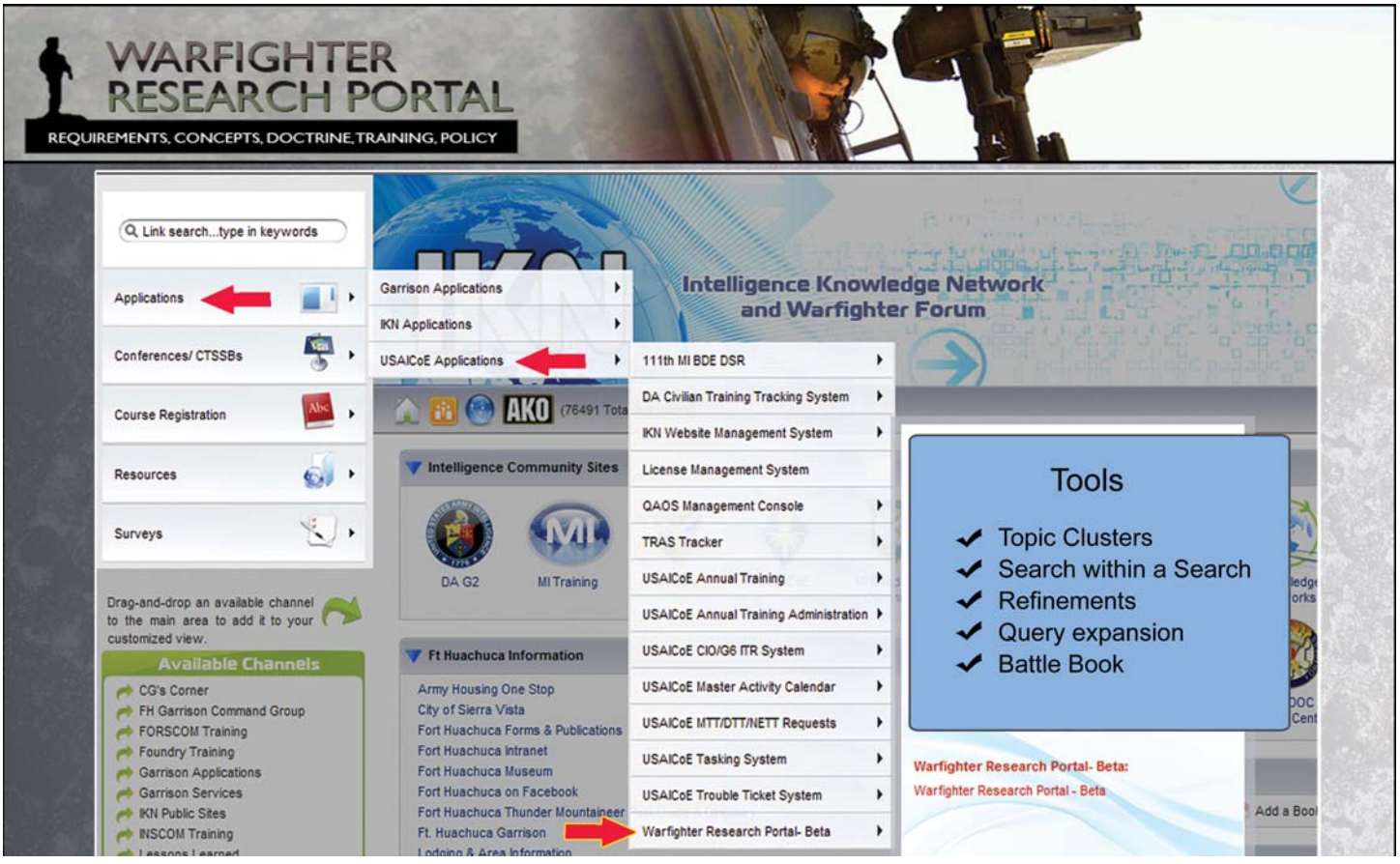
teams has suffered due to the COIN focus over the past decade. Current training is often focused on equipment training and set up and fails to address tactical skills necessary for SIGINT Soldiers to operate forward with maneuver elements. Additionally, radio frequency and antenna theory classes have been removed from SIGINT training causing a knowledge gap for operators. The days of teaching hide site construction and basic long range surveillance tactics to LLVI teams are gone. This type of training is essential to the FSO fight.

Many observations from the 3/82 ABN October 2010 JRTC FSO rotation were similar to those from our normal COIN MRE rotations. The greatest difference was the critical need for training SIGINT Soldiers to operate in FSO outside of an established OE. The SIGINT community must allocate Soldiers, equipment, and time to "retrain" on critical FSO tasks such as IPB and tactical SIGINT asset employment. The Army is more technologically advanced in SIGINT operations than ever before, but the critical flaw in tactical SIGINT is that we have become fixated with the current COIN fight and let that fixation shape our training for FSO.

WO1 Jones is an AOC 352N currently serving as the Senior BCT SIGINT Trainer/Mentor at the JRTC. Mr. Jones has over 14 years in the SIGINT community as a former Morse Code operator and Signals Intelligence Analyst. He has served multiple tours in South America and Iraq with a diverse background in the Special Operations Forces community. His assignments range from national level strategic collection and analysis to battalion and brigade size tactical SIGINT operations to include SI/ISR collection management.

SFC Rodriguez has over 14 years of service in the U.S. Army as a Signals Intelligence Analyst. He is currently serving as the Senior Brigade S2 NCOIC Trainer/Mentor at the JRTC and previously served there as the Senior SIGINT Trainer/Mentor for the 2 years. He has a diverse background in tactical and strategic Signals Intelligence assignments.

The Warfighter Research Portal provides Intelligence Knowledge Network users content discovery solutions in a repository of current authenticated Army doctrine, approved Army operating and functional concepts, and other official publications. Log on to the IKN website at https://ikn.army.mil and follow the path below to try this beta content discovery site. Look for details in the Jul-Sept 11 issue.



The Shadow Tactical Unmanned Aerial System: Enabling The Enablers

Sergeant First Class Bryan J. Ward

Introduction

The Shadow tactical unmanned aerial system (TUAS) is a key part of the intelligence, surveillance, and reconnaissance (ISR) package directly under the brigade combat team (BCT) control. It is often the most valuable (or the only) means of collecting live video feed within the BCT area of operations (AO). That unique capability can be absolutely critical to the commander in full spectrum operations (FSO), allowing him to see contiguous, non-contiguous, and unassigned areas that would otherwise become defacto blind spots.

Where is the Shadow Platoon? Only the Enemy Knows...

In the moving gun fight called FSO, it is especially easy to leave that asset vulnerable. Years of mission readiness exercises (MREs) have accustomed commanders to secure base operations for TUAS. FSO, at least in part, strips away much of that security blanket. Most TUAS platoons across the Army are currently undermanned. During a conflict where the platoon is launching and recovering from a location that is not built up and easily secured, the platoon is unable to provide its own site security. Remember, a TUAS platoon on the ground has an easily detectable signature but the Shadow at altitude is hard to detect. That all changes when it lands or takes off. In FSO, if the TUAS platoon is to operate securely it is essential that a minimum of an Infantry or Military Police (MP) platoon be assigned to provide security for the launch and recovery site (LRS) as well as engineer support to help provide a defensive perimeter and fighting positions.

Securing the LRS, Secure the BCT

A fully manned TUAS platoon will conduct split site operations effectively removing half of the platoon from the LRS. During consolidated flight operations the entire platoon is located at the LRS and is expected to provide its own security. This is not a realistic requirement. Flight operations require at a minimum five personnel for launching an aircraft, three to fly the actual mission, three to prepare the follow-on aircraft for the next mission, and five to conduct recovery operations. Using the platoon to provide its own security would hamper the ability of the platoon to provide continuous coverage. The unit would have to sacrifice security for operational necessity when forced to provide internal security at the LRS between phases of flight operations. As those phases of flight operations start, Soldiers have to be pulled from security leaving areas of the LRS perimeter exposed. Tasking an Infantry or MP platoon to provide LRS security will help alleviate the need for the TUAS platoon to have to provide its own security. Securing the TUAS provides better security for the entire BCT.

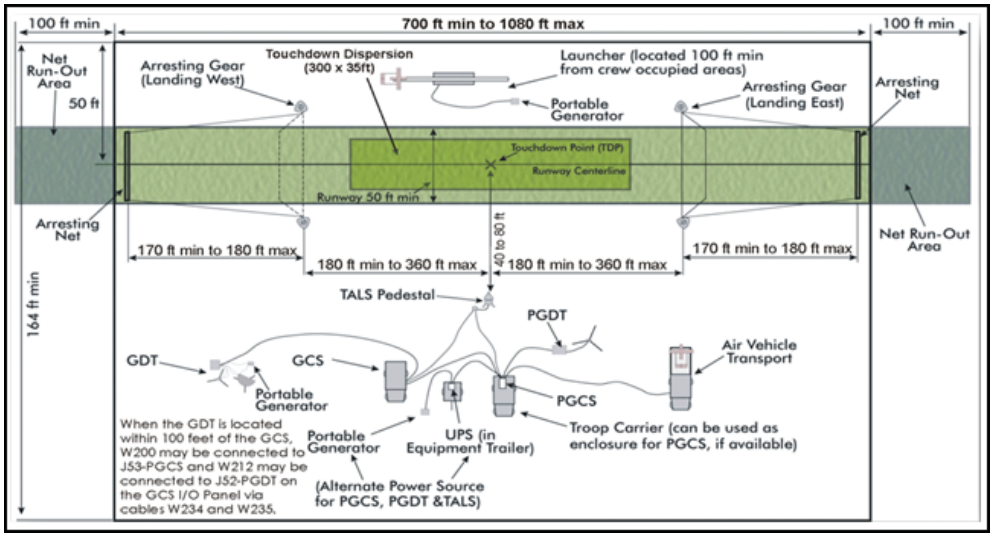
Incorporating Engineer Enablers

The same holds true for Engineer enablers. Providing Engineer support for runway preparation and repair is a no brainer. The same Engineer assets can help build up defensive perimeter or dig out fighting positions. This assistance will substantially increase the TUAS platoons chances of surviving contact with enemy forces. The TUAS platoon also needs to be provided with the materials (concertina wire, barricades, etc.) to assist with forming a perimeter around the LRS. While there is no way to ensure complete survivability during combat, these changes would effectively increase the chances that the TUAS platoon would

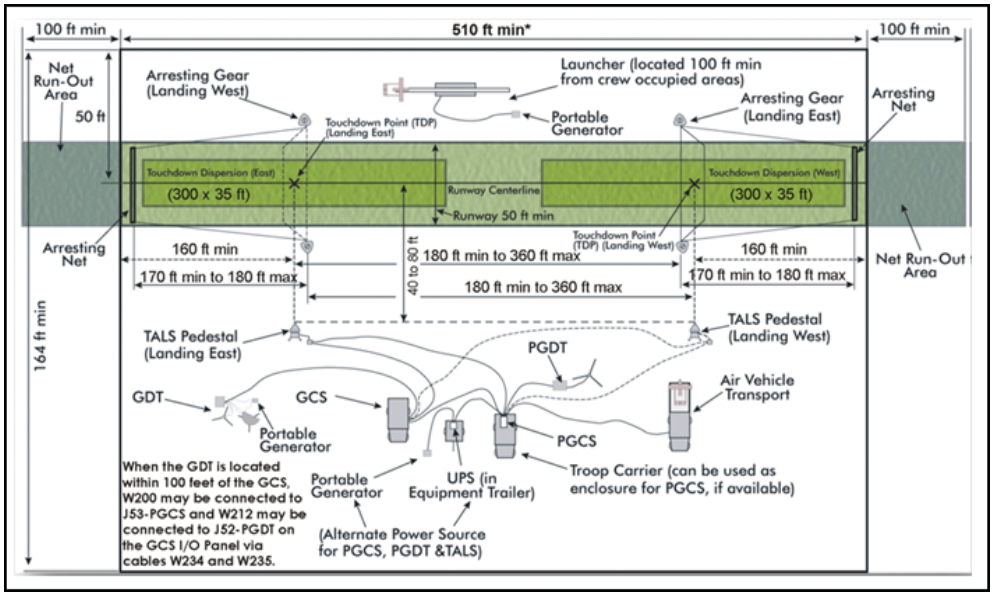
be able to survive enemy engagements and continue providing the BCT with live video feed of the AO and current maneuver unit operations.

Proper LRS selection is vital to the performance of flight operations during any conflict or exercise. During most operations, BCTs will locate the LRS at the same airfield where air land operations take place and often where all supporting rotary wing aircraft are located, especially during the initial entrance into an AO. This is ideal for consolidating all assets in one spot for security reasons. However if the TUAS platoon is required to launch/recover aircraft on the same runway being used for air lands and rotary wing, safety issues will require the TUAS platoon to displace their equipment after each launch and recovery. Incorporating Engineer support into the TUAS platoon will allow for the creation of and repair of an auxiliary runway a safe distance from the main runway allowing for continuous TUAS operations.

The TUAS platoon can operate from any location, given a clear flat surface from which to launch/recover. A long runway setup as shown below allows for launching and recovering in both directions without being required to move any emplaced equipment due to wind direction change. The long runway setup requires a minimum of 900 feet total length and 164 feet wide, this is including 100 feet of runoff on either end.



A short runway setup as shown below allows for launching and recovering in both directions without having to move any of the emplaced equipment due to wind direction change. The short runway setup (to include 100 feet of runoff on either end) requires a total length of 710 feet and 164 feet in width.



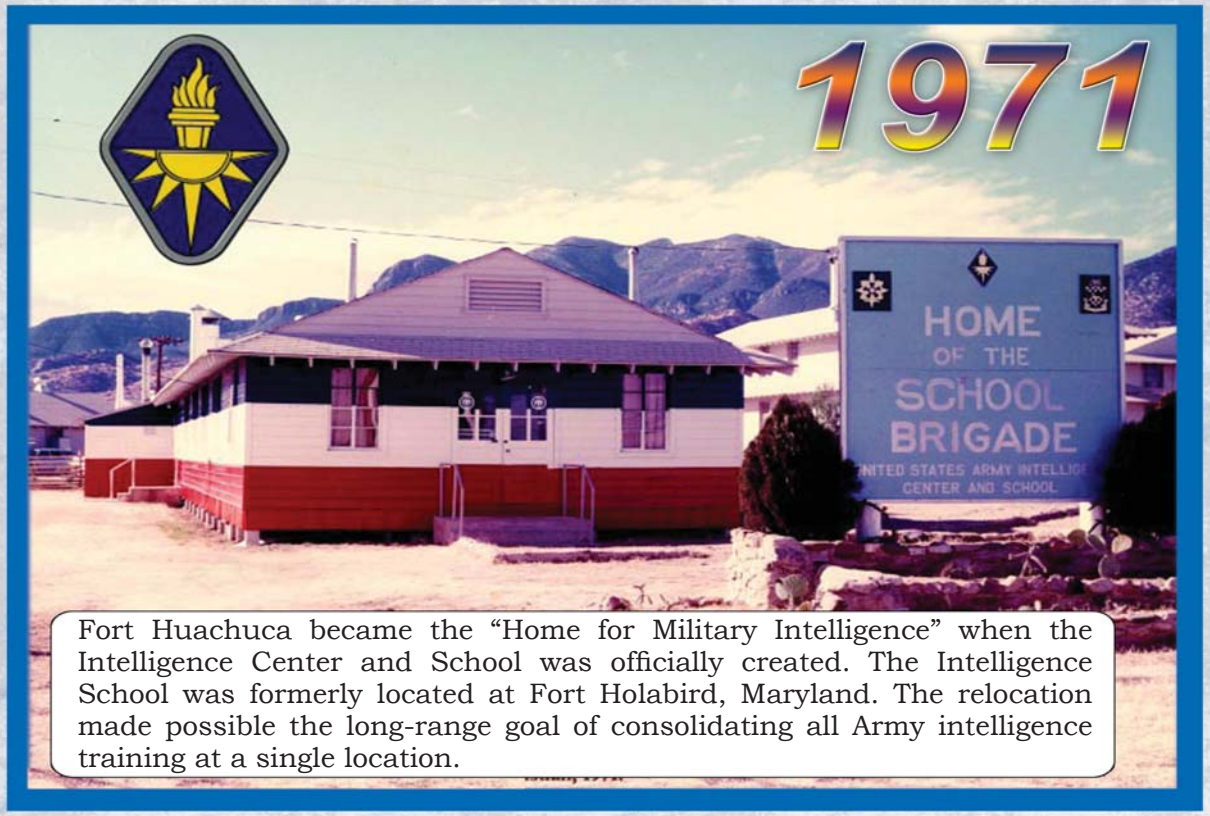
Engineer support provided to the TUAS platoon will allow them to create a runway in almost any area allowing the TUAS platoon to provide the BCT with continuous support. If the platoon is required to perform launch and recovery operations from a main runway or field landing strip, operational support may be degraded due to having to displace equipment for safety reasons while rotary wing and air land operations are taking place.

Summary

None of this is rocket science but it still requires some forethought. Commanders have come to depend on Shadow to cover operations in Iraq and Afghanistan. Years of operations and MREs have made the TUAS a key tool in the commander's ISR collection. A return to FSO will not change that trend; it will however require some changes to how TUAS operations are established and secured.

SFC Bryan Ward is currently the Task Force 4 (BSTB) Senior TUAS Trainer/Mentor at the JRTC. He served as the TUAS Platoon Sergeant for the 3rd BCT, 4th Infantry Division from July 2005 to June 2009. During the Brigade's OIF 05-07 deployment, he served as the Platoon Sergeant and LRS NCOIC at FOB Warhorse, Baqubah and during the Brigade's OIF deployment 07-09 deployment, served as the G2 Fusion LNO at Camp Victory Baghdad and the Consolidated LRS NCOIC at Camp Taji, Iraq. His stateside assignments include Kelly AFB, Texas, Voice Intercept Section Supervisor; Hunter Army Airfield, Georgia, Guardrail Collection Squad Leader; Fort Irwin, California, Collection and Jamming Platoon Squad Leader; Fort Huachuca, Arizona, 111th MI Bde Training NCO, and Fort Carson, Colorado, 3rd BCT TUAS Platoon Sergeant.

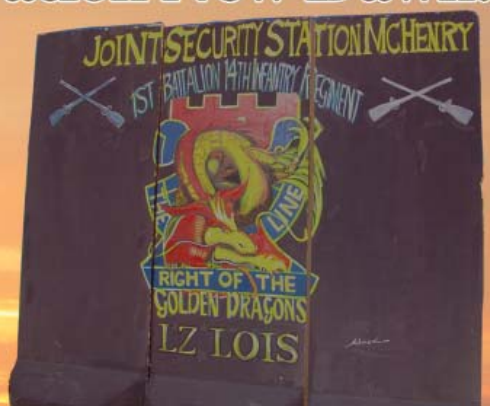
Defining Moments in MI History



Fort Huachuca became the "Home for Military Intelligence" when the Intelligence Center and School was officially created. The Intelligence School was formerly located at Fort Holabird, Maryland. The relocation made possible the long-range goal of consolidating all Army intelligence training at a single location.

Tactical Intelligence in Operation New Dawn: Notes from the Front

by Captain Christopher M. Gin and Staff Sergeant Bennett J. Strobel



New Dawn Challenges and the Way Ahead

September 2010 heralded a significant time of change across the nation of Iraq in more ways than one. September saw the end of Ramadan, where the most devout Muslims spend their days fasting and their nights reinvigorating their relationship with Allah. For the American Army, and specifically our unit (the 1st Battalion, 14th Infantry Regiment (Stryker)) of roughly 600 Soldiers, it also marked the advent of Operation New Dawn and an end to combat operations. Now nearly eight months since this benchmark, it is prudent to look at what the change of mission means for the Intelligence Community (IC).

Prior to deploying to the last months of Operation Iraqi Freedom this past June, all intelligence personnel in our Brigade were required to read Major General Flynn's paper, *"Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan,"* and consider it the way ahead for conducting operations during our deployment. The paper was not only suggestive as a paradigm shift, but even more so directive to the IC for its implementation of new methodology for collection down to the junior analyst level.[1] The main takeaway from General Flynn's article, as briefed by our commanders, was that the methodology behind our intelligence collection and analysis was flawed because of how narrow and enemy-focused our scope had become.

Admittedly, in our previous deployment when this Battalion partnered with one Iraqi brigade and was in charge of nearly 200 square kilometers at the height of the surge, focusing on "red" was far more prominent than "white" and "green" concerns. Predictive analysis was the goal of our Battalion S2 shop almost to a fault in order to keep Soldiers safe and improve our tactics, techniques, and procedures as the enemy improved theirs in an unending game of one-upmanship. Looking at insurgency in terms of counter- versus anti-insurgency is helpful in the context of the Advise and Assist Mission, but needs to be appropriately facilitated from the top to achieve the desired implementation at the bottom. Reconciling the strategy with the implementation is the preeminent challenge for the Battalion S2 section deployed to Iraq.

Identifying the Problems and Shortcomings

Advising the Iraqi Security Forces (ISF) on how to take a holistic assessment of their operating environment helps them understand what drives the insurgency, and ultimately where they can apply influence to help counter it. To measure our mission success, we ought to measure ourselves by how effective we make our ISF partners in securing the population and identifying where civil issues–if unresolved by civilian government–will morph into security problems. These are precisely the target points that insurgent groups like the Islamic State of Iraq and Ansar Al Sunna take aim at to achieve the effect of discrediting the government and security forces. Attacks against U.S. Forces are infrequent when compared to provincial data at the height of the war and are assessed mainly as information operations (IO) to win populist support for groups vying for position in post-U.S. Iraq. Where we, the Army, fall short in the "advise and assist"

model is the lack of appropriately trained personnel with experience and credentials to advise and assist on more than just military matters.

Our senior combat leaders have experience through their time in grade and multiple deployments, but they are used sparingly through key leader engagements and well-crafted talking points with Iraqi leaders across a much larger landscape than in previous deployments. Simply put, there are not enough commanders to go around and those that are on the ground experience a diminishing marginal utility as the Iraqis react and plan for our withdrawal. The companies and platoons that interact daily with key ISF partners are typically limited by virtue of their own work experience, being young military professionals. It does not take a Master's Degree in Social Sciences to identify problem sets in various subsections of Iraqi society, but coming up with solutions for the Iraqis to realize and enact does take training, innovation, and throughput.

It is even more difficult convincing ISF that they should take up the mantle of responsibility when their faith in the civil leadership wanes and varies, especially in a diverse cultural landscape like Kirkuk Province. Pervasive issues of personnel, mission clarity, and strategy versus execution are the biggest challenges to tactical intelligence personnel from here until end of mission in Iraq. This article is meant to provide some simple recommendations in a not so simple environment and only speaks to our experiences as one of a handful of battalion S2 sections left in Iraq.

Embracing the Change of Mission

The media attention that Operation New Dawn received did not clarify for the American public what the military's role in post-combat operations in Iraq is, and is not. In our microcosm, this was evidenced by the scores of phone calls and emails from confused family members after President Obama stated prior to 1 September 2010 that the last combat troops had left Iraq. The mission, as described by our commanders, is the only thing that has changed. The "advise, train, and assist" mission is still being carried out by American Soldiers, who by definition are combat trained troops.

The paradigm shift to ISF completely in the lead has not meant that we sit around on bases and wait for the trip home. On the contrary, operation tempo increased, but in a different way. We still roll outside the "wire" with up-armored vehicles, in full protective gear, each wielding a personal weapon, and travelling in convoys. Unilateral travel to and from specific destinations is still permitted by Iraqi law, as is the inherent right to self-defense to include force protection patrols. What does this mean for Intelligence?

IA and IP officers planning a mission based on Joint Intelligence.

If anything, it means that instead of assessing only the enemy, we need to readjust our focus to security in a broader sense and "target" influencing those Iraqis we think can have the greatest lasting impact on security. As physical enablers like ground troop sensors pull back from engaging the population directly, collection assets like human intelligence (HUMINT) source pools and unabridged notes from key leader engagements are the best way to keep situational awareness. The question we pose to ourselves and our team daily is how can we engage ISF Intelligence officers and assist and advise them? However, the more we ask this question, the more we realize that we rely on them in terms of intelligence collection.

It is important for commanders to have realistic expectations of what battalion S2 sections and company intelligence support teams (COISTs) can do to "advise and assist" Iraqi Intelligence officers on, since they live in and amongst the population, speak the language, and know the people more intimately than we ever will. However, there

are a number of areas in which we can help them develop an enduring capacity, and because time is so limited we must move to set the conditions for Iraq post-December 2011 now. Reinforcing the existing intelligence architecture by getting undertrained personnel into the Intelligence schools their own forces offer or offering exchange scholarships at Fort Huachuca to the brightest and most promising young officers might be a start. The problem is that even though the Iraqi Army (IA) has an established system of schooling, training, and on-the-job experience, the culture of mistrust when sharing information hampers further holistic development. As our Commanding General put it, "We must do some expectation management of what we can affect because we are looking at the IA system from an American standpoint and looking for ways to make it more efficient, whereas they are looking at the system with a legacy of corruption and attempting to fix that internally first."[2]

It seems we spend half of our time trying to catch-up with the Iraqi brigade and division S2s who are not so willing to share information about their current targeting, not only with us, but also with each other and especially with sister security force organizations like the Iraqi Police (IP). As the country attempts to transition to police primacy, IA leaders must also understand how this affects the nature of their organization. In turn, the U.S. Forces' mission to advise, train, and assist can ultimately be successful if we have the Iraqi Forces' cooperation. Evaluating staff integration and coaching staff exercises to the willing may be an effective way to get the ISF to see the battlefield with a cross-sectional lens, but they have more on their plate than simply attending our recommended staff classes.

Our focus should assist through tangibles like Actionable Intelligence derived from our technologically advanced platforms, but also significant time or more efforts spent on the advising aspect such as teaching tradecraft in bilateral programs and providing a focus through which the ISF will be able to conduct a full security assessment, not limited to threat actions. In order to be relevant and contribute to mission success in the Intelligence Warfighting Function, the mission tasks of "advise and assist" must be accomplished simultaneously, but should also take into account on what the Iraqis want to be advised and assisted.

Finding Intellect in Intelligence

Eighteen months following this unit's redeployment, reset, and an NTC-rotation focused on the transition to an Advise and Assist Brigade, and here we are back in Iraq, in a new province with new problems spread over 4,000 square kilometers. As of 1 September 2010, the total strength of U.S. Armed Forces was capped at 50,000 personnel versus nearly 170,000 at the war's height. In operational terms, this translates to roughly two battalions per province. In Kirkuk, where we are deployed, there is a Cavalry Squadron partnered with the IP in the City. Our Infantry Battalion is partnered with the ISF (to include the IA and IP) and Sons of Iraq (SoI)) in all areas outside of Kirkuk and the Combined Security Area. The challenge is being responsible for, "Kul Kirkuk, maad Medina," or, "all of Kirkuk, except for the City," as our IA counterparts like to say, highlighting the fact that everything affecting our area stems from the political developments in the provincial capital. In order to meet reduction in force numbers, our Intel section was reduced below the modified table of organization and equipment, without the augmentation of analysts that General Flynn's article advocates.[3]

Analyst shortfalls, however, have helped us focus on being more efficient and utilizing all available assets to include building competent COISTs that work in conjunction with direct-support HUMINT Collection Teams. What COIST leaders lack in formal intelligence training, they make up for in aggressive attitudes of would-be platoon leaders. Prior to deployment, familiarization with our proposed targeting process and tactical intelligence equipment was essential for their ability to cope with an ever-demanding deployment battle rhythm. Most of the COIST officers-in-charge are from the Field Artillery branch and use this additional assignment as an effective way to help focus their company's targeting efforts. Still, getting the right personnel in the right jobs is always a challenge.

While there has been some continuity in COIST makeup, many of the junior Soldiers were redistributed in order to meet line platoon shortages. That leaves us heavily dependent on OICs and NCOICs to take the initiative and be more than just an IST and who are, in reality, the company commander's staff for all areas in which he wishes to advise and assist the ISF. What we've tried to instill in our

COIST members is that their focus must be broader than just the enemy; otherwise, we'll always be in a reactive posture. This is achieved by commanders involving the COIST in all lethal and non-lethal missions.

In many ways, it is tougher being a COIST OIC than a Battalion S2 because of the amount of full-spectrum data one must gather, process, and analyze to several layers of command often without the required personnel support to dig through data and review notes from every commander's meeting. While this model for implementation does align with General Flynn's suggestion to separate analysts by geographic area (partnered IA brigade boundaries in this case), its overall effectiveness is hindered by too much information. In light of troop drawdown, battalion and higher intelligence shops do not have the manpower to detach to the companies even though it is the companies who provide the raw intelligence that shapes commanders' decisions at higher levels. Thus, the strategy for augmenting intelligence personnel and the implementation of this strategy at ground level are still divorced from one another.

Three recommendations come to mind for intelligence sections in units that are preparing to deploy to Operation New Dawn and facing similar manning issues. These may also be prescriptive as we begin the Afghanistan drawdown in the next few years. First, achieve greater efficiency through cross-training all analysts in current and future planning of operations so that no position is one person deep in terms of technical know-how. Instilling senior leader confidence in your assistant or NCOIC is paramount to an effective S2 section since this confidence will translate to authority when the primary is out on mission and subordinate and higher elements require the "S2" input. Improving Soldier and NCO writing skills by sharpening their verbiage and getting them more comfortable with their own language in order to brief and write is far more valuable than sending them to sporadic Arabic classes. Advising and assisting skills must first succeed with our own commanders before we can hope to apply them to the host nation forces.

Second, send the S2 personnel forward soonest during the transition period and ask to keep the current unit's S2 for an extra two to three weeks. It is the S2 Officer who has the greatest responsibility for data exchange in order to give the battalion an accurate, historical picture long after the previous unit departs. The typical two-week Relief in Place/Transfer of Authority process is not an adequate amount of time to conceptualize all the enemy and allied problem sets in an Iraqi province. Retaining institutional knowledge is a premium in the IC and will pay lasting dividends throughout the deployment.

The Battalion S3 and the author with children at a school opening built using U.S. CERP funds.

Third, identify your Soldiers' and junior officers' best traits and assign them meaningful work that will help drive the intelligence that in turn drives operations. People–and Soldiers are people–tend to have more satisfaction and achieve greater success in their profession when their daily work consists of autonomy, complexity, and a connection between effort and reward.[4] Morale, in an environment like today's Iraq, is as important as intellect because it keeps people engaged and helps ensure information is not lost in the shuffle because someone simply does not care. The human factors certainly affect the efficiency of any section in an ambiguous environment and promoting professional growth and critical thinking on a daily basis is necessary when tackling a challenge as big as a province. A good example of this was when we took a branch-detailed Infantry lieutenant assigned as the Battalion IO Officer and made him the Assistant Intelligence

Officer. While it took some convincing, reassigning him to a set of tasks he was more professionally interested in created the opportunity for on-the-job development in his future field of Intelligence. It also reenergized his efforts to perform above and beyond the standard even eight months into a deployment.

Merging Strategy and Execution

In a recent issue of Harvard Business Review, Roger L. Martin writes about how the idea that execution distinct from strategy is a flawed assumption, and that it is not good management practice to say, "We have a brilliant strategy, but it may fail because of its implementation."[5] Looking at the Intelligence mission through a wider lens, it is imperative that the leaders who developed the strategic vision for Iraq during Operation New Dawn see to it that the tactical implementers have more than just "buy-in." "Buy-in" has been misused in corporate and military planning sessions and has lost its intended meaning of getting everyone to an agreeable compromise based on near-equal vested interests–like shareholders in a joint venture. In Operation New Dawn, the term seems to have adopted a lingering connotation of a cheap deal in which one party (U.S. Forces) gets another (the ISF) to agree on means in order to achieve the former's ends. If we are not deliberate in our information campaign, the "buyers," in this case the ISF, will feel they do not have a say in the best methods to achieve those ends. They thereby run the risk of being too dependent on the U.S. military to reach the stated ends, since they did not take at least equal part in endstate formulation.

In order to move further into the advisory role, the ISF needs to have more than just "buy-in" in order to achieve the best results. At the tactical level, we are trying to enforce this new deal on a daily basis through interaction and influence. The same compromise should be the goal at the strategic versus tactical levels of the Intelligence Warfighting Function. Tactical units and the intelligence staff that support post-combat missions in Iraq ought to have genuine access to strategists and forums in the IC where policymakers look for the ground truth. This way, they remain a part of strategy's ongoing refinement and not just its execution. Sending specialized, handpicked analysts from higher to circulate at the battalion level would be welcomed by S2 shops that are under manned in order to build rapport and understand the ground analysts' methodology for collecting, analyzing, and processing information for higher visibility.

However, these "specifically trained analysts…empowered to methodically identify everyone who collects valuable information, visit them in the field, build mutually beneficial relationships with them, and bring back information to share with everyone who needs it," have not yet materialized down at the battalion level.[6] In fact, coordinating for brigade Intelligence fusion has been a challenge because of how spread out we are geographically.

Escorting the BN S2 from an intelligence sharing meeting with the District Police Chief. Hand grenades and sniper fire still pose a serious threat to U.S. troops in urban areas, so Infantry dismounts are often used in conjunction with armored vehicles going to and from meeting areas in the heart of cities.

Collecting intelligence that is of immediate interest to higher echelons is important, but allowing the ground unit time to analyze at their level before sending the information directly to the policymakers is absolutely necessary. First, going around the traditional chain of command and stove-piping the Intel is a tenuous proposal and makes ground commanders wary because they are responsible for the Intelligence that their staff provides higher. Second, if an S2 provides unanalyzed intelligence directly to a policy or strategy maker which may then turn into directives for that S2's commander, it leaves little room for further development or argument against top-driven operations. I agree with General Flynn's argument that commanders need to hold S2s accountable for answering the command's priority information requirements, but being relevant still means conducting analysis at the ground level be-

fore information is pulled away by higher and analyzed by echelons that are not "in the field."

Strategy and execution should not be distinctly separate in the environment that currently exists in Iraq. The volume of enemy attacks is not nearly as high as it was in previous years, so there is time to reflect on the best way ahead between the strategists and the executors. Taking the time to build a cohesive Intelligence sharing network among the few units and agencies still in Iraq is beneficial for everyone's situational awareness, but more importantly accomplishment of the advise and assist mission. As the transition to the New Dawn mission is fully realized at the strategic level, it is likely to be more successful in its implementation if the tactical Intelligence personnel feel their efforts and ideas of how to accomplish that mission are routinely integrated in the planning process.

Additionally, assuming that there is a ready pool of the hungriest analysts ready to serve on the strategic Intel "pull" teams is not the reality. In my humble experience, the lower an analyst is in the food chain, the hungrier the analyst is to get after information of real Intelligence value. In addition to pushing strategically tied analysts down to the ground level, it would be effective to pull battalion analysts up to the strategic level on occasion for short durations in order for them to see how their information affects the broader strategic planning. Empowering the executors by including them in the strategic vision and ongoing review helps ensure higher and lower echelons stay tied in with one another.

Advocating the Rule of Law

In order to secure the population, the IP must win the trust of the people they serve by adhering to the letter of the law. Advising the ISF on how to identify the challenges in their own systems and aggressively assisting them in overcoming Intelligence shortfalls at the ground level may be the best way ahead in the limited time we have left. The current biggest challenge the ISF now face is evidence collection and management within the legal system. Evidence has become the greatest Intel gap and the system for detainment has a revolving door if there is no evidence against the accused.

This is likely to be an enduring issue as the government of Iraq tries to curb corruption and develop a transparent legal system equipped with checks and balances. Gone are the days when a warrant was enough for the ISF to hold someone on suspicion of terrorism for an indefinite amount of time. In order to make the society a more secure place, the Iraqi Government must continue to emphasize the rule of law and show its ability to build cases and exercise fair judgment.

IP squad conducting a raid at a suspected location of a warranted insurgent.

On February 25th of this year, we witnessed Iraq's version of the widespread, anti-government protests that caught fire throughout the Middle East in recent months. In the province of Kirkuk, the largest protests occurred just down the road from our Contingency Operating Location. Although the protest began peacefully with an emphasis on more government provision of essential services, the demonstration eventually turned violent and a mob stormed government and police buildings. Paramount in the protestors' demands was the immediate removal of the City Council and the Police Chief. In addition to the underlying ethnic tensions that keep Kirkuk at the forefront of Arab and Kurd relations, the rule of law and the way the government and security forces apply it to their society needs improvement. As tensions mount between officials and unofficial leaders, we have had to come to terms with our effectiveness in influencing the judicial process at our local level. Fixing the judicial and security systems at higher levels is a desirable end state, but it will take the Iraqis' own commitment to social justice and judicial transparency development long after U.S. advisors depart.

Realizing our Enduring Partnership

Our enduring vision is for a strategic partnership with an Iraq that has a professional force able to secure the population internally and keep disruptive international influence at bay as it pertains to security within the country. What that means for Intelligence Warfighters is that their relevance is inextricably linked to providing overall security assessments and advice. These security assessments ought to be rooted in raw intelligence that is analyzed at the grassroots level to best inform policy and strategy makers at higher levels. Utilizing the available assets like the COIST and experienced Intel analysts that have already begun to understand an area will help in the aggregation of cross-section security information that is not limited to the threat.

Embracing the mindset change and our role as advisors is difficult, but necessary, for an honorable reduction of U.S. forces. It is also humbling when the ISF now reserve the right to say "no" to our suggestions. The positive effect of ISF evolution is that they are taking more deliberate action in the planning and execution of missions targeting violent extremist networks. After we realize that we're limited on what we can assist and advise them in terms of Intelligence based on our own training and capabilities, our action still cannot simply be inaction. U.S. leaders making strategic decisions about advising on all Warfighting Functions and beyond should also understand the challenges that we, the executors of that strategy, are facing and the support we need to succeed.

Endnotes

1. Michael Flynn, Matt Pottinger, and Paul D. Batchelor, *"Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan,"* Center for a New American Security, January 2010, 9-10.

2. MG David G. Perkins, 4th Infantry Division Commanding General, during a visit to the 1-14 Battalion Headquarters at JSS McHenry, Iraq following a full-spectrum briefing by the Battalion Staff on 19 January 2011.

3. Flynn, 12.

4. Malcolm Gladwell, *Outliers: The Story of Success,* (New York, New York: Little, Brown, and Company, 2008), 149.

5. Roger L. Martin, "The Execution Trap," *Harvard Business Review*, July-August 2010.

6. Flynn, 17.

Captain Christopher M. Gin serves as the Battalion S2 for 1-14th Infantry currently deployed to JSS McHenry, Kirkuk, Iraq in support of Operation New Dawn. He is a 2005 graduate of the USMA with a BS in English and Field of Study in Chinese. He earned his Master's in Asian Studies from the University of Hawaii while a Fellow at the East-West Center. His military education includes the Armor Officer Basic Course, Airborne, Air Assault, and Ranger Schools, as well as a deployment as the Battalion Assistant S2 in Iraq from 2008 to 2009.

Staff Sergeant Bennett J. Strobel serves as the Senior Intelligence Analyst and NCOIC of the 1-14th Infantry S2 section currently deployed to JSS McHenry, Kirkuk, Iraq in support of Operation New Dawn. His military education includes MOS 35F AIT and the Warrior Leaders' Course. He was awarded the Bronze Star award for his contributions to defeating Al Qaeda in Iraq networks north of Baghdad on a 15 month deployment from 2007 to 2009.

Uncertain about Uncertainty: Improving the Understanding of Uncertainty in MI Doctrine

by Major Ismael R. Rodriguez

Military operations are uncertain and unpredictable... Leaders who understand the dynamic relationship that time and uncertainty have on enemy and friendly forces are better equipped to develop effective plans. Given the nature of operations, the object of planning is not to eliminate uncertainty but to develop a framework for action in the midst of it.[1]

How do intelligence professionals contend with uncertainty on the battlefield? Is uncertainty a simple concept? Is there more than one way to define uncertainty? Uncertainty has long been central to the way the American Army conducts operations. Despite this, the Army has no clear definition of uncertainty. More importantly, there is a limited understanding of how uncertainty fits into the broader planning and intelligence responsibilities within the Army. There are many ways of considering uncertainty. While the prevalent approach of the Army is essentially mathematical, the fields of organizational design and wicked problems offer compelling alternatives for the intelligence community to consider.

The grand theories of warfare that developed during the Napoleonic era are fundamental to the understandings of uncertainty. Two prominent military thinkers provided compelling descriptions of uncertainty. That said, Clausewitz and Jomini offered differing points of view. Perhaps the more famous description of uncertainty is from Clausewitz, who directly addressed uncertainty and probability in his writings on intelligence. Building upon an earlier discussion of the probability and risks of warfare, he noted "no other human activity is so continuously or universally bound up with chance. And through the element of chance, guesswork and luck come to play a great part in war."[2] He later goes on to remark that "many intelligence reports in war are contradictory; even more are false, and most are uncertain…an officer…should be guided by the laws of probability."[3] It was Clausewitz's notion of the fog of war which is most prevalent. Indeed, he portrayed all information as uncertain, arguing that "the general unreliability of all information presents a special problem in war: all action takes place, so to speak, in a kind of twilight, which, like a fog or moonlight, often tends make things seem grotesque and larger than they really are. Whatever is hidden from full view in this feeble light has to be guessed at by talent, or simply left to chance."[4]

Jomini had a somewhat different take on uncertainty. While he does not address uncertainty explicitly, he offers a prescription for attending to it. In particular, he argues that it is essential to understand both military geography and the type of calculations involving military order of battle. He noted that there were misunderstandings by different military organizations throughout Europe on not just the lay of the land, but also the strengths and weaknesses of military organizations. Above all, he considered the study of such conditions as a scientific endeavor necessary to properly develop military plans.[5] At the operational level, Jomini had several specific recommendations. He strongly affirmed that through a thorough, multi-faceted collection of information, and despite the risk of misinformation, the truth can be discovered.[6] Still, Jomini recognized that there is a need for probability to determine likely enemy courses of action. Notably, he confidently proclaims that for a military leader who follows such a prescription "nothing very unexpected can befall him and cause his ruin."[7] Perhaps most tellingly, he immediately anticipates criticism of this concept, recognizing that while surprises happen, even these could in all probability be determined.

Clausewitz and Jomini cemented a traditional approach to understanding the role of uncertainty in military operations. Like other tenets attributed to them, their descriptions have largely withstood the test of time. As the American military evolved

in the 20th century, these themes of friction and fog, or reconnaissance and surveillance, would become increasingly evident in American military doctrine, as expressed in the Cold War era FM 100-5, Operations:

> ***Combat intelligence provides knowledge of the enemy and the area of operations vital to the successful conduct of operations. It reduces the unknown factors and, therefore, is of great significance to the commander and his estimate of the situation.[8]***

Perhaps the simplest understanding of uncertainty derives from the realm of mathematics. Solving for the unknown is a concept familiar to anyone who has completed a course in algebra. As in an algebraic equation, there is a problem and ultimately a solution. Indeed, engineers and scientists are familiar with this clear cut framework for problem-solving.[9] The military has a host of problems that fit these criteria, of which risk management is a prominent example. Army doctrine requires a consideration of probability in the calculation of risk. FM 5-19, Composite Risk Management, uses an implicitly mathematical approach that includes estimating the frequency that a event may occur.[10] Whether firing artillery, delivering an aerial resupply drop, or planning the company organization day, there are calculations to be made and risks to be mitigated. The Army demands that its leaders determine "an initial risk assessment that compares the potential for threat (tactical) and hazard (accident) risk against the factors of METT-TC."[11] Indeed, this first step of risk analysis aligns closely with the thinking of Jomini about uncertainty. Arguably, this notion of risk and probability offers the most widespread framework for uncertainty available to the Army.

Outside of the military arena, there have been vast improvements in the description of uncertainty. One field that deserves attention is organizational design. In essence, organizational design considers how an organization relates with the larger world. In defining uncertainty within an environment, there are two essential variables. As Richard Daft explains in his text *Organization Theory and Design*, "…uncertainty means that decision makers do not have sufficient information about environmental factors, and they have a difficult time predicting external changes…Characteristics of the environmental domain that influence uncertainty are the extent to which the external domain is simple or complex and the extent to which events are stable or unstable."[12] With this basic definition in hand, it is easy to identify different ways in which an organization contends with its environment. Put simply, these two variables create a simple two dimensional framework for interpreting an environment. The first dimension spans from simplicity to complexity. Think of this as all the different types of information necessary to survive. The second dimension spans from stability to instability. Think of this as the pace of change taking place. Some organizations operate in a stable, simple environment. In such a world, it is fairly easy to predict what will take place. Still, other groups may face a great amount of instability in addition to a very complicated set of environmental conditions.[13]

Wicked problems emerge from this challenging environment of uncertainty. By definition, a wicked problem is one that cannot be easily solved. Horst Rittel and Melvin Webber offer an enduring observation of such problems. More importantly, they critique the planning profession as inadequate for a complex environment, noting that "the classical paradigm of science and engineering…is not applicable to the problems of open societal systems."[14] They continue by challenging a central tenet of military planning, arguing that the step-by-step process of first understanding the problem, then gathering information in order to analyze and then solving a problem cannot work for a wicked problem. Instead, Rittel and Webber contend, "For wicked problems… one cannot understand the problem without knowing about its context; one cannot meaningfully search for information without the orientation of a solution concept; one cannot first understand, then solve."[15]

So how does uncertainty relate to wicked problems? For one, the complex open societal model described by Rittel and Webber is similar to that of the organization design model of uncertainty driven by complexity and instability. Still wicked problems present other aspects of uncertainty. Because there are no underlying rules for solving wicked problems, it is impossible to know if the problem has been solved. A planner stops work on such problems not because a definitive solution has been found, but because critical resources run out.[16] It is moreover impossible to identify all the potential solutions to a wicked problem, sometimes there may

be no solution at all. Thus, determining the feasibility of potential plans is dependent "on realistic judgment, the capability to appraise 'exotic' ideas and on the amount of trust and credibility between planner and clientele."[17]

As evident in FM 5-0, Army Planning and Orders Production, some military doctrine takes a realistic view of the world. It fully accepts the notion that uncertainty exists and that it yields unpredictability.[18] Yet, is this commonplace in other military doctrine? Unfortunately, the doctrine is inconsistent, and there seems to be a disconnection between operational and intelligence doctrine on this subject. Predictive intelligence analysis has long been the gospel for intelligence professionals. At a minimum, FM 2-0, Intelligence pays lip service to the uncertain environment of the modern battlefield, accepting that "The environment we operate in is characterized by violence, uncertainty, complexity, and asymmetric methods by the threat."[19] This is not quite the case with other intelligence doctrine. In fact, quite recently, the dogma of predictive intelligence is still evident throughout FM 2-01.3, Intelligence Preparation of the Battlefield.[20]

On the other hand, operational doctrine is largely clear in its perception of uncertainty. TRADOC Pamphlet 525-5-500, The U.S. Commander's Appreciation and Campaign Design even builds upon the wicked problem theory.[21] Instead of harping on prediction, FM 3-24, Counterinsurgency, chooses to emphasize understanding. The field manual's chapter "Intelligence in Counterinsurgency," contends that "the purpose of this IPB step [determine threat courses of action] is to understand insurgent approaches and tactics so they can be effectively countered…The insurgents' approach is based on their objectives, desired end state, and requirements of the operational environment."[22] Understanding essentially replaces prediction. If the very nature of uncertainty makes it is impossible to predict, then the emphasis on prediction seems ill informed.

Is there a way to reconcile prediction and uncertainty? The linear methods of solving certain intelligence problems may still hold some relevance. For one, not all adversaries are insurgents. Moreover, the scientific methods used to determine cause and effect will continue to have value. Even in a challenging human environment, the military intelligence community could tap into a variety of social science related fields in order to predict certain human behaviors and activities. These applications should also have strong spatial components. As such, the application of geospatial information systems could be of great value. For instance, military doctrine has taken notice of these trends. FM 3-24, devotes much of its Appendix B to Social Network Analysis.[23] The intelligence community has invested heavily in geospatial capabilities that could have the potential to tap into cutting edge techniques used by the academic and research communities.

The doctrinal foundations of the intelligence and operations planning community offer several practical means to decrease uncertainty. The tenets of the Military Decision Making Process present a systematic method of understanding the intricacies of an operation. While intelligence planners may wish to focus their efforts on defining the operational environment and assessing the capabilities of the enemy, there are still other important ways to contend with uncertainty. By sorting out a complicated landscape and describing an adaptive enemy, the intelligence planner essentially presents an uncertain environment. The intelligence planner can then turn attention to the means of contending with that uncertainty.

One possibly overlooked method of contending with uncertainty is task organization. Simple changes to the command and control of intelligence organizations can have profound effects. Major General Flynn, Captain Pottinger, and Paul Batchelor recently noted this phenomenon in Afghanistan. In their example, a Marine infantry battalion chose to send its intelligence analysts down to the company level, placing skilled professionals at a level where they could have first hand access to an assortment of front line collectors.[24] From a theoretical standpoint, this approach makes sense. From the perspective of organizational design, a decentralized organization can contend with the challenges of a complex and dynamic situation.[25]

Flynn's proposal to use a journalist-style network of contacts fits within this context as well. In essence, these investigative officers provide a critical linkage to the outside environment, creating what Daft terms "boundary spanning roles" in order to "link and coordinate an organization with key elements in the external environment."[26] In any case, the traditional top heavy bureaucratic field organi-

zations of the Army do not present a good fit for an uncertain environment. Large intelligence units may play an important role in some future conventional conflict. However, such use by large intelligence units would be best in a case of a fairly simple, stable environment.[27] Developing an organization that has inherent flexibility would give commanders the ability to contend with more uncertain challenges.

Of the tools available to decrease uncertainty, perhaps the most effective is a strong relationship between the commander and the intelligence officer. Nearly two decades ago, Major General William Hertzog encapsulated this point in his "Intelligence Commandments for Commanders" when he decreed "to defeat the enemy, you must tell your intelligence officer what you must know and when you must know it."[28] The method for doing this has largely remained unchanged since World War II. Originally known as Essential Elements of Information, this selective information was "needed by a commander in a particular situation in order to make a sound decision and avoid being surprised."[29]

Future doctrine would refine the concept into intelligence and operations requirements. Commonly recognized as Commanders Critical Information Requirements (CCIR), these guidelines are essential in the effort to cut through the vast stores of information available to the modern intelligence organization. At first glance, the doctrinal decree that "the commander designates intelligence requirements tied directly to decisions as CCIR" seems too restrictive.[30] This construct may work well in a conventional setting with a well defined enemy. Fortunately, there is some leeway in the doctrine since a commander can singlehandedly designate any information requirement as a PIR.[31] Moreover, information can support decisions in different ways. For instance, information that provides context can aid in decision making. Indeed, a lack of context has been a critical deficiency in recent military operations.[32] So, if context is a gap, then the commander could choose to prioritize collection and analysis of information that fills in context. Indeed, the decision becomes how best to allocate intelligence resources in order to contend with an uncertain environment.

The Army should revisit how it approaches uncertainty. While its doctrine regularly refers to the concept, there is no easily referenced definition. As the Army evolves in the 21st century, a more nuanced multi-faceted understanding of the concept will become useful. The Army has learned much in its operations over the last decade. These operations have taken place in a complex and changing environment. In essence, this is the kind of difficult environment that should form the basis for defining uncertainty. While there will be a continued role for the traditional, largely mathematical concept, the two-dimensional, organizational-design based construction deserves a central role in the planning and implantation of future Army activities. That said, such a framework highlights where an organization can seek to contain uncertainty. Whether by modeling the dynamic activities of an enemy, or prioritizing the volumes of information available to an analyst, the end result may not be less uncertainty, but instead an effective means of operating "in the midst of it."[33]

Endnotes

1. FM 5-0 Army Planning and Orders Production, 2005, 1.

2. Carl von Clausewitz, *On War* Rev. Ed., Translated and Edited by Michael Howard and Peter Paret (Princeton, New Jersey: Princeton University Press, 1984), 85.

3. Ibid., 117.

4. Ibid., 140.

5. Antoine H. Jomini, *The Art of War* (Novato, California: Presidio Press, 1992), 39-40.

6. Ibid., 273-274.

7. Ibid., 274.

8. FM 100-5 Operations, (Change 3), 1958, 47.

9. Horst Ritteland & Melvin Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences 4* (1973), 155-169, 160.

10. FM 5-19: Composite Risk Management, 1-8.

11. Ibid., 3-6.

12. Richard Daft, *Organization Theory and Design*. 8th ed. (Mason, Ohio: Thomson/South-Western, 2004) 144.

13. Ibid., 142-143.

14. Rittel and Webber, 160.

15. Ibid., 162.

16. Ibid., 162.

17. Ibid., 164.

18. FM 5-0, 1

19. FM 2-0 Intelligence, September 2008, 3-2.

20. FM 2-01.3, MCRP 2-3A: Intelligence Preparation of the Battlefield /Battlespace, 2009.

21. TRADOC Pamphlet 525-5-500: The U.S. Commander's Appreciation and Campaign Design, January 2008.

22. FM 3-24 Counterinsurgency, December 2006, 3-20.

23. Ibid.

24. Michael Flynn, Matt Pottinger, & Paul Batchelor. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan,* (Washington: Center for a New American Security, 2010) 14.

25. Daft, 152.

26. Ibid., 145.

27. Ibid., 152.

28. FM 34-8 Combat Commander's Handbook on Intelligence, 1992 Front Cover.

29. FM 100-5 Operations, 1944, 49.

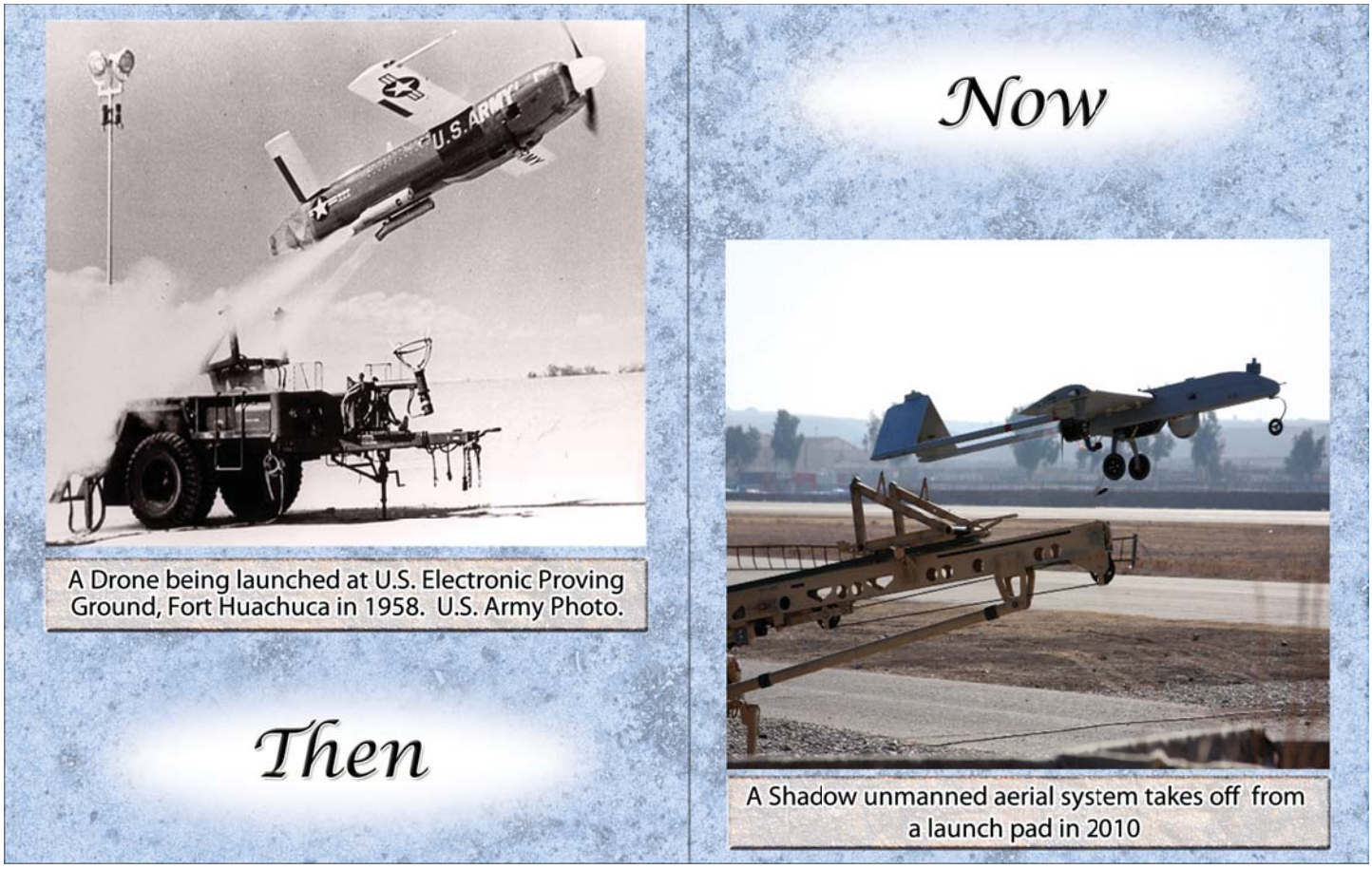
30. FM 2-0, 1-11.

31. Ibid., 1-12.

32. Flynn, Pottinger, and Batchelor, 2005, 1.

33. FM 5-0, 1.

MAJ Ismael Rodriguez is a 2010 graduate of the Naval Postgraduate School Special Operation Irregular Warfare Masters degree program. He is currently in ILE at Redstone Arsenal and is on orders to the AF/PAK Hands Program. He has deployed to Iraq with the 172nd SBCT, and has served as an intelligence planner at the ASCC and brigade level, an SBCT Surveillance Troop Commander, and a battalion intelligence officer for both a Field Artillery and light Infantry battalion. He can be contacted at ismael.r.rodriguez@us.army.mil.



The Threat of Mexican Cartels' IED Proliferation North of the Border

by Sergeant Matthew Ludwig

The opinions expressed in this document are my own and do not represent any official Department of Defense or U.S. Government policy or position.

Introduction

The U.S. was caught off-guard by the use of improvised explosive devices (IEDs) in both Afghanistan and Iraq. In Afghanistan, IEDs were an unexpected threat used by remnants of the Taliban after their removal from power. While IEDs were expected to be used by pro-Saddamist insurgents following the invasion of Iraq, the level of sophistication achieved by groups affiliated with alternate extremist movements could not have been foreseen. Despite the lessons learned about IED use from these two conflicts, the U.S. has failed to prepare itself and will again be caught off-guard, this time by the cartels currently causing turmoil in Mexico. Despite news reports detailing the cartels' use of IEDs and their recent transition to vehicle borne IEDs (VBIEDs), the situation remains under-analyzed, and security forces are unprepared for a situation that may involve IED use along the border. If the U.S. does not prepare for this eventual occurrence, it will run the risk of attempting to play catch-up again, only this time with an enemy who is harder to catch. Accurate prediction as to when IED use will move north requires an understanding of the situation in Mexico and the conditions and events that could prompt the use of this tactic.

Warring Cartels

The current reality in Mexico is that the government is caught in the middle of a war between two groups of cartels. On one side is the New Federation, led by the Sinaloa, La Familia, and Gulf Cartels, while on the other side is the group consisting of the upstart Los Zetas and their allies. The fighting between these two factions is the reason for the current cycle of violence that has left Mexico in turmoil. The effort to gain power and influence has led to an increase in ruthless and brutal tactics. As with any conflict, innovation breeds imitation and Mexico is no exception. Los Zetas are the driving force behind the increase in brazen violence. Their consistent effort to instill fear in their enemies is driving their opponents to retaliate in kind.[1]

The New Federation, headed by two former enemies, namely the Gulf and Sinaloa Cartels, is currently the larger of the two alliances. The Gulf and Sinaloa Cartels joined forces due to the threat posed by the newer cartels. The violence propagated by groups such as Los Zetas had destroyed the symbiotic relationship the cartels had previously maintained with the Mexican people and their government. The New Federation appears to receive less attention from the Mexican government and security forces than their competitors. The reasons for this vary, but the prevailing theories are government corruption and the fact that the Sinaloa and Gulf Cartels are similar to the American Mafia, as they prefer to keep their operations quiet in order to draw less attention to their activities. The likely truth is that the New Federation is the lesser of the two evils in the eyes of the Mexican government, and the initial decision was to focus security efforts on defeating the most violent of the cartels. Despite the New Federation's stated intentions, whether grounded in truth or not, the current violence spurred by Los Zetas shows no sign of lessening. The New Federation continues to practice the same type of violent tactics as their rivals.[2]

Los Zetas have a history full of twists and turns. They were initially a group of former Mexican Special Forces members who deserted to become

a bodyguard and assassination unit for the Gulf Cartel. After the death of Gulf Cartel leader Guzmán Decena in 2002, Los Zetas began their own drug smuggling efforts, thereby transforming themselves into a group allied with, but separate from the Gulf Cartel.[3] Los Zetas organization has grown in both size and influence since 2003, and their vicious tactics have brought unparalleled violence to the Mexican drug war.[4] Los Zetas turned against the Gulf Cartel in early 2010 and have since allied themselves with the Beltran-Leyva Cartel. The Beltran-Leyva Cartel was originally formed by the Sinaloa Cartel in response to Los Zetas, but the group changed sides to work with Los Zetas in their fight against their former parent organization. Los Zetas may also be assisting the Juarez Cartel in their fight against the Sinaloan Cartel's effort to seize the city of Juarez and the key trafficking corridor in the vicinity of El Paso. The Sinaloa Cartel's aggression has provided Los Zetas with a prime opportunity to gain a critical ally and to undermine their adversaries in one stroke. The use of VBIEDs by the Juarez Cartel members is an indication that an agreement is already in place with Los Zetas.

Los Zetas and the Mexican Government

While all the cartels routinely conduct audacious and often brutal attacks, Los Zetas appear to be on a path that would lead them to be classified as a financially-motivated insurgent organization rather than an international cartel. Their recent actions imply that they are taking steps aimed at completely collapsing the Mexican government rather than simply attempting to take advantage of its current weakness. While their attacks on law enforcement and military personnel, as well as the professional assassination of political figures, are obvious attempts to increase their influence, other events are of a more covert nature and suggest a well-thought-out effort to destabilize the Mexican government as a whole.

Los Zetas have been targeting Petróleos Mexicanos (PEMEX), Mexico's state-owned petroleum industry, which is the third largest producer of crude oil in the world.[5] While limited to siphoning oil from pipelines in 2009, Los Zetas began kidnapping PEMEX employees in May 2010.[6] Mysterious explosions have frequently occurred at pumping and refining stations throughout Zeta-controlled eastern Mexico. The explanations for these disasters have been ambiguous at best. PEMEX production, along with its profitability, has reportedly been crippled by Los Zetas, and analysts worry that its fall will drag the government down.[7] As the center of gravity for the Mexican economy, PEMEX is not allowed to declare bankruptcy. If it is unable to achieve its production goals, Mexico's financial problems will be exacerbated by the loss of revenue from exports and the need to import what it cannot produce.[8] If Mexico's fragile economy collapses, it is very likely that the government would shortly follow suit, creating the failed state that is currently feared.

Another key indication of a step towards both insurgency and blatant terrorism is the attack on civilians, particularly those belonging to the news media. All of the cartels are known to retaliate against those who report on their activities. The increasing attacks on members of the media are taking their toll, and many Mexican news organizations are unwilling to report on cartel activities. Los Zetas will go to great lengths to portray their alignment as coinciding with the desires of the Mexican people, despite the destructive nature of their activities. Videos showing children stating that they want to be members of Los Zetas are reminiscent of the various media portrayals of Arab children claiming their desire to be martyrs. They are also indicative of a generation that is growing up accustomed to extreme violence.[9]

Los Zetas claim to give back to the communities under their protection, and they hang signs and banners declaring themselves part of Mexico's culture.[10] Any news outlets or journalists that broadcast a message counter to this are targeted for attack. This was exemplified by the 27 August 2010 VBIED in Ciudad Victoria, which targeted a TV station that had been reporting on the Los Zeta murder of over 70 immigrants who had refused to work for the cartel after traveling into the U.S.[11] If allowed to continue, events such as this will perpetuate the cycle of violence and will serve to undermine any security gains experienced in Mexico.

Threat of IED Attacks

The lawlessness in Mexico and its government potential for collapse should not provoke the use of IEDs north of the border. The use of this type of weapon falls into a cost versus gain debate for the cartels, and it is currently not worth the attention

it would garner. However, it is a fact that these devices could serve a very practical purpose in the effort to move drug shipments unimpeded across the border. While it is unlikely that Sinaloa and its allies will turn to IED use, largely due to their effort to avoid garnering unwanted attention, Los Zetas have shown no such inclination. They appear to conduct their attacks with the intent of gaining additional exposure and to instill fear in those who resist them. Therefore, Los Zetas are the most likely group to use IEDs in the U.S., and it is not surprising that they are the cartel that has been the most proactive in increasing the use of IEDs in Mexico.

The reason Los Zetas have not begun using IEDs north of the border is because they still have other successful methods to traffic drugs into the U.S., and they fear that the attention that would be drawn to the border by the use of IEDs would result in increased security and decreased profits. This is likely to change in the near future since border security is currently a key issue, even without the use of IEDs. As systems such as the Secure Border Initiative Network (SBInet) are emplaced along the border, trafficking will become increasingly difficult, and the likelihood of apprehension for traffickers will become extremely high.[12] In addition, the increased use of National Guard Forces on the border to supplement the increasing numbers of Border Patrol agents will provide the manpower necessary to respond to the alerts given by the newly emplaced systems. As Los Zetas and their associates face an increasingly difficult smuggling environment, the fear of increased attention and border security as a result of IED use may become a non-issue.

In addition to the threat of increased border security, a second factor may hold the potential to force Los Zetas toward IED proliferation. The New Federation led by Sinaloa is not only the largest alliance of cartels, but it frequently declares its desire to eliminate Los Zetas due to their increasingly unorthodox and casualty-producing tactics.[13] In addition, the government has focused its attention on Los Zetas and their allies, with the Beltran-Leyva Cartel suffering the most from the recent capture of multiple high-ranking leaders.[14]

While Los Zetas are currently holding their own, they are beginning to show signs of weakening due to the constant attrition of their personnel and resources. If Sinaloa completes its takeover of Juarez and Los Zetas fail in their recent bid to expand their influence in Monterrey, they will face an increasingly desperate situation. With less trafficking routes available for use, they will be hard-pressed to match the growing resources of the New Federation. Their only recourse will be an attempt to do more with less, providing a prime opportunity for IED use. The cost of an IED pales in comparison to the amount of funds a successful shipment can provide, and any fallout in the form of additional border security would affect the New Federation as much as it would Los Zetas. As has been seen in other insurgencies, a pressured organization commonly retaliates by increasing attacks in an effort to increase public and political pressure on those who are targeting them. If Los Zetas find themselves backed into a corner, the use of IEDs would serve the dual-purpose of increasing pressure on the Mexican government as well as hampering the activities of the New Federation.

Once any of the cartels decide to begin using IEDs, the time between order and action is likely to be very short because the infrastructure necessary to build the devices and to conduct the attacks already exists. Spotters, whose only job is to monitor the U.S. Border Patrol movements, are actively assisting traffickers, and the transition from solely watching patrols to executing attacks would likely be very quick. The intent to injure or interdict Border Patrol agents is already present, as exemplified by the occurrence of barbed wire being stretched across patrol routes and sharp objects being placed on footpaths. Drug mules face varying threats if they return home without delivering their product, and they will carry and use weapons in order to defend their product. IED use is the logical next step as the traffickers will have to adopt new measures to disrupt Border Patrol operations as their likelihood of capture increases.

The cartels already contain many former engineers and miners who are experienced in the use of explosives, and they could easily transition into IED builders. TOVEX, a water-gel explosive that was released by E. I. du Pont de Nemours and Company (DUPONT) as a replacement for dynamite, is prolific in Mexico and has been found in both caches and IEDs throughout the country.[15] Despite the ruggedness of the border, many areas have a stable cellular network, thus allowing spotters to detonate the

device from a distance without exposing themselves to capture. Since not all IEDs are emplaced on roadways, it is likely that alternate tactics that are used in Mexico, such as placing the device next to a body, would also be employed. Cartel members know that security forces will have to react to this discovery, making a successful strike all but certain.[16]

The emplacement of an IED inside a drug bundle is also a likely scenario. The Border Patrol is known to simply stack these bundles together and to move them into a warehouse or holding area after they are found which provides numerous opportunities for a casualty-inflicting remote detonation.

In addition, the cartels have the potential to create more sophisticated devices than those that have been seen in either Iraq or Afghanistan. They have the luxury of learning from these insurgencies since the methodologies learned by those who participated in fighting U.S. forces are widely available on the Internet. The cartels have greater financial capabilities than the threat groups in Iraq and Afghanistan, and they have the money to construct devices that use technologies that cannot currently be defeated. The cartels would also have a distinctly different target set, as the Border Patrol is a paramilitary force that is not trained in or equipped for CIED (counter-IED) operations. The cartels would likely outpace current CIED efforts and capabilities very quickly, and the U.S. would find itself at a serious disadvantage in a short time period.

In reference to the threat of IED proliferation, the intelligence community has been limited to reactive rather than proactive measures, and the situation along the southern U.S. border is shaping up to become a scenario that will be similar to what has been seen in the past. The only thing currently preventing the use of IEDs along the border is an unsteady decision by the cartels. Appropriate measures must be in place and concrete steps must be taken to diminish any potential gain that could be obtained from IED use if the U.S. is to avert this threat.

The reason IEDs are employed is because they are easy to use, effective and relatively inexpensive. If the cartels suffer more loss than gain from their early attempts to employ IEDs, they will be much less willing to spend the time and money to advance their devices and to overcome any countermeasures. However, if the cartels experience early success due to a lack of preparation on the part of the U.S., they will have the opportunity and motivation to build upon their experiences, and to adjust their tactics and upgrade their devices, as any countermeasures are likely to arrive piecemeal. If early IED attacks by the cartels succeed, this kind of tactic will be perceived as cost-effective, and will turn what might have been a short-term threat into a long-term one.

Protective Measures against Potential IED Threat

A critical measure that must be implemented is the addition of various cartels to the *Declared Terrorist Organizations* list that is maintained by the U.S. State Department. This list currently contains no groups related to Mexico's violence, despite these groups meeting all the necessary criteria, as they are an obvious threat to both U.S. citizens and interests.[17] The parallels between the cartels and other groups already on the list are readily identifiable, particularly since some of their more heinous acts of beheading, assassination, and mutilation are identical in nature.

Adding these groups to the *Declared Terrorist Organizations* list would open new avenues for the prosecution of individuals associated with these organizations and would provide a secondary benefit of encouraging detained cartel members to work against their former comrades due to the threat of

long prison sentences. Officially declaring the cartels as terrorists allows for the freezing of business and organization assets known to be associated with these activities. This would provide agencies such as the Drug Enforcement Administration (DEA) and the Bureau of Alcohol, Tobacco and Firearms (ATF) more opportunities to target those responsible for working with the cartels to provide the *counterflow* of money, weapons, and supplies into Mexico from the U.S.. These pipelines remain a primary concern since 36 percent of the illegal weapons found in Mexico in 2008 were sent to the ATF for tracing and 90 percent of these weapons were found to have originated in the U.S.[18] Security agencies would have a greater case when seeking more resources to combat these groups since working against a declared terrorist organization makes for greater justification when requesting the allocation of additional resources.

The intelligence community must significantly improve its interagency sharing of information that already exists, as the individuals and networks being hunted by the Federal Bureau of Investigation, DEA, and the ATF, for their smuggling activities would also be the ones responsible for any IED use. The information on these individuals and networks must be shared between these organizations and with the Border Patrol in order to hasten any potential incident interdiction and response once an IED event occurs. Cooperation and liaison with Mexican authorities to jointly target individuals associated with the current IED use in Mexico must increase, as this will degrade the current and future capabilities of the cartels. Information sharing with Mexico will provide the groundwork required to understand and defeat the cartel networks responsible for operations north of the border. Using the time available to obtain fingerprints of builders, to establish building styles, and to identify the more experienced builders will ensure a quick, precise, and decisive action following any IED event. These, and other forensic measures, will prove critical in defeating IED networks in Iraq and Afghanistan, and bringing them into play now will greatly enhance the targeting capabilities of the U.S. and Mexico.

New tools and training regarding this threat must also be given to the Border Patrol and regional law enforcement organizations, as they are the most likely targets of any attack. Various sprays capable of detecting explosive residue are widely available and can be used in a variety of practical ways. Any attempt to have counter remote-controlled IED (RCIED) electronic warfare (CREW) systems placed on Border Patrol vehicles on a large scale is unlikely due to both cost and high frequency of clearance issues involving the Federal Aviation Agency and Federal Communications Commission. However, a plan to have few vehicles per sector equipped with CREW devices for limited use only during suspected IED threats would likely be authorized and would meet budget constraints. As there is a large pool of professionals who have vast experience in dealing with IED attacks, an effective training program would be easy to implement and would be low cost if combined with existing programs.

Intelligent procedures must be implemented so that the cartels lose far more than they gain from conducting these attacks. This will also ensure that these threats have limited duration. The primary intent of an attack will be to draw Border Patrol agents away from their duties to respond to a situation thus opening the way for traffickers. It will be much easier for Border Patrol agents to maintain their assignments if they know that the situation is being handled effectively, rather than being caught off-guard with no set of tested procedures in place for emergency response. Training for an IED event in advance will result in reaction based on established procedures rather than on hesitation and will result in a manageable situation rather than a crisis situation. The secondary motivation for these attacks is to instill fear and caution into Border Patrol agents and to slow their response due to the real or perceived threat of an IED. Proper training that involves IED recognition and reaction procedures, along with the availability and presence of countermeasures, will undermine this more subtle effect, which is the intent of current IED use in Mexico.

Conclusion

As the saying goes, the intelligence community must stay *left of boom,* and the opportunity to do this is slowly slipping away as this threat draws ever nearer. Rather than wait until the situation gets out of control, security services must prepare now to ensure that any attempt to exploit the border using IEDs is short. The U.S. has learned numerous lessons in regard to IED use due to its experiences in

Iraq and Afghanistan. None of these lessons, however, are being used on the border. The longer this threat is ignored, the more devastating its effects will be once attacks occur. The U.S. has willingly ceded the initiative, and its inaction has provided the cartels an opportunity to implement explosive devices whenever they so desire. As conditions inside Mexico and along the border change; and as it becomes more worthwhile to risk reaction to IEDs, the attacks will begin. If the U.S. undertakes a quick and comprehensive strategy now, it still has an opportunity to both prepare for and eventually negate its effectiveness.

Endnotes

1. Kimberly Dvorak, "Los Zetas Drug Cartel Seizes 2 U.S. Ranches in Texas," *The Examiner*, 24 July 2010, retrieved at http://www.examiner.com/county-political-buzz-in-san-diego/los-Zetas-drug-cartel-seizes-2-u-s-ranches-texas.

2. George W. Grayson, "Mexico and the Drug Cartels," *Foreign Policy Research Institute*, August 2007, retrieved at http://www.fpri.org/enotes/200708.grayson.mexicodrugcartels.html.

3. Samuel Logan, "Los Zetas: Evolution of a Criminal Organization," *ISN Security Watch*, 11 March 2009, retrieved at http://www.isn.ethz.ch/isn/CurrentAffairs/SecurityWatch/Detail/?id=97554&lng=en.

4. Ibid.

5. Robert Campbell, "Drug War Puts Mexican Oil Industry on Defensive," *Reuters*, 4 August 2010, retrieved at http://www.reuters.com/article/idUSN0417574420100804.

6. Tracy Wilkinson, "Mexican Drug Cartels Cripple Pemex Operations in Basin," *Los Angeles Times*, 6 September 2010, retrieved at http://articles.latimes.com/2010/sep/06/world/la-fg-mexico-pemex-20100906.

7. Ibid.

8. Matt Badiali, "One of the World's Biggest Oil Producers Is Going Bust," *Daily Wealth*, 10 April 2010, retrieved at http://www.dailywealth.com/1323/One-of-the-World-s-Biggest-Oil-Producers-Is-Going-Bust.

9. John Murray, "Ciudad Juarez: War against Los Zetas, Along the Gulf and Into America," *The AWL*, 22 April 2010, retrieved at http://www.theawl.com/2010/04/ciudad-juarez-war-against-los-zetas-along-the-gulf-and-into-america.

10. Martin Barillas, "Is Mexico on the Verge of Collapse?" S*pero News*, 9 February 2009, retrieved at http://www.speroforum.com/a/18087/Is-Mexico-on-the-verge-of-collapse.

11. E. Eduardo Castillo, "Car bomb Damages Mexico TV Building," *The Washington Post*, 28 August 2010, retrieved at http://www.washingtontimes.com/news/2010/aug/27/car-bomb-damages-mexico-tv-building/.

12. Border Patrol Announcement. *SBInet*, 2009, retrieved at http://www.cbp.gov/xp/ cgov/border_security/sbi/sbi_net/.

13. Jen Phillips, "Mexico's New Super-Cartel Ups Violence in Power Play," *Mother Jones*, 13 April 2010, retrieved at http://motherjones.com/mojo/2010/04/evolution-mexicos-cartel-war.

14. Earl Cebedo, "Alleged drug cartel leader in Mexico, arrested," *All Voices*, 12 September 2010, retrieved at http://www.allvoices.com/contributed-news/6741041-alleged-drug-cartel-leader-in-mexico-arrested

15. Alicia A. Caldwell, "US Official: Industrial Explosive Tovex Likely Used in Car Bomb Attack Against Mexican Police," *The Associated Press*, 19 July, 2010, retrieved at http://www.news1130.com/news/world/article/79260--us-official-industrial-explosive-tovex-likely-used-in-car-bomb-attack-against-mexican-police.

16. Oscar Villalba, "Massacre in Mexico: 17 killed at party," *The Associated Press*, 8 July 2010, retrieved at http://www.wfaa.com/news/world/Massacre-in-Mexico-17-killed-at-party-98705879.html.

17. Office of the Coordinator for Counterterrorism, *Foreign Terrorist Organization*, 6 August 2010, retrieved at http://www.state.gov/s/ct/rls/other/des/123085.htm.

18. William La Jeunesse and Maxim Lott, "The Myth of 90 Percent: Only a Small Fraction of Guns in Mexico Come from U.S.," *Fox News*, 2 April 2009, retrieved at http://www.foxnews.com/politics/2009/04/02/myth-percent-small-fraction-guns-mexico-come/.

Works Cited

Ganor, Boaz. *The Counter-Terrorism Puzzle: A Guide for Decision Makers*. (NJ: Transaction Publishing, New Brunswick, 2008).

Walsh, Mark. "Explosion at Pemex refinery kills 1 in Mexico," *The Associated Press*, 8 retrieved at September 2010, retrieved at http://www.760kfmb.com/Global/story.asp?S=13111843.

Sergeant Ludwig has deployed twice in support of OIF, in 2006-2008 with the 1st Cavalry Division G2 assigned as the Al Qaeda in Iraq High-Value Individual Targeting Analyst and in 2009, again with 1CD as the Lead AQI and Sunni Insurgent Analyst until the Division redeployed in 2010. He is currently assigned to the CIED Branch of the Intelligence Electronic Warfare Test Directorate at Fort Huachuca, Arizona.

Intelligence Support to the Prevention and Mitigation of Civilian Casualties

by First Lieutenant Nathaniel L. Moir

Introduction

It is an oft-quoted truism that "Intelligence drives Operations," as the Intelligence Section is responsible for the preparation and assessment of the battlefield. However, many Intelligence sections do not always fully utilize enablers in shaping and assessing the battlefield environment as it relates to preventing and mitigating civilian casualties (CIVCAS). This may lead to an incomplete assessment of the battlefield which potentially weakens the prevention of CIVCAS. What, then, is the role of Military Intelligence (MI) as it relates to CIVCAS incident prevention and mitigation and why is it important?

The issue of CIVCAS is addressed in this article along two main themes. The first regards support that may be provided in preventing CIVCAS. This is examined by looking at how force 'enablers' may contribute to Intelligence Preparation of the Battlefield (IPB) as a tool in mapping human terrain more extensively. Increased use of enablers is also discussed as a way to increase population-centric approaches to counterinsurgency (COIN) operations such as Operation Enduring Freedom (OEF). Population-centric approaches, versus enemy-centric approaches, are keys to more effective prevention of CIVCAS and this may be achieved through greater inclusion of enablers into the IPB process.

The second theme of the paper addresses the mitigation and control of CIVCAS when it does occur. This focuses on how intelligence sections, through use of enablers and Information Operations (IO), may more effectively assist in lessening the operational impact of CIVCAS in the public's perception at both local, and potentially, international levels.

CIVCAS–Why it is Important, Why it is a Problem

The issue of civilian casualties continues to be a major issue during OEF and directly impacts the effectiveness and legitimacy of the International Security Assistance Force (ISAF) mission. Therefore, the importance of preventing, and quickly responding to CIVCAS in the battlespace, whether caused by insurgents or Coalition Forces (CF), is critical. In this regard, CIVCAS has important operational implications for the local base of support for the CF. Insurgents seek to manipulate incidents of CF-caused CIVCAS. They further blame the CF of CIVCAS that insurgents themselves have unintentionally caused and, in many cases, intentionally caused for the explicit purpose of weakening support for the ISAF's mission.

Due to the speed and ease of communications technology, reports of CIVCAS may be broadcast internationally. This factor is manipulated by insurgents to decrease support for Coalition and the Government of the Islamic Republic of Afghanistan's efforts in courts of public opinion. CIVCAS, thus, is an ostensible strategic concern; its prevention and mitigation should be a priority for battlespace owners from squad leaders and up the chain of command. Unfortunately, Intelligence Sections are not fully utilized in efforts to prevent and mitigate CIVCAS. All too often, S2 Sections demonstrate an overall enemy-centric focus.

This, of course, is Intelligence's modus operandi but all operational approaches must be consistently refined and adapted to the conflict at hand. This is not to suggest that targeting and destroying the enemy effectively should be shortchanged or under-resourced in any way. Finding, fixing, and destroying the enemy is absolutely critical to achieving security in an area of operations (AO). The scope here however, is preventing and mitigating CIVCAS. Gaining local support for operations entails support for multiple lines of operations to include governance, and development, not just security. Regarding COIN, population-centric efforts remain the preferred approach to achieving long-term success as multiple historical case studies indicate.[1]

Whether a maneuver unit is enemy-centric or population-centric is demonstrated by the operations it conducts. In the case of enemy-centric operations, the obvious and inherent focus is the enemy and its courses of action (COAs). The army is traditionally enemy focused so the process of IPB is inherently enemy-centric. In the case of OEF, enemy-centric approaches have caused the U.S. Intelligence community to conduct an anti-insurgency campaign rather than a COIN campaign. As one source states, "Anti-insurgent efforts are, in fact, a secondary task when compared to gaining and exploiting knowledge about the localized contexts of operation and the distinctions between the Taliban and the rest of the Afghan population."[2]

Intelligence can better adapt to COIN however, by adding substantive augmentation and greater population-centric assistance as it relates to the prevention and mitigation of CIVCAS. Including enablers such as Human Terrain Teams (HTTs), Psychological Operations (PSYOP), Red Teams, and Civil Affairs (CA) provides such augmentation for developing more population-centric IPB. Perhaps paradoxically (but not surprisingly), most of these enablers are not organic to brigades which may explain why Intelligence, Operations, and Planning Sections (which are organic to brigades) are hesitant, slow, or even refuse to incorporate enablers into their operations.

Even within brigades, some battalions will be very receptive to 'outside' organizations while others may not. Ultimately it depends on the unit. However, until maneuver elements plan and direct population-centric operations, and thus direct Intelligence Sections to increase its focus on the population rather than solely on the enemy, COIN will continue to challenge the U.S. military's ability to achieve the results it seeks. Such a "shift" in approach is a paradigm change with many challenges that authors such as John Nagl and David Kilcullen have cogently discussed at great length.[3]

Prevention of CIVCAS–Mapping Human Terrain

Increasing the communication channels between S2 sections, HTTs, Red Teams, CA Teams, PSYOP Teams, along with other enablers, is a key factor in making Intelligence Sections more relevant in the prevention and mitigation of CIVCAS. An example is in order to highlight this issue. The Field Artillery is one of the most lethal capabilities within the U.S. Army; it is critical to emphasize the importance of ground clearance of fires. One way to achieve this is by utilizing Collateral Damage Estimation methodology. This process is already in place for lethal en-

gagements but could potentially be used every time a lanyard is pulled to include ground clearance. This is relevant because indirect fire is a primary source of CIVCAS. However, while all CF-caused CIVCAS is unintentional, the source of CF-caused CIVCAS is irrelevant.

Regarding improvised explosive devices (IEDs), for example, local nationals still hold CF accountable for having failed to protect them. A commonly stated argument by Afghans is, to paraphrase, "Insurgents wouldn't plant IEDs if the CF weren't present." The CF are regularly put into such paradoxical situations regarding CIVCAS in the public's perception. Direct fire, and especially indirect fire, however, may be potentially prevented, and certainly mitigated with more success, through a greater understanding of the human terrain in AOs through Open Source Intelligence and greater input from enablers.

Population-centric approaches to successful COIN operations are imperative. To be successful with more population-centric approaches, S2 Sections must allocate more analysis of the civilian environment rather than allocating its attention solely on the enemy. Clearly, this would require a major shift in priorities but one that is necessary for conventional forces to truly address counterinsurgencies successfully. As it is noted in the paper, *Fixing Intel*, co-authored by Major General Flynn, a "vast and underappreciated body of information, almost all of which is unclassified, admittedly offers few clues about where to find insurgents, but provides information of even greater strategic importance: a map for leveraging popular support and marginalizing the insurgency itself."[4] Reducing CF-caused CIVCAS, and communicating the fact that insurgents are the primary cause of CIVCAS, is possibly one of the most powerful tools to successfully conduct COIN that the CF can further refine. One possible solution, as discussed earlier, is to bring enablers and analysis of human terrain together for more effective and relevant IPB. This could also be accomplished by an extended Fusion Cell Structure that incorporates and applies more population-centric analysis to operational planning.

Due to the importance of gaining Afghan local nationals' confidence and support, MI has an important role in preventing and controlling the negative effects of CIVCAS when caused by CF. When CIVCAS is caused by insurgents, communicating the occurrence to the local population more appropriately falls within the IO (S7) lane. However, S2 sections, and potential population-centric Fusion Cells, are relevant and provide critical support to shaping the Information Environment.

Mitigation of CIVCAS–The Information Environment

S7 staff sections cannot work in a vacuum. To more accurately and quickly address CIVCAS, S7 sections should proactively assist in contributing to the population-centric elements of IPB that S2 staffs develop. Naturally, this entails S2 sections seeking and accepting S7 sections' contributions. CIVCAS preventive steps, as clearly articulated steps within the IPB process, could be a reference that demonstrates measures in place to prevent CIVCAS. Further, these steps could be referenced, in an unclassified format, as insurance when CIVCAS incidents still occur that CF did everything possible to prevent. When CIVCAS does occur, efficient mitigation of its negative consequences in the Information Environment has a significant impact on mission success at tactical, operational, and potentially strategic levels. This is especially true in COIN where success is measured by local nationals' confidence in counterinsurgent forces' efforts. Failure to successfully mitigate authentic CIVCAS incidents at the tactical level may have operational and strategic consequences. Therefore, S7 sections, which synthesize multiple enablers such as PSYOP, Public Affairs, Combat Camera, and may include HTTs and Red Team depending on the brigade combat team, should be more directly partnered with Intel Sections regarding assessment and IPB development.

For example, IPB development may be affected by nomadic populations that enter an AO as part of seasonal migrations; the Kuchi Tribe in Eastern Afghanistan is one such example, possible influxes of refugees into an AO is another. However, understanding human terrain is more than knowing simple facts of where people reside. A possible COA, and one discussed earlier, is utilizing Intelligence that supports specific efforts made to prevent CIVCAS (for example, as part of pre-operations check-lists similar to Karzai's 12). Just as Most Likely COA and Most Dangerous COA are articulated, clearly de-

fined steps to prevent CIVCAS should be included as part of IPB and shared with maneuver and S7 sections in particular. These steps will assist in mitigating CIVCAS when it does occur.

- Adopt holistic Population-Centric approaches to Intelligence Preparation of the Battlefield.
- Further develop and increase Analysis of Human Terrain through IPB. Implement a human terrain-specific modified combined obstacle overlay.
- Develop an Intel Fusion Cell at brigade level that assists in formulating CIVCAS preventive steps and coordinates this preparation with IO Sections.
- Directly assist IO Sections in the mitigation of CIVCAS when it occurs. Utilize prescribed preventive steps, in an unclassified format, for reference in mitigating CIVCAS through press statements, and in shuras conducted to lessen operational impact of CIVCAS. Prescriptive Solutions

Prescriptive Solutions

Conclusion

Civilian casualties will happen in war. However, any mistake in this area is inexcusable to the majority of local nationals. It thus begs the question: Is any potential CIVCAS worth the operational risk of losing local national trust or confidence? In counterinsurgencies, such as OEF, CIVCAS typifies tactical incidents that have strategic repercussions. As one source states, "one of the peculiarities of guerrilla warfare is that tactical-level information is laden with strategic significance far more than in conventional conflicts."[5] Conventional IPB and current approaches to preventing CIVCAS can always be more effective. To achieve this, population-centric approaches to IPB and greater synchronization between IO Cells and S2 Sections is necessary. This may happen through greater inclusion of non-traditional 'enabler' assets into IPB: HTT, CA Teams, PSYOP Teams, and, overall, an increased focus on and analysis of human terrain.

In conclusion, CIVCAS must be effectively prevented and mitigated in order to gain the trust of local nationals. Clearly, local support for CF and the partnered efforts of Afghan Security Forces are critical in counterinsurgencies, such as that ongoing in Afghanistan. When insurgents cause CIVCAS, communicating their criminal actions to the local populace is important in order to degrade their bases of support. Conversely, poorly handled CIVCAS management, when caused by CF, is highly damaging to operations and may irreparably negate the credibility of CF. CIVCAS will continue to be a problematic issue with long-term consequences. It is also likely that CIVCAS will only gain in importance as news cycles increase in speed and reach. Even if CIVCAS remains impossible to completely prevent, greater utilization of enablers and Open Source Intelligence in preventing and mitigating CIVCAS is critical. Intelligence sections are urged to remember that their work should entail more than analysis focused on the enemy. In counterinsurgencies, lack or loss of popular support for counterinsurgents is arguably as much of an enemy, possibly more, than insurgents themselves. Preventing and efficiently mitigating CIVCAS is a cornerstone to fighting both enemies effectively.

Endnotes

1. David Kilcullen, *The Accidental Guerilla: Fighting Smalls Wars in the Midst of a Big One* (New York: Oxford University Press, 2009).

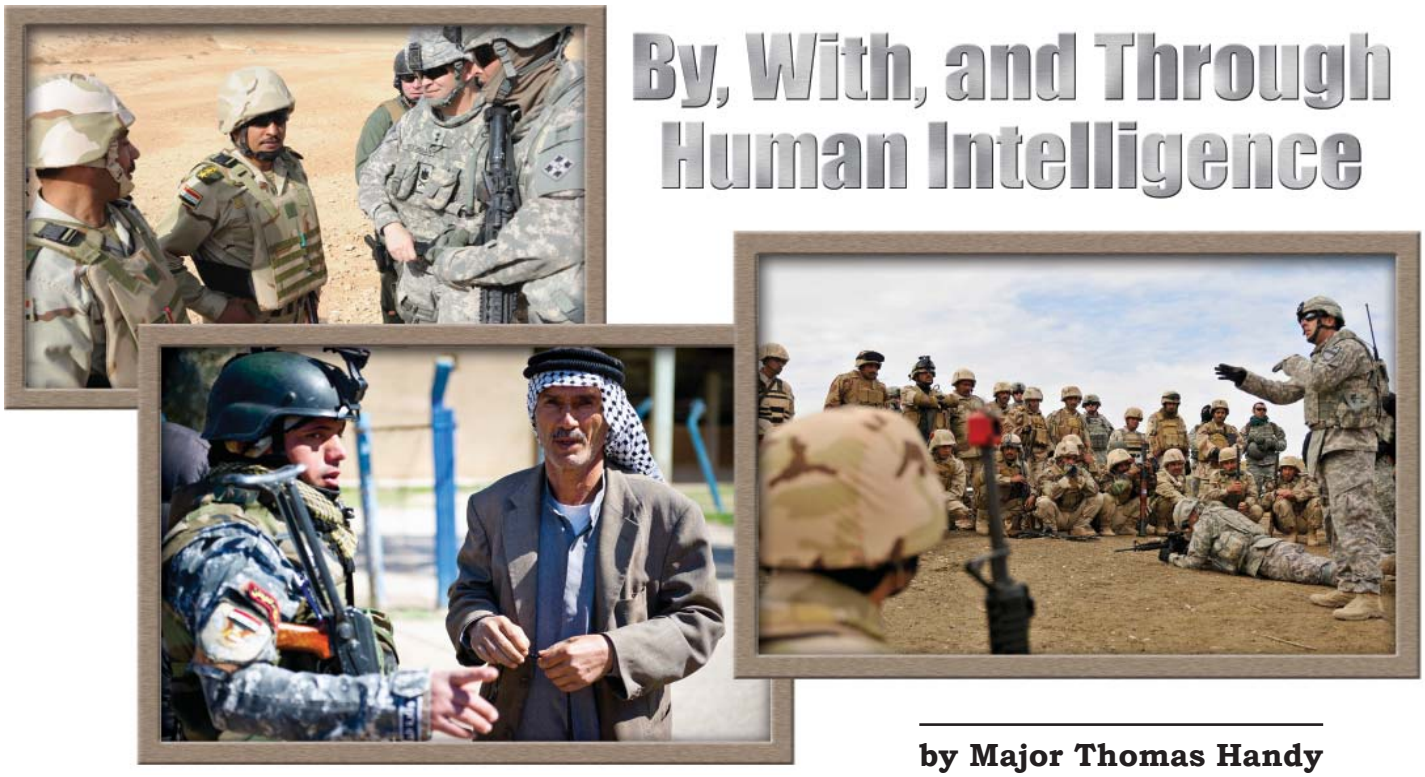
2. Major General Michael T. Flynn, Captain Matt Pottinger, and Paul D. Batchelor, *"Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan"* Center for a New American Security (Washington D.C., January 2010) 23.

3. Kilcullen, *The Accidental Guerilla* and John Nagl, *Learning to East Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Chicago: University of Chicago Press, 2005).

4. Flynn, 7.

5. Ibid., 11.

1LT Nathaniel L. Moir is a PSYOP Detachment Commander who recently completed a deployment to Afghanistan in support of 1BCT, 101st Airborne Division (AASLT) for OEF XI. He is branch qualified as a Military Intelligence Officer and has an ASI in Tactical Information Operations. His parent company is the 319th PSYOP Company..



By, With, and Through Human Intelligence

by Major Thomas Handy

Editor's Note: HUMINT team numbers have been changed to preserve the sensitivity of the teams and members.

Introduction

The country of Iraq went through tremendous changes in 2009 with the implementation of the security agreement. One U.S. Army unit in particular witnessed these changes first hand. Charlie Company, 303rd Military Intelligence Battalion, 504th Battlefield Surveillance Brigade (BfSB), based out of Fort Hood, Texas, deployed to southern Iraq in the fall of 2008 to provide Human Intelligence (HUMINT) in support of Operation Iraqi Freedom. Charlie Company's HUMINT Collection Teams, (HCTs) composed of three to four personnel, provided direct support to four brigade combat teams (BCT) in southern Iraq. During this critical period of the war, the U.S.-Iraqi security agreement provided more authority to the Iraq military. U.S. forces needed to minimize this change while still providing intelligence to support battlefield commanders.

Iraqi intelligence receives training from the Taji Academy where basic Military Intelligence is taught. To further Iraqi's intelligence education, Charlie Company was given the mission to validate a proof of concept to partner with U.S. Military Transition Teams (MiTT). HCT 356 partnered by, with, and through Iraqi forces as they supported 10th Iraqi Army (IA) MiTT under the direction of 4/1 BCT from Fort Hood, Texas. Within a year, the HCT was able to gain intelligence from the 10th IA Division and the local Iraqi Police (IP) intelligence sections to gather information to answer the battlefield commander's priority intelligence requirements and the lines of operation.

During the course of the year, several other HCTs in theater also partnered with Iraqi Forces in locating weapon caches and deterring rocket attacks on U.S. and Iraqi installations. This new partnership drastically improved the intelligence collection and analysis capability of Iraqi forces. FM 3-24, Counterinsurgency, states "even in situations where the U.S. goal is reducing its military force levels as quickly as possible, some support for HN institutions usually remains for a long time."[1] The overall intent of the HCT and Iraqi partnership was for Iraqi forces to increase their capacity building as they provided their own intelligence, while U.S. forces begin to draw down in Iraq.

FM 3-24 served as a basis for this partnership. The framework for this discussion is described in the manual:

Insurgencies are protracted by nature. Thus, COIN operations always demand considerable expenditures of time and resources. The populace may prefer the HN government to the insurgents; however, people do not actively support a government unless they are convinced that the counterinsurgents have the means, ability, stamina, and will to win. The insurgents' primary battle is against the HN government, not the United States; however, U.S. support can be crucial to building public faith in that government's viability. The populace must have confidence in the staying power of both the counterinsurgents and the HN government. Insurgents and local populations often believe that a few casualties or a few years will cause the U.S. to abandon a COIN effort. Constant reaffirmations of commitment, backed by deeds, can overcome that perception and bolster faith in the steadfastness of U.S. support. But even the strongest U.S. commitment will not succeed if the populace does not perceive the HN government as having similar will and stamina. U.S. forces must help create that capacity and sustain that impression.[2]

The Iraqi Partnership Program

As the security conditions in Iraq changed, the local populace needed to see the Iraqi face on military operations as the Iraqi Security Force (ISF) defending their country. This capacity building provided an assurance that the country would be in the capable hands of the ISF as they carried out the operations. To ensure this transfer of authority was complete, the ISF needed to adopt some U.S. methods to ensure they could capably assume the mission given the withdrawal of U.S. forces. The HCT proof of concept was the critical link to ensure the intelligence process would develop and provide the framework for Iraqi forces in future military operations.

In early January, HCT 356 began the process to partner with the 10th IA Division MiTT. HCT 356 conducted training with their IA and IP counterparts over the course of the year. Team members trained the Iraqis on tasks such as tactical questioning, evidence collection, gathering sworn statements, and the warrant process to detain suspected persons. As part of the security agreement, the Iraqi warrant process had to be explained to the IA and IP so they could understand the process U.S. forces used to detain suspected persons. The HCT led the Iraqis through a crawl, walk, and run training plan to ensure the lessons were accurately retained. Other HCTs who partnered with Iraqis taught classes on the use of GPS, map reading, and basic questioning techniques. This training foundation gave the Iraqis the confidence to use these enablers in their daily operations and prove their ability to the Iraqi populace.

Establishing an Iraqi partnership is not as easy as it sounds. The Iraqi unit must be willing to engage in the partnership program. This may require several informal agreements between the U.S. and Iraqi military prior to formally establishing the partnership program. There are also several external factors necessary for the partnership to be successful. First, the HCTs supported unit has to be willing to support the HCT and align it with an Iraqi unit for the partnership to begin. The HCT may have the experience to begin the partnership immediately, but without the unit's support, the HCT and Iraqi partnership will be ineffective. Also, the supported unit has to provide the logistical resources for the HCT to establish operations since the team is not an organic asset to the BCT. The HCT brings basic requirements such as computers, printers, and intelligence equipment but basic necessities such as office space, lodging, and meeting rooms are still needed to conduct operations. The supported unit needs to provide the logistical support for the HCT to be effective so they can concentrate on establishing the intelligence partnership program.

Once the ISF was prepared to conduct operations, they demonstrated that they can locate indicators of impending attacks as well as weapon caches. With the assistance of HCT 098 and the supported unit, 172nd BCT, the IA identified over twelve weapon caches. The items found were improvised explosive device components and rockets that were planned

for use in future attacks. This partnership saved an unknown number of lives.

Conclusion

The partnership program is a valid concept that was implemented as U.S. forces began to draw down in Iraq, paving the way for the future. The Iraqi forces continue to partner with HCTs with effective results. Still, more learning is required for Iraqi forces but they are on the right path and will continue to improve over time. The same concept can be utilized in Afghanistan when certain conditions are met and the Afghanistan National Army is prepared to conduct operations on its own with limited assistance.

Endnotes

1. FM 3-24, Counterinsurgency, 2006, 1-134.

2. Ibid.

Major Tom Handy is the former Company Commander for C Co, 303rd MI Battalion, 504th BfSB during OIF 09-11. Currently he is the 162nd Infantry Brigade S2 as the senior intelligence officer advising the Foreign Security Forces Combat Advisor for units deploying to OEF and OND. He holds a BA in Political Science from Norwich University and an MA in Public Administration from Central Michigan University. Previous assignments include Current Operations Officer, 504th BfSB, 504th MI Bde Planner in OIF; J2, Joint Logistics Command in OEF; S2, 2-35th Infantry BN; AS2 1-27th Infantry BN, and DISE Platoon Leader, 532nd MI BN. Major Handy can be contacted at thomas.c.handy@us.army.mil.

Taliban Networks:

Assessing The Role of Non-Kinetic Operations in the Battle of Kandahar and Beyond

by First Lieutenant Tyler Jost

In 1994, a group of relatively unknown Afghan students based in southwestern Pakistan, and now commonly known as the Taliban, began a campaign to oust the Burhanuddin Rabbani regime in Kabul. This article examines the Taliban's first military engagements in the battle for Kandahar Province and the ways in which the Taliban tailored their strategy to fit the political realities in which they operated. In doing so, it argues that the kinetic aspects of the operation are necessary but insufficient to understand military outcomes. The non-kinetic components of Taliban operations played an equally, if not more, significant role in securing the Taliban's victory.

The first documented kinetic operation began on 12 October 1994. A group of Taliban militants raided a Hizb-i Islami arms depot, which was located fifteen kilometers north of Spin Boldak (See Figure 1) and was operated by the political-military network under Gulbuddin Hekmatyar.[1]

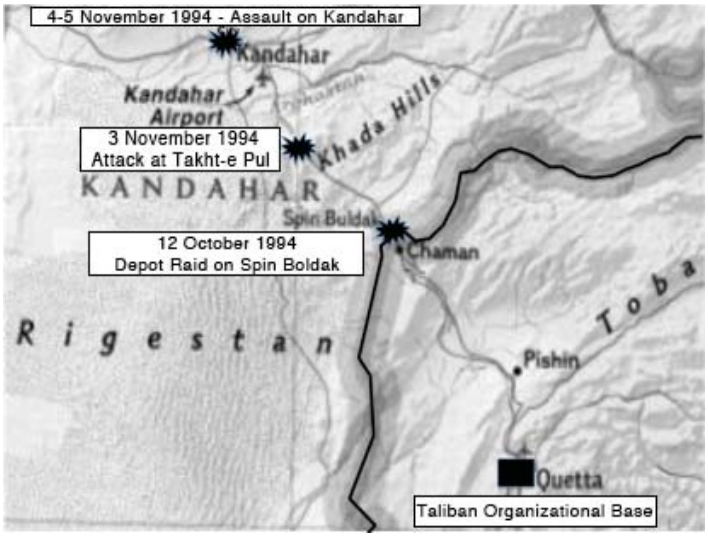


Figure 1. Taliban Activity in the Battle of Kandahar

Hiding themselves in two tarpaulin-covered Hino trucks and reportedly paying off forty-two highway checkpoints along the way, Taliban drivers under the command of Mullah Omar and Mullah Borjan transported the fighters to the depot undetected, took enemy commander Mullah Akhtar Jan by surprise and quickly secured the area.[2] In capturing the depot, the Taliban gained approximately 18,000 Kalashnikovs, dozens of artillery pieces, and hundreds of thousands of rounds of ammunition.[3] More importantly, the victory lent credibility to the Taliban movement vis-à-vis the array of competing warlord networks.[4]

The second major operation came in early November, after a local warlord named Mansur Achakzai stopped a Pakistani military convoy containing thirty vehicles loaded with medicine, consumer goods and foodstuffs. The convoy was detained near Takht-e Pul (See Figure 1) in hopes of exacting political concessions from Islamabad. Mansur and two other Kandahar commanders–Amir Lalai and Ustaz Haleem–sought two outcomes: To tax Pakistani trade transiting through Kandahar, and to end Pakistani support for the Taliban movement.[5] On 3 November, Taliban commander Mullah Borjan led two hundred followers in assaulting and defeating forces detaining the convoy.

In the following days, Mullah Omar and Mullah Borjan, although outnumbered, initiated a final maneuver to secure the provincial capital. According to one former Pakistani military officer, government forces under General Naqib consisted of "2,500 troops, 120 tanks, 80 to 90 artillery pieces, six MiG-21 fighter aircraft, and six Mi-8 helicopters."[6] However, Taliban leaders successfully co-opted

Naqib. In fact, one recently released first-hand account from a former Taliban fighter refers to Naqib not as "general," but as "mullah." That is, the Taliban radically redefined battlefield force distribution by turning potential adversaries into allies.[7]

Moreover, while Naqib may have been the most powerful warlord that the Taliban co-opted, he certainly was not the only one. The Taliban developed numerous relationships with other Kandahar strongmen, including Keshkinakhud administrator Hajji Bashar and Argestan religious leader Mullah Rabbani Akhund.[8] Indeed, the decisive victory in Kandahar seems to have come–not on the battlefield–but during a meeting in Panjwayi, in which six Taliban leaders forged an informal agreement to coordinate efforts against the last remaining warlord, Ustaz Abdul Haleem. After the removal of Ustaz, the Taliban quickly gained control of the capital, with only a minimal number of governor Gul Agha Sherzai's troops resisting.[9]

The Taliban's ability to mobilize previously existing political-military networks in order to alter battlefield dynamics highlights a broader trend in their campaign to control Afghanistan. Indeed, the Taliban established a unique set of tactics, techniques and procedures that differed significantly from the mujahedeen era hit-and-run tactics. Instead of relying on insurgent advantages in guerilla warfare, the Taliban adopted a dynamic, mobile, and aggressive operational tempo.

While Taliban propaganda suggests that success in employing such tactics stemmed from the movement's popular support and Taliban combatants' ideological zeal, Anthony Davis argues that Taliban proficiency in mobile warfare instead resulted from successfully integrating networks of former soldiers, who had been trained during the Soviet occupation in the employment of air, artillery, mortar and armor assets. The most notable of these networks was that of Defense Minister General Shahnawaz Tanai, who mobilized and persuaded former colleagues to assist in Taliban military operations. In fact, one source estimated that 1,600 officers from the People's Democratic Party of Afghanistan (PDPA) regime were serving with the Taliban by 1995.[10]

It is worth asking why the Taliban succeeded in network mobilization, as opposed to their competitors.[11] As Abdulkader Sinno describes, one important reason was the Taliban's understanding of human geography, which informed their decisions on which approach (co-option, repudiation, or assassination) to utilize with adversary commanders (See Figure 2).[12] In particular, Taliban leaders often engaged subordinates of a targeted leader first in order to undermine his power base, before subsequently offering the leader the choice of disbanding his militia, joining the Taliban organization, or facing lethal persecution.[13]

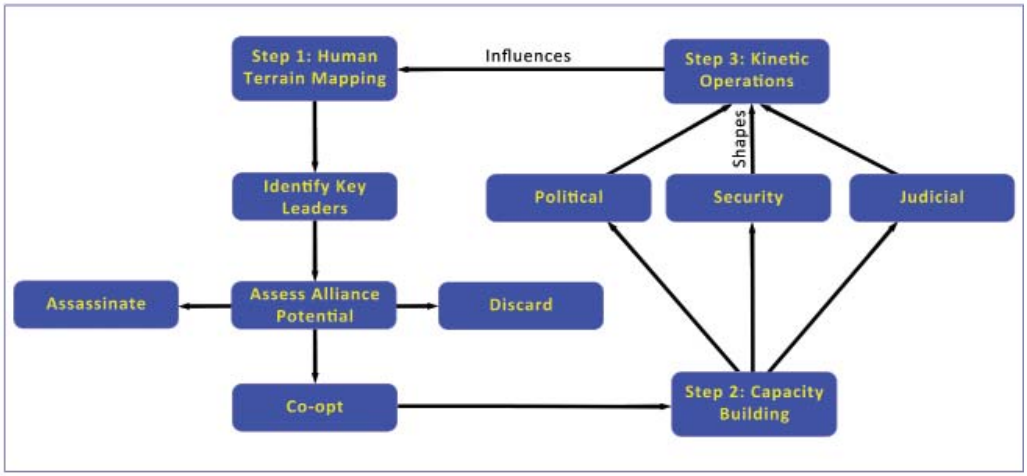


Figure 2. Taliban Networking Operations[14]

In addition, Taliban identity itself increased persuasive efficacy. In Afghanistan, tribe, ethnicity, and clan (qawm) influence identity far more than in Western nations.[15] As such, many of the failures of Afghan state modernization can be traced back to organic preferences for local autonomy and traditional power structures that oppose a central state.[16] Yet, the Taliban were not commonly associated with such state centralization efforts, as Taliban did not share the anti-tribal, urbanite background commonly associated with political leaders seeking to revolutionize Afghan society, such as rival Pashtun warlord Hekmatyar.[17] On the contrary, the Taliban marketed themselves as a neutral party capable of restoring justice and order in a country plagued by warlord exploitation and brutality.

Finally, Taliban networks enjoyed support outside Afghan borders, most notably in the Pakistani Inter

Services Intelligence (ISI), the organization that had previously coordinated mujahedeen resistance to the Soviet occupation.[18] These connections substantially shaped operations in Kandahar. One report indicates that Pakistan provided indirect fire support during the Spin Boldak raid. Pakistan also provided logistical assistance. In the final assault on Kandahar City, Taliban combatants were reportedly armed with new weapons, supplied through Pakistani channels.[19] In addition to military assets, Pakistan provided political and financial support. For example, Colonel Imam, the Pakistani ISI representative in Afghanistan at the time, reportedly assisted in securing Naqib's cooperation through a 1.5 million USD bribe.[20]

The Taliban's ability to shape the battlefield through managing political-military networks before kinetic operations commenced proved an overwhelming advantage against a clearly divided group of self-interested warlords. Such insights might help inform modern International Security Assistance Force (ISAF) operations in Afghanistan. While historical comparisons must be drawn cautiously, co-opting political-military networks represents a viable strategy that would likely assist counterinsurgency (COIN) efforts. As Michael Semple argues, the Taliban is a patchwork of political loyalties:

> ***[...] the current insurgency is not monolithic, but rather a loose association of different commander networks that have some overlapping interests but that also have varying degrees of adherence to the leadership of the Taliban movement. Although [...] the prospects of a general political agreement between the Afghan government and the insurgency are poor, [...] there is potential for the reconciliation of particular commander networks [emphasis added].***[21]

However, ISAF cannot exploit these divisions if it does not invest sufficient intelligence resources into mapping human terrain. "Friendly" link diagrams and orders of battle are just as important as their "enemy" counterparts, as distinctions between friend and foe in a COIN environment should be proactively manipulated rather than passively accepted. Thus, ISAF intelligence operations can and should incorporate lessons learned from Taliban successes into its own process.

Yet, the Taliban continues to possess a substantial advantage over ISAF forces in network mobilization, as foreign advisors will never be able to match the Taliban's understanding of human geography. The Afghan National Army (ANA) may prove more adept, but even they will face challenges, as most ANA soldiers deploy to locations outside their native province.[22] At the same time, the Taliban has gradually lost its reputation as a neutral and just governor in many parts of the country.[23] This presents an opportunity for ISAF to leverage popular discontent in order to solicit intelligence that facilitates network mapping in exchange for security and socio-economic assistance. As stated in Major General Michael Flynn's recent report on intelligence in Afghanistan, the key is to focus on the non-lethal elements–including network manipulation–rather than massing resources to plan the next "kill-or-capture" mission.[24]

Endnotes

1. Reports on the exact number of individuals involved in the attack range from forty to two hundred.

2. Abdul Salam Zaeef, *My Life with the Taliban*, Editors: Alex Strick van Linschoten and Felix Kuehn (New York: Columbia University Press, 2010), 72 and David Loyn, *In Afghanistan: Two Hundred Years of British, Russian and American Occupation* (New York: St. Martin's Press, 2009), 181-2. Zaeef's account indicates that fighting may have ended in as little as fifteen minutes.

3. Ahmed Rashid, *Taliban: Militant Islam, Oil and Fundamentalism in Central Asia* (New Haven: Yale University Press, 2001), 27-8.

4. Kamal Matinuddin, *The Taliban Phenomenon: Afghanistan 1994-1997* (Oxford: Oxford University Press, 1999), 60-2.

5. Anthony Davis, "How the Taliban Became a Military Force," *Fundamentalism Reborn: Afghanistan and the Taliban,* Editor: William Maley (New York: New York University Press, 1998), 47-8.

6. Ibid, 67.

7. Zaeef, 72-3. Some scholars argue that then incumbent President Rabbani supported Naqib's decision to cooperate with the Taliban. See also Davis, 49-50. Such explanations seem plausible given that Rabbani likely viewed the early Taliban movement as a means to undermine Hekmatyar, who was heavily engaged in armed conflict against the Rabbini coalition in Kabul. Whatever the case, not only did Naqib not resist, but he offered heavy weapon support for Taliban fighters as well.

8. Zaeef, 69-70.

9. Ibid, 73-5. Some reports indicate that additional militants under Mansur Achakzai, Amir Lalai and Sarkateb continued resistance into the final two days of fighting.

10. Davis, 54. The PDPA was the communist regime that ruled in Afghanistan from 1978 to 1992. Given that the allegation was made by one of the Taliban's adversaries, Hekmatyar, the number is likely exaggerated. However, even if inflated, the report still highlights the extent of Taliban influence in former military networks.

11. For background information about warlordism and the political landscape in Kandahar, see Antonio Giustozzi and Noor Ullah, ""Tribes" and Warlords in Southern Afghanistan, 1980-2005," *LSE Crisis States Research Center*, September 2006.

12. Abdulkader H. Sinno, *Organizations at War in Afghanistan and Beyond* (Ithaca: Cornell University Press, 2008), 240-1.

13. Abdulkader H. Sinno, "The Taliban's Ability to Mobilize the Pashtuns," *The Taliban and the Crisis of Afghanistan* (Cambridge: Harvard University Press, 2008), 79-82.

14. Drawn loosely from various sources, including: Mohammad Osman Tariq Elias, "The Resurgence of the Taliban in Kabul: Logar and Wardak;" *Decoding the New Taliban: Insights from the Afghan Field*, edited by Antonio Giuztozzi,51; Pravin Rajan, "Networks of Faith and Community: The Taliban and Political Mobilization in Contemporary 'AfPak," unpublished paper, and Sinno, *Organizations at War in Afghanistan and Beyond.*

15. Anthony Hyman, "Nationalism in Afghanistan," *International Journal of Middle East Studies* 34 (2002): 299-300.

16. David B. Edwards, *Before Taliban: Genealogies of the Afghan Jihad* (Berkeley: University of California Press, 2002).

17. Sinno, *Organizations at War in Afghanistan and Beyond*, 242-3.

18. Ahmed Rashid, "Pakistan and the Taliban," *Fundamentalism Reborn: Afghanistan and the Taliban.*

19. Davis, 49-50. Reports from the battle describe a plethora of grease paper left "everywhere as the madrassa students removed the new weapons from their wrappings."

20. Ibid, 49.

21. Michael Semple, *Reconciliation in Afghanistan* (Washington, D.C.: U.S. Institute of Peace Press, 2009), 3.

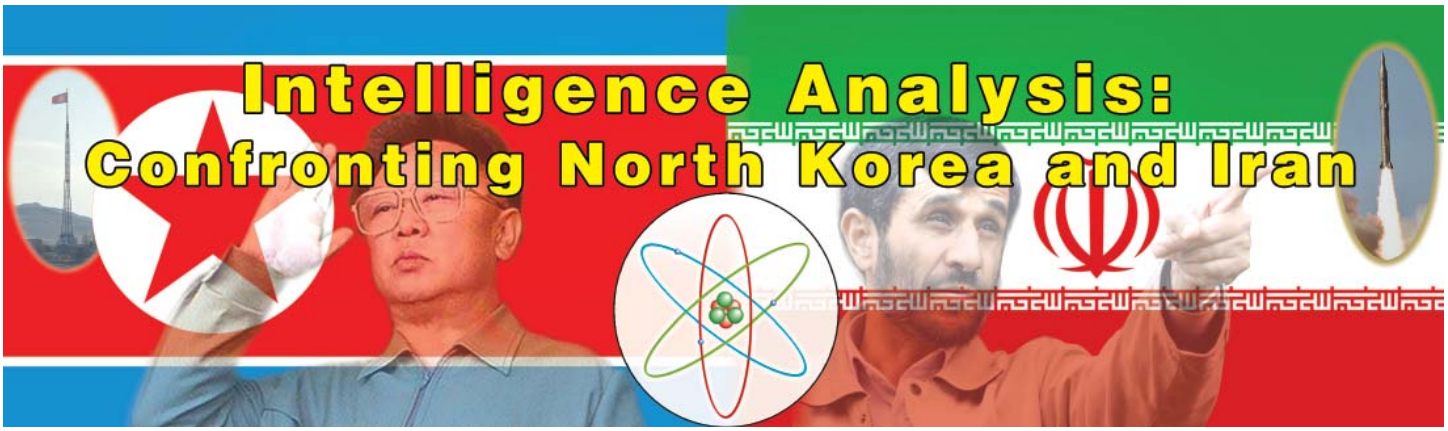
22. See Samuel Chan, "Sentinels of Afghan Democracy: The Afghan National Army," *Military Review,* January-February 2009 and Antonio Giustozzi, "Afghanistan's National Army: The Ambiguous Prospects of Afghanization," *Terrorism Monitor* Vol. 6, Issue 9, May 2008.

23. Semple, 46-7.

24. Michael T. Flynn, Matt Pottinger and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington: Center for New American Security, January 2010).

First Lieutenant Tyler Jost is a Military Intelligence officer with 1st Brigade, 101st Airborne Division. He holds a BS from the U.S. Military Academy at West Point and an MA from the School of Oriental and African Studies at the University of London. He can be contacted at tyler.jost@us.army.mil.

The order creating the Army Intelligence and Security branch is signed by Army Chief of Staff Gen. George H. Decker on 1 July 1962. The Assistant Chief of Staff for Intelligence, Maj. Gen. Alva Fitch, is at the far left



by Robert J. Leach

In the U.S., intelligence analysis enables policy makers to make informed decisions that reverberate globally. This article explores two major challenges facing analysts over the next twelve months that will influence U.S. policy for many years to come. The first challenge is the question of what North Korea will do given its self-declared nuclear capability. The second question revolves around Iran's nuclear capability.

North Korea has declared its nuclear capability. The intentions of the declaration remain a mystery to most analysts and government organizations alike. North Korea, arguably the most reclusive nation in the world, remains in the headlines of news organizations around the world. Even China, its greatest ally, seems to be at a loss on the recent escalation of nuclear rhetoric displayed by North Korea. Historically, when North Korea behaved in a manner unbecoming of a nation, they sought concessions. Policy makers previously rewarded deliberate and hostile North Korean behaviors with energy and other nation stabilizers (i.e., food supplies and commerce.) Perhaps the concessionary negotiations of the previous policies with North Korea allowed it to formulate a standard behavior in order to achieve a desired result.

It is possible that the U.S. currently faces nuclear rhetoric, testing, and possible proliferation by North Korea as a direct result of a standard practice of quid pro quo. Analysts focused on current behaviors must look at previous activities and rewards to understand possible goals of the current escalation of hostilities on the Korean Peninsula. In 2002, North Korea faced severe energy and food shortages. It responded to the labeling as a member of the "Axis of Evil" by President Bush with predictable hostility.[1] The expected reaction, based upon previous acts of aggression, led North Korea to admit: "to U.S. officials that it was pursuing a highly enriched uranium program in violation of several international agreements, including the 1994 Agreed Framework signed with the Clinton administration."[2] Through the Six-Party Talks, which involve the U.S., North Korea, South Korea, Japan, China, and Russia, North Korea agreed to disband its nuclear pursuits in exchange for energy resources and also received further commitments from South Korea for foodstuffs and cooperation with building the "Kaesong Industrial Complex just north of the demilitarized zone."[3]

The South Korean equation limits military action against North Korea by the U.S. Any U.S. military response would likely cause North Korea to unleash a wave of military counter-responses, which would cripple South Korea. Protection of South Korean and Japanese economies is vital in any response by the U.S. or any U.S. ally. North Korea understands the vital role played by the economies of South Korea and Japan in measured responses by the U.S. and its allies. Based on decades of tit-for-tat exchanges of rhetoric and sanctions, North Korea plays a chess game one move ahead of U.S. policy. The North Korean advantage stems partly from regime and policy changes on the part of the U.S. However, the isolated nature of North Korea plays an additional role in staying one step ahead of American predictive analysis of reactions by party leaders in Pyongyang.

Kim Jong-Il's recent health concerns brings into question who has really been in charge of North

Korea. Information released by party leaders in Pyongyang spin the truth right out of the story broadcasted by the Korean Central News Agency (KCNA). Party leaders, especially Kim Jong-Il, must represent a strengthened party at all costs. At times, the KCNA released digitally altered pictures of Kim Jong-Il in order to create an illusion of a healthy leader. An example of this occurred in 2008, when rumors speculating that the North Korean leader had a stroke.[4] The KCNA released a picture that Kim Jong-Il had supposedly taken with military members in order to quash speculation concerning the health of the North Korean "Dear Leader."[5] The picture showed shadows behind Kim Jong-Il that were at a different angle than the shadows of the soldiers around him, proving that the picture was a fake.

Analysts may deduct that the current round of rhetoric is in support of Kim Jong-Il's third son, Kim Jong-un.[6] Kim Jong-un is reportedly in line to succeed Kim Jong-Il as the leader of North Korea. Kim Jong-Il may want to put an increased amount of pressure on the international community prior to his death in order to set his son up for success. This is viewed from the perspective typical of many familial patterns of love and succession. Kim Jong-Il may feel that the increased pressure and nuclear rhetoric might bring about greater concessions to North Korea. This gift to his son would put him in great light in the eyes of the people. This logic may seem too risky for Westerners; however, when dealing with the instability of an ailing leader, this scenario becomes plausible. Having a new leader bring great fortunes to his country may give the appearance that the new leader is in charge and self-reliant.

Self-reliance, or *Juche*, is the key leadership principle or ideology that guides many awkward maneuvers by North Korea.[7] North Korea relies on China for many staples to keep the nation running. If North Korea created a hasty and deplorable venue to display their seemingly unstable might, perhaps the concessions drawn could reduce the amount of support required of China. These concessions could give the appearance of self-reliance to the people, and suppress any instability as the result of a regime change within North Korea. Another way to gain self-reliance is with the sale of military equipment and technologies to a paying customer.

Weapons and weapons related technology are the main goods that North Korea exports. Consumers range from possible terrorist organizations to countries like Yemen, Iran, and Syria. In 2002, the U.S. along with the Spanish Navy intercepted a cargo ship bound for Yemen loaded with twelve disassembled SCUD missiles.[8] Even though the sale of these missiles turned out to be within international legal guidelines, it brought to light the proliferation of military weapon systems from North Korea to other nations. Assurances by Yemen allowed for the continuation of the shipment, as it made a guarantee of sorts to the U.S. that the missiles would not end up in the hands of terrorists.[9] In 2007, North Korean technology proliferation reared its head again in Syria.

Syria secretly built a nuclear reactor at Al Kibar that included specific technical help and assistance from North Korea. In September 2007, Israel bombed this site, amidst speculation that the site included a nuclear reactor similar in size, dimension, and features to the nuclear plant in Yongbyong, North Korea.[10] Supposedly, a video shared with members of Congress showing North Koreans in the Syrian

plant, gave concrete evidence to these lawmakers of North Korean nuclear proliferation.[11] Sharing this technology with Syria likely brought a significant amount of financial support to the reclusive regime in North Korea.

The current show of nuclear capabilities by North Korea could include a capability demonstration to potential customers. A North Korean sale of a nuclear weapon to a terrorist organization like Al Qaeda, Hezbollah, or Hamas would serve many purposes. A condition of a sale might include conducting a detonation on U.S. soil, or at least against a large U.S. military population such as in Iraq or Afghanistan. The sale would generate both revenue for North Korea, and achieve a military victory against the U.S. The revenue gained would enable North Korea to purchase both commodities and military related equipment. The commodities would give stability to the nation and satisfy Juche ideology. A military victory in a war of proxy against the U.S. would cleanse North Korean hands of allegations of wrongdoing, and keep the U.S. military on its heels. With the U.S. military reeling from a possible significant loss, the North Koreans could capitalize on this event and launch a preemptive strike against South Korea. A unified Korean Peninsula under the rule of North Korea has been a long-standing goal of the isolated nation. Key indicators should allow analysts to determine intentions by North Korea.

Analysts must take a holistic look at the entirety of the North Korean military in order to determine possible aggressive intentions from this rogue nation. A North Korean military conflict would be precipitated by movements of large units and pieces of equipment from storage areas to areas of anticipated engagement. Indications and Warning would allow only limited time for reaction. However, the movement of such large forces would take time in order to be prepared for engagement. Understanding non-typical military movements is paramount to the warning of potential direct military conflict with North Korea. Proliferation of technology and weapons from North Korea to Iran are predictable and understandable from this perspective.

Many weapons, especially missile technology in the Iranian inventory seems to replicate North Korean missile systems. As the other remaining "Axis of Evil," it would only make sense that the foes of the U.S. unite and share information, technology, and equipment in order to defeat the common enemy. The commonality between the two nations stems from purchasing technology and information from Abdul Qadeer Khan.[12] A. Q. Khan, a renowned Pakistani with expertise in nuclear energy and weapons, purportedly sold centrifuge technology to North Korea and Iran before his capture.[13] Iran is likely paying great attention to western reactions to North Korea's nuclear declaration and testing.

Iran's policy to the U.S., Israel, and the rest of the world will take shape as world reactions to North Korea's nuclear ambitions evolve. Confronting Iran is difficult given the significant U.S. military presence in the Middle East. Analysts must determine whether the intention of Iran is to build peaceful nuclear energy or a nuclear weapons capability. Given the limited resources, information from within the withdrawn nation makes analysis difficult. The miscalculated analysis of the presence of weapons of mass destruction in Iraq prior to military conflict in 2003, may lead analysts to refuse to make a concrete determination on the capabilities of the Iranian nuclear program. This bias could place the security of the Middle East in jeopardy.

If the U.S. does not engage Iran prior to a declared nuclear weapons capability, then it is forced to deal with the aftermath of a nuclear weapons capable Iran. U.S. policy towards Iran would likely change in the advent of austere changes in Iran's nuclear capabilities. In the event that Iran is simply interested in peaceful nuclear energy, and the U.S. attacked Iran, the world would hold the U.S. directly responsible for the aggression. A miscalculated judgment could cost the U.S. insurmountable losses in the financial sector, a loss of authority within the world, and create retaliations by Iran against the U.S. with the gravest conditions. This burden on analysts creates a bias that unless gotten rid of makes the right decision by policymakers nothing short of questionable.

The analyst's job is not to influence policy. The analyst's job is to inform policymakers on events and potential courses of action by the enemy. In-depth analysis utilizing the political, economic, military, social, infrastructure and information factors enable analysts to take into consideration multiple aspects when drawing conclusions. Competing hy-

potheses allow analysts to think of other potential results without bias in order to inform the policy-maker on threat courses of action.

An additional factor to take into consideration is Israel. Iran has vowed to destroy Israel. Israel's nationhood is potentially in jeopardy given an Iran armed with a nuclear weapon. The U.S. has a covenant with Israel to protect its existence. Analysts must determine possible repercussions of an Israeli preemptive strike against Iran. Additionally, Iran is known to be a state sponsor of terrorism to Hezbollah and Hamas. Iran also supports Syria with weapons, technology, and additional considerations.

Any attack on Iran could unleash terrorist organizations kept in reasonable reserve recently, or, in the case of Hamas, at least since the end of "Cast Lead." This period of relative calm has enabled these organizations to rearm and rethink attack scenarios against Israel. With the support of Iran, Hezbollah likely upgraded its military capabilities since the end of the 2006 conflict. With the help of North Korea, the potential exists that Iran could already be in possession of a nuclear device. If such a device were transferred to either Hezbollah or Hamas, with deliberate instructions for use given a preemptive strike by Israel against Iran, then the possession of such a device by terrorist organizations could throw the world into global chaos.

The need for additional consideration due to the possibility of Iran closing the Strait of Hormuz resonates throughout the intelligence community. According to one news outlet, "between 15 and 16.5 million barrels of oil transit the Strait of Hormuz each day, roughly 20 percent of the world's daily oil production."[14] Iran may attempt to close the Strait if attacked. This closure would severely disrupt the flow of oil to world markets. This could cause global inflation never before seen. In fact, the likelihood of global chaos could include a breakdown of life saving services in many areas. Analysts should watch the movement of mine laying equipment near the Strait of Hormuz in order to complete their predictive analysis.

Based on previous Israeli strikes against Iraq under "Operation Opera" in 1981, and the attack against Al Kibar, predictive analysis should lead analysts to believe that Israel will not allow for a nuclear-armed Iran.[15] In fact, Israel has already conducted much of the preparations needed in order to conduct a preemptive attack against Iran. In June 2008, Israel conducted an air exercise that mimicked the same distance from Israel to the uranium enrichment plant in Natanz, Iran. During this exercise, over 100 aircraft conducted what many analysts view as a prelude to an inevitable attack on Iran.

The U.S. presence in Iraq creates a unique strain on Israeli attack planning. The U.S. controls most of the air space over Iraq; any Israeli strike against Iran would include the need to fly through space controlled by the U.S. Questions loom over how the U.S. would react to a surprise maneuver by Israeli Air Forces to strike Iran without approval by the U.S. to utilize Iraqi air space. Alternatives from flying over Iraq are not realistic. Interestingly, Israel has a history of militarily engaging the U.S. in a hostile manner when the need for security dictates such intervention.

In 1967, during the Six Day War, Israel engaged the USS Liberty, which led to 34 Americans killed, and wounding more than 170.[16] At the time, the USS Liberty was an information-gathering vessel located off the coast of Israel in the Mediterranean Sea. Although many believed the attack was intentional, "Israel has maintained since the attack that

it was a case of mistaken identity, an explanation the Johnson administration did not challenge formally."[17] Even if the U.S. did not inform Israel of the presence of this American vessel, Israel supposedly did not take the necessary steps to rule out the vessel was American. The precedence of this historic event must make analysts calculate to what degree Israel might be willing to attack Iran without U.S. approval or possible notification. The analytical process must include "out of the box" thinking to evaluate a potential Israeli no notification strike against Iran.

The analytical process requires a "red cell" thought process in order to be unique and thorough. A military analyst must formulate conclusions about potential enemy or even friendly scenarios that achieve their goals and objectives. The thought process must begin with: "If I were the leader of this organization or country, what would I do to defeat my enemy?" The analyst must take into consideration many cultural aspects along with a historical perspective to evaluate an enemy using "red cell" thinking. Although challenging, it gives great insight into the mind of an adversary with a unique spin. If performed properly, predictive analysis becomes an easier task.

As the next twelve months evolve, the two remaining "Axis of Evil" countries will continue to be in the headlines, and to draw the attention of persons globally. Understanding the ambitions of these countries to achieve a nuclear capability deserves great caution and understanding by the intelligence community. Predicting behaviors, as radical as they may seem, is paramount to national security interests for the U.S. The potential for these rogue nations to transfer a nuclear weapon to a terrorist organization to undermine world peace efforts is reaching a critical stage. Defeating the plausibility of this scenario falls to the hands of analysts with the ability to think unconventionally.

Endnotes

1. Glenn Kessler and Peter Baker, "Bush's 'Axis of Evil' Comes Back to Haunt United States," *The Washington Post,* 10 October 2006, retrieved at www.washingtonpost.com/wp-dyn/content/article/2006/10/09/AR200-6100901130.html.

2. Balbina Y. Hwang, "Don't Make Concessions To North Korea," *The Heritage Foundation*, 25 February 2004, retrieved at http://www.heritage.org/Press/Commentary/ed022504a.cfm.

3. Wonhyuk Lim, "*Inter-Korean Economic Cooperation at a Crossroads*," Korea Development Institute, December 2006, retrieved at http://www.nautilus.org/fora/security/07008Lim.pdf 2.

4. Nico Hines, "Kim Jong Il Photoshop Error Betrays Leader's Health Problems?", *The Huffington Post*, 6 November 2008, retrieved at http://www.huffingtonpost.com/2008/11/06/kim-jong-il-photoshop-err_n_141927.html?show_comment_id=17767070.

5. Ibid.

6. Kim Sue-Young and Michael Ha, "Kim Jong-il's 3rd Son Emerges as Successor," *Korea Times*, 15 January 2009, retrieved at http://www.koreatimes.co.kr/www/news/nation/2009/02/117_37961.html.

7. Global Security, "Juche [Self-Reliance or Self-Dependence?]", 2009, retrieved at http://www.globalsecurity.org/military/world/dprk/juche.htm.

8. Thomas E. Ricks and Peter Slevin, "Intercepted Missile Shipment Released to Yemen," *The Washington Post,* 11 December 2002, retrieved at http://www.washingtonpost.com/ac2/wp-dyn/A39775-2002Dec11?language=printer.

9. Ibid.

10. Robin N. Wright, "Korea linked to Syrian nuclear plant," *The Washington Post*, 28 April 2008, retrieved at http://www.boston.com/news/world/asia/articles/2008/04/24/n_korea_linked_to_syrian_nuclear_plant/.

11. Ibid.

12. Gerald M. Steinberg, "North Korea and Iran: Will Any Lessons Be Learned?", *Jerusalem Center for Public Affairs*, 11 October 2006, retrieved at http://www.jcpa.org/brief/brief006-12.

13. Ibid.

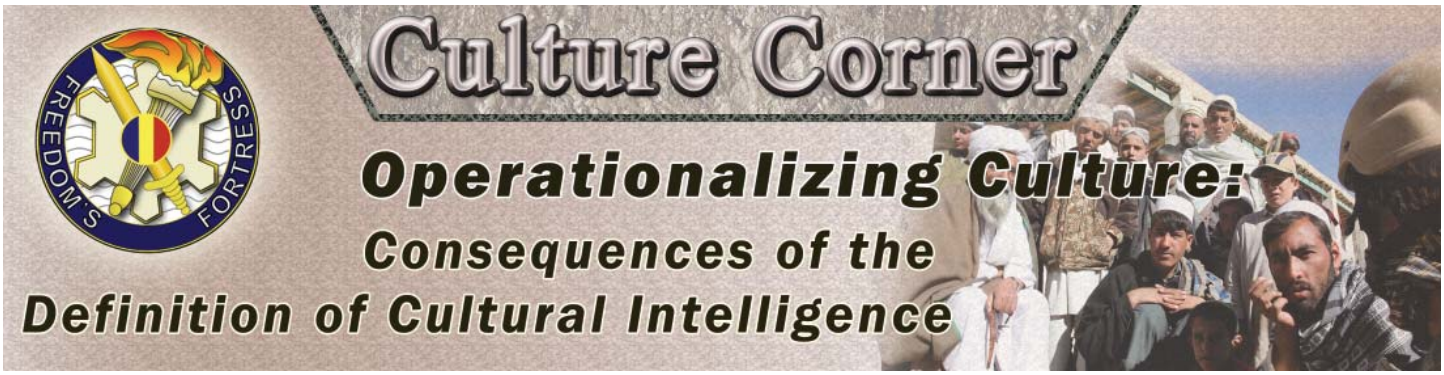
14. Kenneth R. Timmerman, "Iran Readies Plan to Close Strait of Hormuz," *NewsMax.com*, 1 March 2006, retrieved at http://archive.newsmax.com/archives/articles/2006/2/28/181730.shtml?s=lh.

15. Avi Hein, "The Raid on the Osirak Nuclear Reactor", J*ewish Virtual Library,* 2003, retrieved at http://www.jewishvirtuallibrary.org/jsource/History/osirak1.html.

16. Israel B. Schweid, "US faulted in 1967 attack: But conclusions don't satisfy some", *Associated Press*, 13 January 2004, retrieved at http://www.boston.com/news/nation/articles/2004/01/13/israel_us_faulted_in_1967_attack/.

17. Ibid.

Robert Leach is a retired Intelligence Analyst and now teaches at the Intelligence Analyst Course at Fort Huachuca, Arizona. He spent his career as an analyst at various tactical and strategic assignments around the world. Mr. Leach holds an MA in the Administration of Justice and Security through the University of Phoenix, and recently completed Lean Six Sigma and Project Management certification through Villanova University. While in the Army, he completed the DIA Indications and Warning Course as well as the Joint Intelligence Analyst Course.



by Hugh M. Lewis, PhD

All intelligence is anthropological intelligence, no matter what forms it may take. Intelligence is anthropological because it defines what it means to be human, how we organize our worlds, and the forms and style-patterns that human civilizations take. Our intelligence is of such a nature that it is unfinished business. We do not see the world or things in it so much for what they are, but for what they seem to mean to us. This is especially so when what we see is ambiguous and uncertain in form—it is the nature of our intelligence to automatically superimpose form and function upon what is otherwise confused and unclear.

Human intelligence was born with the capacity to deliberately deceive, exaggerate, tell half-truths and prevaricate, and to also apperceptively recognize when one is being deceived by imagining the possibilities of truth behind the deception. It is the veil of culture that stands between our intelligence and the hidden realities of the world, permitting both possibilities of deception and enlightenment.

What we anthropologically call culture underlies and contextualizes all of our intelligence. We are culturally dependent creatures of intelligence because without culture to predefine the form of what we see and how we see it in the world, to provide common reference points, our intelligence would be simple irrationality and insanity. This cultural process works mostly upon an unconscious level in our daily lives as well as in the larger human world, necessarily so, because the more we fly by habit and training, the less we fly by the proverbial seats of our pants.

There have been many anthropological definitions of culture. The multiplication of definitions of culture tells us that the science of culture is far from unified, and its primary object of study remains far from being clearly or completely understood. It matters most that the definition we adopt for culture has inevitable consequences in how we think about things cultural, and for what we consider to be important to cultural understanding or otherwise. Our definitions of culture preclude how we operationalize our methods and methodologies in acquiring cultural intelligence, and in how we apply our culturally-based knowledge and understanding to the world.

What is critical to our understanding of culture is the recognition that whatever formal or practical definitions of culture we may adopt, processes of global culture currently impact upon multiple levels, and the contemporary cultural realities we are dealing with daily in our world are changing continuously, chaotically, often indirectly, and at increasing rates. Culture in our world is itself changing, and the traditional and conventional boundaries that defined our cultures and our knowledge of culture by which we were raised and educated are breaking down in the face of the digitial information revolution and technological development, by which cultural values and variables, always soft in their human undercurrents, always hard in their final consequences, are being transmitted and broadcast instantaneously around the entire world at accelerated rates.

These globalizing influences of modern human civilization create a transnational parallax, a shift of realities of collective consciousness vis-à-vis one another. They determine how we adapt to the world and challenge all of us with a fundamental sense of discrepancy in how we see and respond to the demands of the world. This process is called trans-

culturation, and one of its consequences is the transmission and development of global culture, or what can be called human civilization writ large upon the earth, for technology knows no cultural boundaries, but breaks these boundaries down through processes of cross-cultural influence, cultural erosion, trans-cultural tectonics, and non-linear patterns of transformational development.

A central challenge in the operationalization of definitions of culture has been the fact that all people are themselves bound not just by a stratified set of cultural realities, but by our universal cultural dependency upon its larger collective realities in shaping both our world and how we see that world. Scientifically, in the objective definition of culture, it becomes the case that if indeed culture shapes how and what we know of our world in basic ways, then we must confront the anthropological relativity of human intelligence, and the fundamental dilemma of not only our bounded knowledge of culture, but of our very capacity to know and understand any or all culture in a completely disembodied and non-subjective manner.

How do we operationalize the definition of human culture, or its cultural intelligence, rapidly transforming itself and our world, in a manner that will be of service to the military in the future? Each branch of the U.S. military has its own definition of culture, sometimes more than one, and each serves critically, well or otherwise, how that branch approaches the problem of culture in its training, doctrine and operational application. In a critical sense as well, how we finally come to agreement in the operational definition of culture will play critically in serving to define the role played by the U.S. military in future global politics of conflict, resource competition and the inevitable human struggle for power and freedom. This role will become increasingly acute in the face of Malthusian realities as the global human population swells to carrying capacity, as energy demand outstrips energy supply, as food prices rise around the world and attendant environmental degradation and circumscription continues inexorably and unabated to make food less and less available to more and more people.

The operational definition of culture hinges critically upon differentials of sharing of human patterns of response that result in coexistence and competition of alternative collective and corporate social realities. Shared patterns of response upon multiple levels of being and social interaction provide consonance and coordination for our behavior in relation to the world, and these patterns, internalized since early childhood, become sanctioned and constrained through secondary institutions and formally embedded and reinforced within a common stock of knowledge, conventions of collective representation, and a shared, received symbology of meaning about the world, or "world view." The integration of our reality, both behaviorally and symbolically, upon multiple psychological and social levels, depends fundamentally upon this process of institutionalized sharing of common knowledge and associated native cultural intuitions.

Behind this definition looms the question of "what is human intelligence" and, in the structure of the large and the long run, how can collective human intelligence (civilization) be best served and serve through military endeavor and dedicated service. Old models of culture, whether our own or others, whether of law, or morality, of economy or politics, do not necessarily serve well new transnational situations and patterns of globalized culture. We are all struggling to catch up to the globalization of cultural human realities, and all that we knew or have known before becomes subsumed under a new aegis of globalized realities and alternative transnational possibilities.

Human intelligence permits us to see the changing world, and ourselves in relation to the changes of the world, in ways we would not have otherwise or previously seen, and hence by so seeing, to adapt to that changed world in a manner that serves our best long term interests. It permits us the freedom to act outside of the constraints of received, tradition-bound culture, and provides us the operational edge over those who cannot escape the boundaries of their own cultural boxes. We may never be able to ultimately escape the consequences of the cultural realities of our own making, but we can seek to shape those consequences in a manner that serves our greater mutual long term interests in the world.

Cross Cultural Negotiations: Skill Building in an Operational Environment

by Mahir J. Ibrahimov, PhD

This article previously appeared in the May-June 2011 issue of Fires.

Introduction

The U.S. Army's Culture and Foreign Language Strategy states that operational experiences in Somalia, the Balkans, Afghanistan, and Iraq have highlighted critical gaps in the Army's capability to influence and operate effectively within different cultures for extended periods of time. Battlefield lessons learned have demonstrated that language proficiency and understanding of foreign culture are vital enablers for full spectrum operations.

Negotiating in indigenous cultures adds new dimensions to the military's missions in Afghanistan, Iraq, and elsewhere. Operating in joint interagency, intergovernmental, multinational environments requires a new, more sophisticated set of skills that are very different than the traditional warfighting in a bipolar strategic environment of the Cold War era.

This new dimension is essential for winning hearts and minds of the populace of regions and countries which are of strategic importance to the U.S. and its allies. In this article we will consider the cultural considerations in negotiations and the factors which influence them in indigenous operating environment.

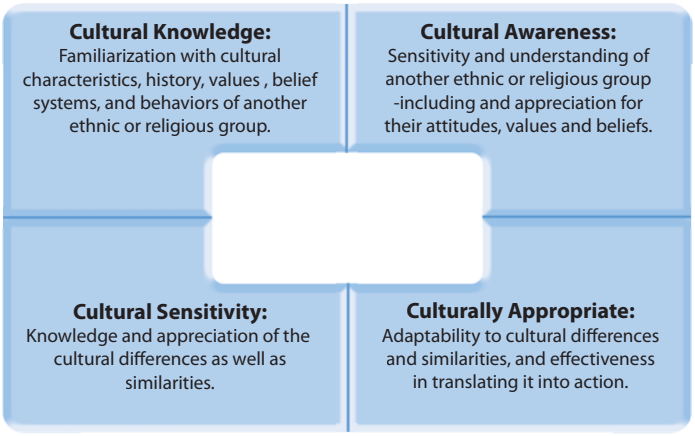
What is Negotiation?

Negotiation is derived from the Latin word *"negotiari."* The root words *neg* (not) and *otium* (ease or leisure) together mean "not leisure," reflecting the uneasy nature of negotiations. Negotiation is a process in which two or more participants try to come to a mutual consensus through a process of interaction and communication by using different negotiation techniques and methods. There are five main elements of international negotiation:

- The players and the situation.
- The style of decision making.
- National characters.
- Cross cultural aspect.
- Interpreters and translators.

What We Need to Know about Culture

Culture (from Latin "cultura" to cultivate) is a combination of behavior patterns, arts, beliefs, and institutions passed down from generation to generation. It's the way of life for an entire society. It includes codes of manners, dress, language, religion, and rituals. There are other cultural definitions that leaders need to be aware of when preparing for negotiations, these include cultural knowledge, cultural awareness, cultural sensitivity, and cultural appropriateness.



Three Phases of Negotiation

Generally, negotiations consist of three phases. Phase I is the pre-negotiation phase. This is often the most critical phase. Each party identifies its strengths, assesses its interests, and works to find a balance between short term tactical gains and long-term strategic relationships. Phase II consists

of the actual negotiation process, and Phase III consists of post-negotiation efforts.

Phase I: Pre-negotiation. Just knowing definitions isn't enough; there are also several things that must be done prior to engaging in negotiations. They include learning as much as possible about the negotiating partners. This means knowing the players, their tribal affiliation, and their political and religious agenda. Leaders must also identify the initiator of the meeting. If the negotiation request comes from a local key or influential leader, it is imperative to identify their socio-economic, political, ethnic or tribal affiliation. Leaders must also determine an appropriate location for the meeting. If hosting, choose a quiet, private location away from possible internal and external distractions.

Finally, leaders must identify an appropriate translator. Choosing the right translator is very important. If they are local, they might have a biased agenda, tribal affiliation, or certain linguistic dialect which might not be well perceived by another negotiating party. Make sure beforehand if a female translator is appropriate, especially for high level negotiation. It is imperative that a translator be knowledgeable of languages and cultures to avoid possible misinterpretations, especially when it comes to proverbs, idioms, etc. and other cultural nuances. Misinterpretations might negatively affect the outcome of the negotiations. Lessons learned have shown that the very lack of cultural knowledge, education, and exposure usually leads to misinterpretations.

My experiences throughout the years in different cultural settings point to that pattern. For example, during a negotiation a Middle Eastern delegation member used the following Arabic proverb, *"min kasratil mallahin gariqat as safina."* During the discussion, the interpreter literally translated the meaning as, "there were too many sailors on the boat and it sank," when in reality it should have been translated as "too many cooks in the kitchen." Because the interpreter did not have a clear sense of the Western cultural realities, he could not translate the nuances of one culture into another.

Another example where literal translations can cause confusion comes from past negotiations between Western oil companies in the former Soviet Republic of Azerbaijan. An Azeri member of the delegation used the popular Turkic proverb or idiom, *"manim gozum sandan su ichmir,"* which actually means, "I am suspicious of you" or "I do not trust you." The interpreter on the scene translated the proverb literally to mean, "My eye does not drink water from you."

In another incident which took place in Moscow in the 1980s, a Russian negotiator used a very popular, old Russian traditional saying, *"vipyem na pososhok,"* while addressing the departing Western delegation. This saying is usually used by Russians to wish each other "safe travel." Once said, everyone would normally sit for a moment, raise their glasses of vodka, drink, and wish everyone a safe trip. However, this phrase is very difficult to translate word for word. The interpreter struggled and could not give an English equivalent. Because the meaning was not clear, the Western delegation was not entirely sure of what was actually said.

In all three cases, the culturally and linguistically incorrect translations caused major confusion and even laughter and were not obviously helpful for the outcome of the negotiations. These experiences show misinterpretations, either deliberate or because of ignorance of cultural, linguistic, political, ethnic or tribal affiliations, can cause miscommunication.

Cross-cultural negotiation training is an important element of the pre-negotiation phase. Negotiators must understand cultural etiquettes as well as cross cultural differences in negotiation styles and techniques when dealing with a Middle Eastern partner. In a cross-cultural setting all leaders need to consider cultural factors impacting the negotiation process, which can include different historical, ethnic and cultural backgrounds, possible emotional perceptions, political systems, and their socio-cultural origins.

Phase II: Negotiation. During this phase your cross-cultural training is no less important. Some cultures adopt direct, simple methods of communication, while others prefer indirect, more complex methods. Middle Eastern cultures fall into the latter category. When communicating with Arabs, pay attention to body language, eye movement and hand gestures. Any negotiation should begin with greetings.

In the Middle East, negotiators usually prefer longer, less formal sessions, insist on addressing counterparts by their titles, and are given to expressing

philosophical statements that are often more important to the negotiation process than the technical issues of the problem. In an indigenous culture it is extremely important to be culturally sensitive and to show your respect and understanding of the culture of the negotiating partner.

When communicating with Arabs, pay attention to body language, eye movements, and hand gestures. The knowledge of the following basics can be helpful:

- Shake hands with the right hand and use the left hand to grasp the other person's elbow as a sign of respect.
- In close, friendly relationship, a hug and a kiss placed on both cheeks upon greeting are a normal occurrence–if the Arab initiates it.
- Placing a hand on the heart with a slight bow is a sign of respect while greeting a person.
- If a Middle Easterner touches you it is a positive sign, it means that he likes you (not a sign of homosexuality.)
- Rise to show respect when a respected or elderly person enters the room.
- You will be on the safer side if you always rise while greeting people.
- Usage of common Arab greetings, however few, such as "*As Salam Aleykum*," or "Peace be with you" accompanied with or instead of "hello" are very much appreciated. See Figure 1.

Gesture	Meaning
Palm of the right hand on the chest, bowing the head a little and closing one's eyes.	Thank You.
A quick snap of the head upwards with an accompanying click of the tongue.	No.
Placing the right hand or its forefinger on the tip of the nose.	It's in my head to accomplish.
Grasping the chin with the thumb side of the right fist is a sign of wisdom.	I am thinking.
Holding fingers in a pear shaped configuration with the tips pointing up moving the hand up and down.	Wait a little bit.
Right hand out, palm down, with fingers brought toward oneself in a clawing motion.	Calling someone to come.

Figure 1: Appropriate Gestures and Body Language.

Other "Do's" and "Don'ts" cultural basics during the negotiation process are extremely helpful as well. See Figure 2.

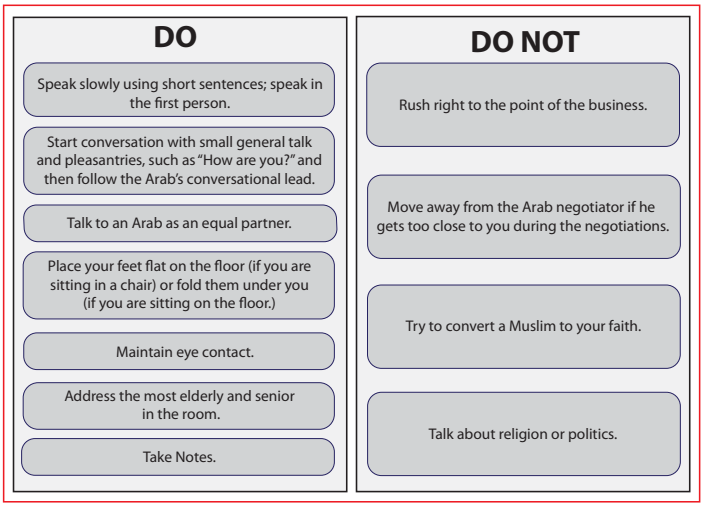


Figure 2: Basic Do's and Don'ts during the negotiation process.

Each culture also has contrasting views of negotiating. Gaining an appreciation for the contrasting views is vital. Goals reflect the purpose or intent of the parties in a negotiation. In business, American negotiators typically regard the signing of a contract between the differing parties as their primary goal. They consider the contract a binding agreement that outlines the roles, rights, and obligations of each party. Americans prefer detailed contracts that anticipate all possible circumstances. These agreements or contracts are usually binding and not subject to further negotiation or debate. This is known as the "Western Tradition of Legalism."

However, Middle Eastern negotiators tend to begin negotiations by establishing general principles that become the framework on which to build an agreement. They usually seek sustainable relationships rather than contracts and "prefer to leave things vague." This is known as the "Middle Eastern Relationship of Trust." Middle Easterners prefer an agreement in the form of general principles rather than detailed rules. They regard an agreement as being relatively flexible and symbolic of the relationship established, rather than a binding legal document.

A Western negotiating team typically organizes itself using a deductive process. Essentially, the group will organize in culturally specific ways that reflect and affect how the group makes decisions. A negotiating team usually will have a designated

leader who appears to have complete authority to decide all matters. See Figure 3.

American	Middle Eastern
Timetables and schedules are important.	Unbound by time for negotiating.
Get down to business quickly.	Exchange pleasantries at great length.
Avoid silent intervals.	Employ silent intervals.
Tend to focus on future.	Tend to focus on past.
Contractual agreements.	Value well-established relationships of trust.
Favor quick decisions and avoid slow deliberation.	Favor consensus-based decision making.

Figure 3. Contrasting viewpoints, American vs. Middle Eastern.

An Arab negotiating team typically uses the inductive process. In the Middle East, a hidden authority rests with the group, and decision making often occurs through consensus. Thus, negotiating teams may be relatively large due to the greater number of personnel thought to be necessary to the decision making process.

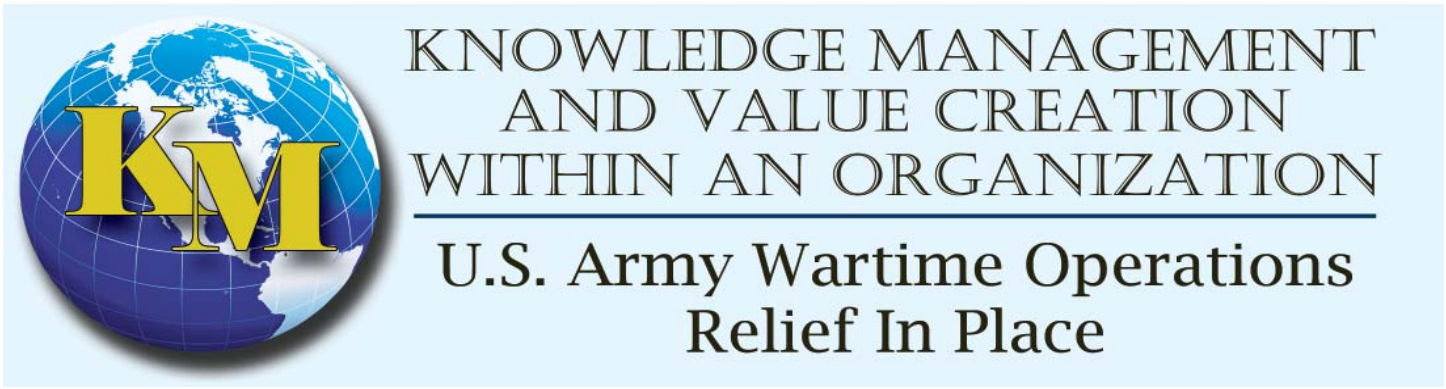
In Arab and Middle Eastern cultures, 'saving face' is strategically important. Face has to do with a person's reputation and the respect in which others hold him. In negotiation, although compromises are reached, they must be done in a manner that allows the Arab partner to maintain dignity or prestige and not appear weak. To an American, losing face may be embarrassing, but to an Arab, it is devastating. Losing face is the ultimate disgrace, and an Arab will go to almost any length to avoid it. U.S. leaders must keep the concept of "face" in mind when conducting negotiations in the Middle East. Failure to do so could freeze or kill a negotiation. Face and the allied concepts of honor and shame are important in the Middle East.

There are other aspects of culture to consider with respect to negotiations. Some cultures are more risk-averse than others. In general, Middle Easterners seek to avoid uncertainty. This proclivity affects their willingness to take risks in a negotiation. Different cultures also have different views about the appropriateness of displaying emotions. Arab negotiators, in a high-context culture, are more likely to display emotions than Americans. However, in Afghanistan, specifically in the Pashto culture, displays of emotion such as impatience, anger, etc. are considered signs of weakness. Finally, in addition to attaching high importance to creating bonds of friendship and trust between negotiators, Arabs believe it is imperative that negotiating partners respect each other's honor and dignity.

Phase III: Post-negotiation. End negotiations with a strong stance. Once objectives have been achieved, summarize what has been agreed to and confirm the key points. Do not allow the negotiating partners to do so, this places them in power. Use common courtesy and tact in an effort to not offend the partners. Try not to rush or push; it might postpone or kill the agreement. It's important to maintain control of the negotiation throughout the entire process, including the closing.

Negotiating is a way of life in Arab cultures. Apply these cultural and negotiation strategies and any mission will reap the benefits.

Mahir J. Ibrahimov is the U.S. Army's Senior Cultural and Foreign Language Advisor at Fort Leavenworth, Kansas. He was the first TRADOC Culture and Foreign Language Advisor at Fort Sill from 2009 to 2011. Dr. Ibrahimov completed his PhD at the Academy of Social Sciences in Moscow in 1991 and has attended several post graduate programs at Johns Hopkins University and other U.S. institutions. He also served in the Soviet Army and witnessed the break-up of the Soviet Union. As a former high-ranking diplomat he helped open the first embassy of Azerbaijan in Washington, D.C. While working for the U.S. Department of State, he instructed diplomats in languages and cultures. He also provided vital assistance as a multi-lingual cultural adviser to U.S. forces during OIF II and became the subject of a Department of Defense newsreel, "Jack of All Languages." Dr. Ibrahimov specializes in the cultural issues of the former Soviet Republics, south central Asia, and the Middle East. He is the author of "An Invitation to Rain: A Story of the Road Taken to Freedom," and numerous other publications. He may be reached at mahir.ibrahimov@us.army.mil.



by Edwin K. Morris

Introduction

The art of warfare is challenging but the role of units rotating in and out of a war zone can impact effectiveness. The process of transferring knowledge between those units is critical to continuing efficiently.

The impact of knowledge management (KM) is very evident in the U.S. Army's process of units replacing other units in a war zone. Commonly referred to as rotational warfare, Relief in Place (RIP) presents a battle flow challenge that relies heavily on the time period both units are concurrently deployed at the same time. With high risk of life and limb, the task of knowledge sharing of the current operational picture (or knowledge base), becomes an insurmountable responsibility upon which lives and missions may depend. Soldiers are given a two-week window in which to exchange knowledge capture and transfer expertise, which serves to demonstrate all related activities, and quickly build rapport between the incoming and outgoing organizations. The Joint Publication 1-02, DOD Dictionary of Military and Associated Terms, defines RIP as:

> ***"An operation in which, by direction of higher authority, all or part of a unit is replaced in an area by the incoming unit. The responsibilities of the replaced elements for the mission and the assigned zone of operations are transferred to the incoming unit. The incoming unit continues the operation as ordered."*** [1]

The purpose of this article is to educate the reader in the Army RIP process by illustrating from anecdotal experience and explicit expertise the essence of KM as a system that is not formally recognized as KM as such. The RIP process is not architecturally KM instrumented into the standard RIP. In order to set the stage within which this combat oriented KM approach operates, we will consider environmental and organizational facets of Army operation from a Military Intelligence (MI) point of view.

A combat unit is assigned to conduct its mission within the designated boundaries of a specific geographic location. By conducting operations in that assigned area over time, the organization produces a very personal and subjective interpretation of that period of time and its events, one which makes exchange or sharing critical knowledge somewhat difficult. The unit's experience may also provide volumes of explicit knowledge which can become difficult for rapid integration by MI due to the massive volume of declarative and procedural knowledge thus represented.

High levels of organizational familiarity achieve a level of expertise representing the internalization of experience into a personal knowledge base that is supported by externalized products. MI operates in a knowledge set different than the rest of the Army and through its operations conducts KM in a much more specific manner that is not a true doctrinally recognized KM methodology. Knowledge discovery and combination are key and very intricate parts of the MI process and the typical mission it performs when deployed in a war zone.

Specific to the field of MI is the discovering, capturing, and applying of knowledge in a manner that is fast paced and hectic. In the operational tempo of the war zone a concept referred to as overcome by events (OBE) exists. This concept recognizes that in warfare the level of explicit knowledge via actions, reports, and analysis may produce the effect of OBE, meaning that what is important at this hour may be OBE by tomorrow. A flurry of information

and data constantly bombards intelligence gatherers and some things may end up falling on the floor. Knowledge is a shifting and constantly moving target that is impacted by many variables, and this sometimes leads to missed opportunities.

Process

Given the conditions and environment of combat operations in a war zone, the official concept the Army employs is referred to as RIP and transfer of authority (TOA).[2] These two events coexist together in happening simultaneously but RIP and its impacts are critical to the focus of this article. The TOA is the culminating event as official orders transfer authority to the arriving unit from the departing one.

Doctrinally, in Field Manual 7-15, The Army Universal Task List, the conduct of a RIP is:

> ***"A relief in place is a tactical enabling operation in which, by the direction of higher authority, all or part of a unit is replaced in an area by the incoming unit. The responsibilities of the replaced elements for the mission and the assigned zone of operations are transferred to the incoming unit. The incoming unit continues the operation as ordered. The relieving unit usually assumes the same responsibilities and initially deploys in the same configuration as the outgoing unit. Relief in place is executed for a number of reasons including introducing a new unit into combat, changing a unit's mission, relieving a depleted unit in contact, retaining a unit, relieving the stress of prolonged operations in adverse conditions ..."*** [3]

As in many operations, the business of war relies solely on a military's personnel; therefore performance is subject to the influence and characteristics of personality. In order to transfer knowledge effectively, the U.S. Army has provided an official two-week window for the RIP cycle to operate. It is commonly referred to as the left seat/right seat, meaning that the first week the departing unit is still driving, but in the second week the incoming unit drives the operation under oversight of the departing unit. During the first week, personnel from both units are teamed together in order to shadow and align to the outgoing personnel by personally conducting the transfer of knowledge. Members are matched up by position to provide a one-on-one exchange capability to reinforce overall mission capability.

This inter-unit teamwork process lends itself to the true KM culture of socializing and relies heavily upon personalities for increasing rates of success. This structure is supported with much explicit knowledge representing the experience of the departing unit and its individual members that transfers to the incoming Soldiers, imparts a baseline comprehension, and highlights all factors relating to the position, the organization, and the mission of the unit. It serves to translate the operational picture and make it personal in nature in order to emphasize the importance and stress of current operational and enemy situation. The departing personnel also set up related "meet and greets" with specific shared organizations, units, and personnel with whom the incoming unit will have to interact. This provides a networking opportunity as not all units rotate at the same time. Such meet and greets provide the relational contacts necessary to secure mission success and install a foundation for future KM opportunities and engagement.

Challenges

Some difficulties arise within the two-week RIP period that can lead to critical failure, and which could result in loss of life. The intrinsic factors of success and importance of this RIP KM transference is demonstrable in quick order. One challenge is not to transfer personal biases and of keeping everything on an objective level. This is a significant test for both the incoming and outgoing personnel alike and both need to be aware of mitigating attitudinal perceptions. A second challenge is that providing the key analysis and all points in an externalization process requires re-focusing to a degree by the effect of departing unit members knowing that they're leaving. Knowledge of one's imminent departure results in a modality shift that can increase the work load and sometimes take away from functional operations. A third challenge is that the transference of hardware and data can be dependent upon equipment, training, and capabilities inherent to the inbound unit.

Related directly to the mission requirements is the challenge of shifting mission changes imposed upon the arriving unit, thus affecting the relevance of the knowledge represented by the out-going unit. The effectiveness of transfer in this formal exchange is not commonly evaluated and relies heavily for success upon the attributes and strengths of Soldiers

of both units. This tends to make the process difficult for the command to gauge the level of achieved success.

In my experience in monitoring and gauging this transfer, knowledge was stored and presented from a PowerPoint presentation. This product reflected all critical knowledge by staff function or by individual Soldiers, in order to calculate what was transferred, and resulted in accountability by demonstrating what had to be accepted and confirmed by both inbound and out-going units.

This gauge provided the basis upon which the TOA was authorized and executed. If the incoming unit disagreed with the fidelity and confidence transferred via the RIP, it could push back the TOA and delay departure. This analysis provided an authoritative account and basis for agreement between units with the understanding they had received all that was presented to a level of proficiency that they could continue the mission without interruption of military capabilities.

In my personal case, I was the primary battalion staff intelligence officer. For the last month before the RIP, an average of 20 to 30 percent of my section's time and effort was spent working upon assembling imperative and empirically explicit knowledge to impart during the RIP. In our case, the checklist and status of all critical tasks was developed with guidance from the battalion executive officer, which by my observation, represented a huge focus for him in preparation and monitoring during that last month. Knowing that the volatility of conducting a war is difficult in and of itself, it is difficult to relate the importance of such work without actually being in such a threatening environment.

So far, the challenges that have been highlighted are those presented during the operation, but looking at the problem foundationally for the Army, there is no training or simulation that might help establish or hone these skills and expectations necessary to the successful conduct of this endeavor.

Aside from the challenges mentioned above, entering into the second week presents an opportunity for the incoming unit to occupy by position and start assuming responsibility of the out-going unit's roles. This provides a mentored and closely observed practice of operating in assigned capacities. This hands-on approach serves to protect the new unit during its novice operational stage, in order to increase that unit's operational confidence and experience. It is a responsibility concluded at the end of the second week at TOA.

This jointly operated two-week period becomes an intensified internship totally designed to transfer as much critical knowledge as possible related to the current threat and operational picture, in order to quickly get the incoming unit up to speed; taking it from an "how to" mode to "now do." It prepares Soldiers for assuming their roles quickly and efficiently in order to provide a continuum of operational effectiveness and impact and to minimize operational interruptions. More importantly, in the eyes of the enemy and the regional inhabitants, this represents a cycle during which the passing of the baton needs to remain unnoticed. The second week allows for some latitude in conducting operations that gives the incoming unit a little wiggle room for making mistakes, because after TOA they will have no side-by-side ability for oversight and assistance.

Measures of Effectiveness

The two-week RIP window is both exhausting and rewarding, and represents a dual situation in which one is expected to systematically approach and rapidly learn to operate in a chaotic and violent venue, and to individually participate as an intricate part in an Army conducting the art of warfare. This process

relies heavily upon on a person-to-person relationship but also produces volumes of externalized experience in data in the some of the following forms:

- Standard operating procedures.
- Tactics, techniques, and procedures.
- Briefing products.
- Reports.
- Analysis.[4]

In this process, the ability to codify experience for incoming units may only serve as a desk reference for knowledge that is often very difficult to express, sometimes representing up to a year or more worth of effort, and sometimes representing lessons learned at a very painful price. It could also introduce mission creep in the out-going unit's operational picture where mission focus might shift away from current operations to this RIP process. All the time and effort taken to create volumes of information representing externalized knowledge might end up actually just collecting dust.

TOA at FOB Danger, Tikrit.

Conclusion

As KM becomes increasingly institutionalized within the Army, these types of business-like processes, such as the RIP, will continue and only improve. The challenge is that as combat operations cease or move from a war zone to peaceful operations, critical steps to capture and transfer knowledge that are not institutionalized doctrinally could hamper proper support to future missions as well as training for such missions. The costs and return on investment is very much relative to the individual nature and culture of the organization, but the entire RIP process is totally dependent upon the mission set of those units' leadership capabilities. The procedures inherent in this process add a safety net for the incoming unit to operate and learn in a threatening environment and represent a temporary bridge for entering into their operational environment. The value created by this effort is as reliant upon the creation of knowledge as it is upon the reception and utilization of that knowledge. This is a shared responsibility encapsulated in the true essence of what KM strengthens. Knowledge resonates in its individually assimilated conveyance but most importantly creates value organizationally, representing a better prepared and innovative culture with attributes that impact operations positively and enhance institutional wisdom.

Endnotes

1. Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, 2010. Retrieved 27 June 2010 from http://www.dtic.mil/doctrine/dod_dictionary/.

2. Field Manual 101-5-1 Operational Terms and Graphics, 1997. Retrieved 23, June 2010, from http://www.fas.org/man/dod-101/army/docs/fm101-5-1/f545con.htm - contents.

3. Field Manual 7-15 The Army Universal Task List, 2009.

4. U.S. Army, Center for Army Lessons Learned, Handbook 10-10, Appendix A, Relief in Place/Transfer of Authority Checklists, 2009. Retrieved 23 June 2010 from http://usacac.army.mil/cac2/call/docs/10-10/ap-a.asp.

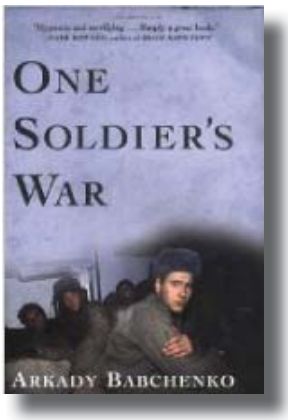
Other References

Sergeant Daniel Nichols, 2nd BCT PAO, 1st Armored. Division., MND-B, "*Relief in place begins between Iron Brigade and Old Hickory,*" (2009) Retrieved 22 June, 2010 from http://www.army.mil/-news/2009/05/09/20874-relief-in-place-begins-between-iron-brigade--and-old-hickory/index.html.

Chief Warrant Officer 3 William S. Sobat, "Relief in Place: Managing Transition of Authority" , *Special Warfare,* Jan-Feb., 2009, Volume 22, Issue 1, Retrieved 21 June, 2010 from http://www.soc.mil/swcs/swmag/Articles_Page6.htm.

Mr. Morris holds a BA in Speech Communication from Edinboro University. He served in the U.S. Army with multiple enlistments as an Infantry Soldier (active duty, National Guard and U.S. Army Reserve), a former Intelligence Analyst and directly commissioned as an All Source Intelligence officer with additional qualification as a Civil Affairs officer. While stationed at Aberdeen Proving Grounds, he earned a graduate certificate in General Administration from Central Michigan University. Additionally, he attained a certificate in Knowledge Management at Fort Huachuca. He is currently attending Kent State University, earning an MA in Information Architecture and Knowledge Management.

Professional Reader



One Soldier's War
by Arkady Babchenko

(Grove Press, New York, NY, 2008)
432 pages, $6.23
ISBN-13: 978-0802118608

Arkady Babchenko served as a Russian soldier in Chechnya in 1996 and again in 1999. Babchenko's book, *One Soldier's War*, documents his wartime experiences in great detail and through the use of easy-to-read vignettes. Except for the short, six-page preface, the book is not strategic in scope or political in nature. Rather, it captures the essence of war from the perspective of a foot soldier on the ground in Chechnya during combat

In spite of its focus on the tactical aspects of war, *One Soldier's War* is an important book for today's soldiers and leaders at all echelons because it reminds the reader of war's horrific nature. Additionally, while Babchenko's book recounts his own experiences in Chechnya, many of his personal observations on the nature of war–civilian casualties, soldier privation, prisoner abuse, maltreatment of subordinates, post-traumatic stress and, above all, violence–could just as well have been written about events in Afghanistan today or World War II seventy years ago.

At one point, Babchenko describes how his unit mistakenly killed several civilians, including children, when they attempted to break contact from a firefight with Chechen rebels. He also describes in great detail how Russian soldiers suffered terribly from the cold, thirst, hunger, and fear. In a poignant illustration, he describes the intense cold he and his fellow soldiers endured during the winter while waiting in an armored personnel carrier for the enemy to attack. In yet another anecdote, he describes how Chechen separatists stabbed or slit the throats of captured Russian soldiers and positioned their bodies in a town to lure out other Russian soldiers while Chechen snipers waited.

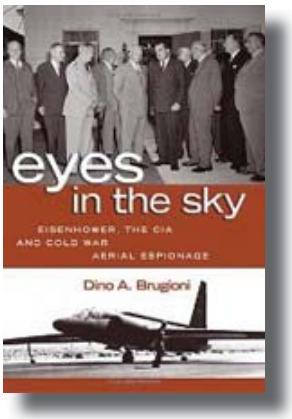
One Soldier's War reflects the tragic but inescapable reality that in war soldiers are often myopically focused on immediate tasks without the understanding of the strategic importance of the war they are fighting. The book paints a picture of frustrated soldiers fighting to survive against the enemy, the elements and their abusive superiors. Babchencko's inner struggles and narrative reflect and illuminate these frustrations.

The book also highlights for the reader several important issues beyond that of a soldier's instinctual fight for survival during wartime. Babchenko repeatedly describes how he and other junior soldiers are beaten by their superiors under the reprehensible system of maltreatment in the Russian army called "dedovshchina" or bullying. Under this shockingly brutal practice, new conscripts are systematically exploited and abused by their seniors. Indeed, the violence is often exacerbated due to drunkenness. He also describes a broken Russian supply system where staples such as food, water, and fuel are lacking and an insufficient property accountability system that fosters an environment where soldiers and leaders routinely sell government property, at times to the enemy, for their own personal gain.

One Soldier's War provides an insightful, albeit singular, look at the Russian army's war in Chechnya from the front line and in the first person. And while the sketches Babchenko uses are choppy at times and perhaps a bit too lengthy in a few instances, they are extremely effective in painting a picture for the reader of the difficult conditions and ambiguous circumstances under which soldiers often exist in war.

At the strategic level, Clausewitz said "war is the continuation of politics by other means." At the tactical level, Babchenko's book reaffirms General Sherman's straightforward notion from the U.S. Civil War that "War is hell."

Reviewed by
Lieutenant Colonel John D. Johnson



Eyes in the Sky: Eisenhower, the CIA,and Cold War Aerial Espionage by Dino A. Brugioni,

(Naval Institute Press, Annapolis, Maryland), 464 pages, $36.95
ISBN: 978-1-59114-082-5.

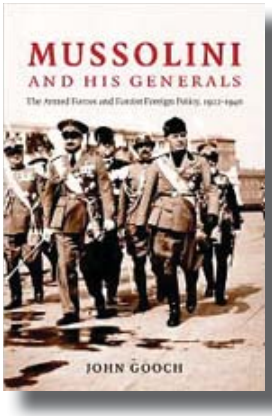
This fascinating book is a tribute to squints. Imagery Analysts rarely receive much attention, let alone praise, sitting quietly in darkened rooms, making sense of distant places, and helping to solve the nation's most difficult intelligence problems. Dino Brugioni's most recent work pays homage to these unsung intelligence professionals who served as Photographic Interpreters before and during the Cold War. More so, *Eyes in the Sky* provides a useful context with which to understand the roots of the American Imagery Intelligence program.

While by no means an autobiography, Brugioni's personal story and his account of aerial reconnaissance are quite closely interwoven. The author, an award winning historian, would spend a full career within the Central Intelligence Agency (CIA), positioning himself in an excellent vantage point to observe the development of strategic Imagery Intelligence. As a senior analyst within the National Photographic Interpretation Center, he had a front row seat in the development of both strategic aerial reconnaissance capabilities as well as the first generation of satellite-based imagery collection. More importantly, the position also afforded him a unique look into the strategic decision-making and the associated intelligence problems of the day. From this angle, Brugioni emphatically suggests that President Eisenhower's steady support for strategic aerial reconnaissance laid the groundwork for American success in the Cold War.

While Eisenhower is obviously a hero to Brugioni, he occasionally depicts villains. Perhaps most tellingly, Strategic Air Command's General Curtis Le May comes across quite unfavorably, underscoring the sometimes strained dynamic between the CIA and the Air Force. Similarly, Brugioni documents the rivalry within the CIA, exposing the conflict between the human intelligence community and the nascent technical intelligence community. He notably takes sides, observing that "we took vicarious pleasure in proving the value of aerial photography over other intelligence sources. The U-2 came to symbolize the rising power of the technical intelligence challenging the Ivy League traditionalists and the OSS holdovers in the Agency." Nevertheless, such honest accounts of internal and external difficulties add vigor to the book, while also exemplifying the passion that Brugioni brings for aerial reconnaissance.

Unfortunately, that passion for strategic aircraft does not quite carry over to a passion for satellites. Despite Brugioni's insistence that the Corona program was Eisenhower's biggest intelligence triumph, the narrative about this program seems almost an afterthought. Instead of treating the development of this important program as a separate topic altogether, he returns to it off and on throughout the book, before finally devoting a chapter to these satellites at the very end. Nevertheless, this is a minor objection. Taken as a whole, Eyes in the Sky is a captivating interpretation of the not so distant past. It meticulously details not only the intelligence problems of the day but also the innovative solutions to those problems. For today's intelligence professionals, especially those making the transition from tactical to operational or strategic intelligence, it is a vital reminder of the necessary relationship between collector and analyst. Moreover, it regularly stresses the broad, holistic approach necessary to provide quality intelligence. In all, Imagery Intelligence succeeded not on the abilities of collectors or analysts acting alone, but on their efforts to collaborate within the broader intelligence community. This is a timeless lesson, one as valuable today as it was nearly half a century ago.

Reviewed by Major Ismael Rodriguez



Mussolini and His Generals by John Gooch

(United Kingdom, Cambridge University Press, 2007) 651 pages, $35.00, ISBN: 978-0-521-85602-7

There have been many books written about the life of Mussolini which is certainly understandable because of his role in enacting a major fascist government during the twentieth century and Italy's participation under his leadership during the Second World War. However, this book focuses on a much more limited aspect of fascism and Mussolini by concentrating on the time between the World Wars I and II and the role of the Italian military during that period. It is a time frame primarily limited to the years from 1922 when Mussolini came into power to the year 1940. The attention given by the author to the role of the Italian military during that time and Mussolini's relation to it are what sets this book apart from many other works concerned with the period of Italian fascist history.

The author provides some interesting information about Mussolini and his military. For example, Mussolini increased the capability of each of the three major parts of the military because of a desire for Italian expansionism and security. Interestingly, it was the Navy that seemed to be his favorite branch, perhaps because of his view that the Mediterranean Sea had important potential military and domestic benefits to Italy. However, Mussolini was never in full control of his military machine as the leader of Italy. Perhaps this was due to the pressures of other responsibilities, and the fact, according to the author that as "military master of Italy, Mussolini brought to this work the limited perspective of his frontline experience and a confident assertiveness founded on ignorance."(519)

Nevertheless, Mussolini found the military useful in a number of ways, including its role in helping him project a powerful image of his country's ability to wage war. He did this by increasing the power of his military forces and his use of military demonstrations and maneuvers which projected an image of a nation capable of offensive and defensive activities. For example, in one situation involving Mussolini's naval and air maneuvers, a commentator suggested that the naval review was "stupefying" and that the Italian Air Force had reached a level of perfection beyond that attained in Germany.(392) However, the reality of the maneuvers may well have been another matter and viewed differently by some other individuals. A general conclusion of the author is that Mussolini's foreign policy was influenced by his military forces, but the same may be said about many other world political leaders then and today.

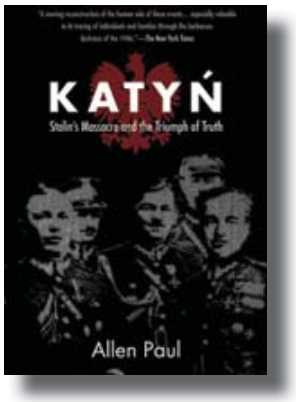
Mussolini's military machine in this book is not pictured in a favorable light. A number of reasons are given by the author to explain this view. For example, although Mussolini was the country's leader, his lack of full control of the military was obvious. This might be explained by the fact that other matters were taking much of his time, and that perhaps the military was insulated in some cases from his direct influence. Another possible problem for the military and Mussolini seems to be a failure on their part to realize that the next war would be a long war necessitating huge resources. Mussolini's own leadership style also contributed to a lessening of the military's capabilities because it lacked a clear form of direction for them.

The author concludes his analysis of Mussolini and his military machine by noting that although Mussolini was responsible for Italy's entrance into the Second World War, his high ranking officers also share some of the blame for the failure of the military due to their ineffectiveness.

The book was written by an excellent scholar who used a wide variety of primary and secondary sources of information to bring it about. It should appeal to a wide variety of readers who desire more information about a specific time frame of Italian politics and the role of its military during that time. For example, students of military history who focus their interest on the preparation for World War II by Italy as well as a number of other countries such as France, England, and Germany will find some

interesting types of information in this book. Other readers who might be interested in knowing something about the role of politics in the preparation of war–especially diplomacy–should find the book informative. In addition, students of Italian politics concerned primarily with the pre-Second World time frame will be pleased with the book because one will find numerous references in it to Italian national political leaders who were quite influential at the time. These readers will also benefit by obtaining some interesting political information about other world leaders and politicians who interacted with Mussolini and his military leaders during the pre-war period. Hence, it is a valuable book written about a novel interesting military topic occurring during an important time.

Reviewed by William E. Kelly, PhD
Auburn University



Katyn: Stalin's Massacre and the Triumph of Truth by Allen Paul

(Northern Illinois Press, DeKalb, IL, 2010) 422 pages, $24.95
ISBN: 978-0-87580-634-1

The Katyn Massacre refers to the murder of thousands of Polish military officers and prominent citizens of that country in a forest by the Soviet secret police in 1940. The victims had been captured by the Soviets, interned in Soviet prisons, and their bodies had been found on Soviet soil. According to this author, its occurrence was a result of the Soviet Government attempting to maintain its control over Poland. We also learn that Stalin and the Politburo approved the killings after receiving a memo from Lavrenty Beria, head of the Soviet secret police at the time. A copy of that memo is found in the appendix of the work and is one of the important items adding interest to the book as it outlines reasons for the massacre to take place.

In this work the Katyn massacre is described as part of a pattern of persecution experienced by the Poles first by the joint Soviet-German occupation, a later German occupation, and then post-World War II communist control. Yet in the end Poland eventually becomes a free country in spite of the negative experiences encountered during a long period of persecution. The massacre has become a symbol of Stalin's brutality to Poland and its people. According to the author "The murders of Katyn were never forgotten because these deaths had come to symbolize the threat to eradicate Poland and her people."(xv)

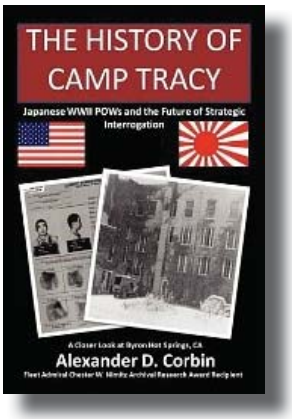
The event itself has been written about in several works and a number of movies have been produced about it. In addition, a Select Committee of the U.S. Congress conducted hearings about the massacre in the early 1950s. Yet, what makes this book different from other works is that it focuses on a series of events affecting three families who were affected by this persecution; the Hoffmans, the Pawulskis, and the Czarneks. In each family a husband was lost who was a professional. One was an attorney, another, a regular army officer, and the third a physician. All three husbands perished at the peak of their professional career. The Hoffmans suffered separation with the mother being sent to Siberia and her infant daughter remaining in Poland. The Pawulskis were deported but eventually made it to America. The Czarnecks suffered daily repression under the German General Government. The book is a narrative of what happened to each family during the war period set around the Katyn massacre itself. We learn of their personal and professional sufferings, but we also learn about how various government officials and others reacted to the wholesale murder. The author conducted numerous interviews with relatives of families to obtain information about how the massacre and the persecution of Poles affected each family. Hence the book has the added favorable element of personal interpretation based on actual experiences relayed among rela-

tives. It is a story about tragedy, suffering, but glory in the end as Poland eventually regains its freedom and independence.

The views of some of the great powers toward the massacre are described in an interesting manner in this work. Germany and the Soviet Union each reacted to the massacre in a manner designed to benefit themselves. When the Germans first discovered the graves, they recognized that it gave them a tremendous opportunity to exploit a negative picture of the Soviet Union. They even invited the German Red Cross to view the grave sites. They also hoped the massacre would weaken the alliance between the Soviet Union and other countries united against them. The Soviets, whose own secret police committed the massacre, attempted to benefit by blaming it on the Germans. Considering the negative image of the Nazis held by many this approach could become believable to some. The Americans and the British are not pictured in a very favorable light in terms of their reaction during the war to their massacre. However, if they had admitted publicly at the time that the Russians were indeed responsible for the massacre it might have made cooperation with the Soviets more difficult at a time when Soviet help against the Nazis was needed. erhaps their reactions at the time reflected the necessities of winning a war against an enemy who should be defeated at all costs.

Politically, the Katyn massacre has had tremendous ramifications. For example, it is described as perhaps the biggest obstacle today to good relations between Poland and Russia even though Gorbachev in 1990 admitted Soviet guilt. Yet, the admittance of guilt by the Russians is not enough to satisfy many Polish individuals. More information is wanted about the events surrounding the massacre. There are still many unanswered questions which are important to the Poles and to their history. Perhaps there will never be answers to these questions, but the Poles will remain attentive to the subject since it is a very important part of their heritage.

Reviewed by William E. Kelly, PhD
Auburn University



The History of Camp Tracy Japanese WWII POWS and the Future of Strategic Interrogation by Major Alexander D. Corbin

(Ziedon Press, Fort Belvoir, VA, 2009)

190 pages, Paperback: $21.95

ISBN-13: 978-0-578-02979-5

In *The History of Camp Tracy: Japanese WWII POWs and the Future of Strategic Interrogation,* Major Alex Corbin provides the reader an extremely relevant and previously unexplored study of the strategic level interrogations program done at Camp Tracy, California during World War II. His book answers the key question of "How can the U.S. obtain the requisite information from a foreign and hostile enemy while abiding by the law and without further alienating the international community." Based on the recent failures at the U.S. interrogation centers in Guantanamo Bay and Abu Ghraib, we must find an answer to this question if we are going to effectively execute operations against extremist factions. Corbin uses the extremely successful operations at Camp Tracy to answer that question by providing clear comparisons and lessons learned for today's fight against extremist Islam.

Of note, Corbin clearly shows how the militant, ideologically driven, and drastically differing Japanese culture from Western culture directly parallels that of extremist Islam, which further emphasizes the relevance of this case study in today's fight. Through his detailed account of how the

Soldiers at Camp Tracy deliberately planned and executed interrogations within the law of war and Geneva Convention, we able to find specific tactics, techniques, and procedures that can be used today. The book is written in a very logical and easy to understand manner allowing the reader to gain a deeper insight into strategic level interrogations operations done during World War II. His ability to seamlessly blend the operations at Camp Tracy with applications for today's War on Terror makes this book a must read for anyone interested in the use and execution of interrogations to achieve our national objectives. It should be on every professional reading list.

Corbin's work provides critical lessons learned and best practices use that can be directly applied in today's era of persistent conflict. The most important lesson, as recognized early by the Office of Naval Intelligence, is that the most critical part of any interrogation process is selecting the right interrogators and is a hard lesson we continue to relearn in each conflict, including most recently in Iraq and Afghanistan. In order to accomplish this, the Office of Naval Intelligence applied strict selection requirements that could be used today. An example of a best practice that led to the success of Camp Tracy was the stringent, multilevel screening process that was used to determine the prisoners of war to be interrogated at Camp Tracy, ensuring that the selected prisoners produced the greatest probability of success. Other best practices include cultural awareness of the detainees, using people of common background, remaining courteous, constant observation in order to use behaviors or weaknesses later, and team work between interrogation teams. Based on the success at Camp Tracy and Corbin's comparison to current operations, the reader gains insight into how a successful strategic interrogation program can be run without violating the rules of war, or the Geneva Convention.

Corbin's logical and easy to follow writing style enhances the reader's ability to rapidly assimilate the concepts presented leading the reader to an answer about "how can the U.S. obtain the requisite information from a foreign and hostile enemy while abiding by the law and without further alienating the international community." So the reader can better understand the topic and comparison, he provides an in depth historical background to the topic that includes comparison between radical Japanese and Islamic fundamentalists, and the operations at Camp Tracy. The book then flows into the interrogation and findings from the case study. Additionally, the appendixes include an actual outline for interrogations and an interrogation packet from Camp Tracy. All of these factors combine to allow the reader to get the most from this case study of strategic interrogation.

The History of Camp Tracy: Japanese WWII POWs and the Future of Strategic Interrogation is a must read for anyone trying to understand how we can gain critical intelligence while remaining within the law of war and the Geneva Convention. Corbin's in-depth analysis of operations at Camp Tracy, comparisons to recent actions in Operation Enduring Freedom, and the lessons learned provide the reader many best practices that can have far reaching positive effects in this era of persistent conflict. This is a must read for anyone interested in wartime interrogation.

Reviewed by
Lieutenant Colonel John D. Nawoichyk

What is the UMI? Where is it? How do I use it?

The University of Military Intelligence (UMI) is a training portal of MI courses maintained by the U.S. Army Intelligence Center of Excellence (USAICoE) at Fort Huachuca, Arizona for use by authorized military (Active, Reserve, National Guard) and non-military (e.g., DOD civilian, Department of Homeland Security, other U.S. Government agencies) personnel. UMI provides many self-paced training courses, MOS training, and career development courses. In addition, the UMI contains a Virtual Campus that is available to users with an abundance of Army-wide resources and links related to MI: language training, cultural awareness, resident courses, MI Library, functional training, publications, and more.

UMI is undergoing improvement and expansion to become available for any approved MI courses (from any U.S. Army MI source) that are designed to be offered as Distributed Learning (dL) via the UMI technologically advanced online delivery platform(s).

UMI online registration is easy and approval of use normally takes only a day or two after a user request is submitted. Go to http://www.universityofmilitaryintelligence.army.mil, read and accept the standard U.S. Government Authorized Use/Security statement, and then follow the instructions to register or sign in. The UMI Web pages also provide feedback and question forms that can be submitted to obtain more information.

Use of the UMI requires:

- User registration (it's free!).
- An active government email address (such as .mil or .gov).
- A sponsor (if user has no .mil or .gov email address) who can approve user's access to training material.
- Verification by UMI of user's government email address.
- Internet access. UMI courses require Internet Explorer 7 or previous browser and Adobe Reader, Adobe Flash Player, Adobe Shockwave Player, Windows Media Player, and/or a recent version of MS Office.

UMI
Powered by
USAICoE

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 (MI) and Intelligence Communities (IC).

Articles about current operations and exercises; TTPs; 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 and it may take up to a year to publish some 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 unit or organization's information and operations security officer/ SSO stating that your article and any accompanying graphics and photos are unclassified, nonsensitive, and releasable in the public domain OR that the article and any accompanying graphics and photos are unclassified/ FOUO (IAW AR 380-5 DA Information Security Program).** A sample security release format can be accessed at our website at https://icon.army.mil.
- 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 Word. Do not use special document templates.
- A Public Affairs or any other release your installation or unit/agency may require. Please include that release(s) 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. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg and note where they should appear in the article. PowerPoint (not in .tif or .jpg format) is acceptable for graphs, etc. Photos should be at 300 dpi.**
- 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 help us ensure a quality product. Please inform us of any changes in contact information.

Submit articles, graphics, or questions to the Editor at mipb@conus.army.mil. Our fax number is 520.538.1005. Submit articles by mail on disk to:

MIPB
ATTN ATZS-CDI-DM (Smith)
U.S. Army Intelligence Center and Fort Huachuca
Box 2001, Bldg. 51005
Fort Huachuca, AZ 85613-7002

Contact phone numbers: Commercial 520.538.0956 DSN 879.0956.

The 11th annual CSM Doug Russell Award ceremony was held on 8 March 2011 during the Military Intelligence (MI) CSM/SGM Conference. This year's award, as well as the Knowlton Award, was presented to Specialist Sasha Fleetwood. Specialist Fleetwood was born in Pampa, Texas, in 1989; the oldest of four brothers and sisters. She graduated from Borger High School, Borger, Texas in 2007 where she lettered in cross country, track, wrestling, cheerleading, and academics. She then completed two semesters at Oklahoma City Community College with a focus on Engineering. She enlisted in the Army in February 2008, and graduated from Basic Combat Training at Fort Leonard Wood, Missouri, in August 2008. Specialist Fleetwood then graduated from the Human Intelligence (HUMINT) Collectors Course at Fort Huachuca, Arizona in March 2009.

Her first assignment was with the 202nd MI Battalion, 513th MI Brigade, Fort Gordon, Georgia. After arriving at Fort Gordon in March 2009, she initially conducted overt debriefing operations in support of U.S. Army Intelligence and Security Command and U.S. Army Central mission requirements. After proving herself as a HUMINT Collector, she was chosen to deploy with a Counterintelligence-HUMINT platoon from Alpha Company, 202nd MI Battalion.

From October 2009 to October 2010, Specialist Fleetwood supported Combined Joint Special Operations Task Force–Afghanistan (CJSOTF-A). During her year in Oruzgan Province, Afghanistan, she was responsible for conducting Military Source Operations and Interrogations in support of Special Operation missions. She wrote more than 40 Time Sensitive Intelligence Reports and 150 Intelligence Information Reports which resulted in a significant reduction of attacks throughout the region. While deployed, she spearheaded the establishment of a female *shura* that gave political voice to the area's female population. During her deployment, Specialist Fleetwood participated in more than 40 combat missions and was awarded the Combat Action Badge for her role as a member of a mortar team during an engagement with enemy forces.

"I really didn't do anything special; I just think I did my job," Fleetwood stated when talking about her deployment and mission in Afghanistan. She went on to say that the best part of the deployment was being able to see she had made a direct impact. "I told myself when I went to Afghanistan that I didn't want to leave feeling unaccomplished and I think I met my goal; I feel I did something good." Specialist Fleetwood says she owes her success to the mentorship she received.

For her meritorious service in support of CJSOTF-A, Specialist Fleetwood was awarded the Bronze Star Medal. She was promoted to Sergeant on 1 May 2011.

The CSM Doug Russell Award recognizes a Soldier (Sergeant or below) who has made significant contributions to the MI Corps. The award was established in 1999. Nominees must be active duty, National Guard, or Reserve MI Soldiers or non-MI Soldiers assigned to an MI unit. Although the nominees need not be MI Soldiers, their achievements must be in direct contribution to the MI mission. Ten MI Corps Soldiers were nominated for the award—four Specialists and six sergeants.

Photo by Amy Sunseri. Portions of this announcement were originally printed in The Huachuca Scout, 17 March 2011 by Amy Suneri.

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

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

PIN: 100933-000