

# MIPB

Military Intelligence Professional Bulletin

July ~ September

2008

PB 34-O8-3

## ON THE HORIZON

MI MISSIONS  
OF THE  
NEAR FUTURE



# FROM THE EDITOR



Military Intelligence (MI) is always engaged and always looking forward with an eye to future threats. This issue takes a look at how MI is adapting to the current operational environment and developing tactics, techniques, and procedures to counter the threat today and in the near future.

Two articles speak to the use of persistent surveillance to support the current fight, capabilities and limitations, and employment in the future modular force.

An article from the 82<sup>nd</sup> Airborne Division talks about an initiative from the 1/82 BCT, the Special Weapons Exploitation Team, an internally resourced BCT capability to analyze enemy effects and counter threat weapons/tactics in today's and tomorrow's complex combat environments.

The MI Noncommissioned Officers' Academy has recently upgraded its automation to enhance training by adding a Thin Client to each student's workstation. This and near future plans to take advantage of OSINT data in training are explained in the CSM Forum.

Also included are articles on the Red Teaming concept, adapting Counterintelligence to counter low intensity collection of technology, and an introduction to the Defense Support to Civil Authorities Disaster Intelligence concept.

Personal experiences from Iraq are related in two articles, one dealing with working with Coalition intelligence forces; and the other with border operations with the Iraqi Security Forces. A historical perspective takes a look at the causes of the resurgence of the Taliban in Afghanistan.

Finally, a reprint of an article from the Defense Intelligence Agency's *Communiqué* describes that agency's efforts to provide its employees with the kind of work environment needed to successfully support the Warfighter.

Check out the inside back cover which summarizes the Initial Draft updates and changes to the Army's keystone doctrine on intelligence, FM 2-0. When published, it will replace the current FM 2-0, 17 May 2004, with Change 1 dated 11 September 2008.

You will notice photos of some very old equipment used by MI professionals in the earlier days of MI in this issue. The photos were taken at the Army Intelligence Museum located at Building 41411, Hungerford and Rhea Streets, Ft. Huachuca, Arizona. A very worthwhile visit, the museum is open Monday through Friday from 0900 to 1600, and Saturday and Sunday from 1300 to 1600.

***We have resumed printing. If your unit or agency would like to receive MIPB at no cost, please email sterilla.smith@conus.army.mil and include a physical address and quantity desired or call me at 520.5358.0956/DSN 879.0956. We are no longer accepting personal subscriptions. We mail to APOs.***

*Sterilla A. Smith*  
Sterilla A. Smith  
Editor

# MILITARY INTELLIGENCE

PB 34-08-3

Volume 34 Number 3

July - September 2008

**Commanding General**  
Major General John M. Custer III  
**Deputy Commandant for Futures**  
Mr. Jerry V. Proctor  
**Deputy Commander for Training**  
Colonel Dennis A. Perkins  
**Director, Directorate of Doctrine**  
Colonel Michael Arinello  
**Chief, ISR Operations Analysis Division**  
Mr. Chet Brown

**MIPB Staff:**  
**Editor**  
Sterilla A. Smith  
**Design Director**  
Patrick N. Franklin  
**Design and Layout**  
Patrick N. Franklin  
Lawrence A. Boyd  
**Cover Design**  
Lawrence A. Boyd  
**Inside Back Cover**  
Patrick N. Franklin  
**Issue Photographs**  
Courtesy of the U.S. Army and DIA

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

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

## FEATURES

- 7 **Tactical Persistent Surveillance**  
by Colonel Sharon R. Hamilton, Mr. Richard L. Smith, and Mr. Martin C. McCleary
- 19 **Special Weapons Exploitation Team: Filling a Technical Intelligence Gap**  
by Captain Micah A. Niebauer with an Introduction by Colonel Charles A. Flynn
- 25 **Collection Management in the COIN: A 3rd Infantry Division Perspective**  
by Chief Warrant Officer Two Martin Schwerzler
- 28 **Red Teaming and the Intelligence Professional: The Environment and the Challenge**  
by Nicholas R. Marsella
- 33 **Coalition Intelligence in OIF: A Year in Iraq with Multinational Division - Central South**  
by Lieutenant Colonel Robert M. Wilkinson
- 38 **Part 2: 3rd Regional BTT - Initial Operational Employment on the Iraq/Iran Border Wasit Province**  
by Lieutenant Colonel Michael P. Spears
- 47 **Synthesis: Intelligence Support for Disaster**  
by Lieutenant Colonel Robert A. Blew, U.S. Army, Retired
- 52 **Secessionist Jihad: The Taliban's Struggle for Pashtunistan**  
by Major Michael D. Holmes
- 59 **Transforming CI to Counter Low-Intensity Collection of High Technology: Forcing the Enemy Back to the Outside Game**  
by Mark A. Thomas, PhD
- 66 **Amateurs Talk Tactics, Professionals Talk Logistics**  
by DIA Staff Writer

## DEPARTMENTS

2	<b>Always Out Front</b>	70	Contact and Article Submission Information
3	<b>CSM Forum</b>		
69	<b>Intelligence Philatelic Vignettes</b>	71-72	CG's Reading Lists
			Inside Back Cover: Initial Draft Updates FM 2-0

By order of the Secretary of the Army:

Official:

*Joyce E. Morrow*  
**JOYCE E. MORROW**

Administrative Assistant to the  
Secretary of the Army

**0822021**

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

# ALWAYS OUT FRONT

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



***"The more things change, the more they stay the same." "The only constant is change."***

A basic tenet of successful operations is that Military Intelligence (MI) assets are always engaged. Even while conducting intelligence operations in the current fight, we also maintain an eye on future threats; potential areas of conflict or instability; rising adversaries, and emerging technology. Our branch constantly looks over the horizon to identify emerging technology, conditions, and developments to determine that which may be used against us or that which U.S. forces could integrate into current or future capabilities. The theme of this MIPB issue acknowledges the inherent nature of the MI Corps being “Always Out Front” while simultaneously looking even farther forward.

The MI Corps is supporting worldwide combat operations with increasingly accurate, timely, and actionable intelligence. Yet, we are also in the midst of a transformation as to how we are organized; the scope and manner in which we perform our missions (tactics, techniques, and procedures); the types and means by which we establish links and relationships with other intelligence organizations; the types of equipment and employment measures, and even changes to military occupational specialties and areas of concentration for MI Soldiers and officers.

Some have said that implementing the changes that are being made within the MI Corps while we are at war is similar to changing all four tires on a car while traveling on a highway. But, we do not have the luxury of stopping to reorganize to meet future threats or conditions, and then resuming MI support to the Warfighter.

I have visited, served with, and currently serve with many of you who are addressing the challenges of today while simultaneously preparing to conduct the

missions of tomorrow. I never cease to be amazed by the degree of dedication, professionalism, and commitment to excellence you display daily in accomplishing these disparate missions. The “Change Train” is not slowing down, and unfortunately our enemies are not slowing down their activities, training, or planning either. Today we face an incredibly adaptable, technologically savvy, and patient group of enemies. The future only holds the promise of an increasingly capable threat. While no other nation’s MI force can rival us; the threat’s increasing reliance on asymmetric intelligence and operations schemes indicate our MI Soldiers will have to perform increasingly difficult intelligence tasks in much more complex environments in the future. While this is a daunting projection, there are U.S. Army Intelligence Center (USAIC) folks hard at work at to ensure we remain the preeminent MI force.

The good news is that we have top-notch people working hard to solve the problems of tomorrow before they even occur. Training is my number one priority and central to the reason for the existence of USAIC. Most of you are familiar with, and have graduated from, training courses here at Fort Huachuca. What you may not know is that we also have an organization here responsible for studying what is happening today; identifying current requirement shortfalls; estimating requirements for the future; developing courses of action to address these future requirements, and then putting into action a series of actions seeking to maintain an MI Corps capable of meeting and defeating any adversary on any battlefield today or in the future. This organization is known by the acronym CDI (*see-dee-eye*); which stands for Capabilities Development and Integration. CDI is led by my Deputy Commandant, Mr. Jerry V. Proctor who holds a Senior Executive

(Continued on page 4)



# CSM FORUM

by Command Sergeant Major Gerardus Wykoff  
Command Sergeant Major  
U.S. Army Intelligence Center and Fort Huachuca

## **USAIC Transforms the NCOA to Leverage the Media Gap with the Army's Intelligence Enterprise in Training**

When most Military Intelligence (MI) senior NCOs think back to their experience in NCOES, they think of a bland classroom with at most a television, VCR, one instructor and 16 students. The small group instruction method of training allowed for the free exchange of thoughts and ideas which tremendously enhanced the training experience; but all-in-all, it was nothing to write home to Mom about. The same could be said about NCOES six months ago. Although we had graduated to A/V suites projected on screens, it still only served to replace the television and VCR/laptop. *Status quo.*

All of that is quickly changing. Over the last six months, dramatic improvements to our baseline automation infrastructure have found your MI NCO Academy (NCOA) setting the pace, ahead of the other NCOAs across the Army. The introduction of a Thin Client solution on a multi-domain backbone has allowed each student the capability of accessing the SIPRnet from his/her workstation. The classroom ratios are still the same: one instructor to 16 students, but each student now sits at a Thin Client workstation. This solution fits well into the MI Corps' Commanding General's focus of weaving the Distributed Common Ground Station-Army (DCGS-A) into the training strategies of the Advanced NCO Advanced (ANCOC) Course and the Basic NCO Course (BNCOC). DCGS-A will become an integral part of MI NCOES (where reasonable and applicable) as early as late August, early September.

In the near future, the MI NCOA plans to incorporate the use of Decisive Analytics Corporation's (DAC) Mainship Enterprise-class Media Asset Management software into MI NCOES. Mainship provides the ability to search for and retrieve video clips and images from international venues to enhance global situational awareness.

The MI NCOA intends to explore every facet of Mainship's capabilities as a potential accompaniment to ANCOC and Phase II, BNCOC.

## **Mainship—A Time for Change**

*A bit of history.*

In February of 1941, the federal government established the first Open Source Intelligence (OSINT) operation to monitor foreign broadcasts over open airways. The service was the Foreign Broadcast Monitoring Service; later to become the Foreign Broadcast Information Service (FBIS). Initially this service monitored propaganda from the Axis Powers thus the importance of OSINT was realized and investments were made in growing collection methods.

Today OSINT includes a wide variety of information and sources:

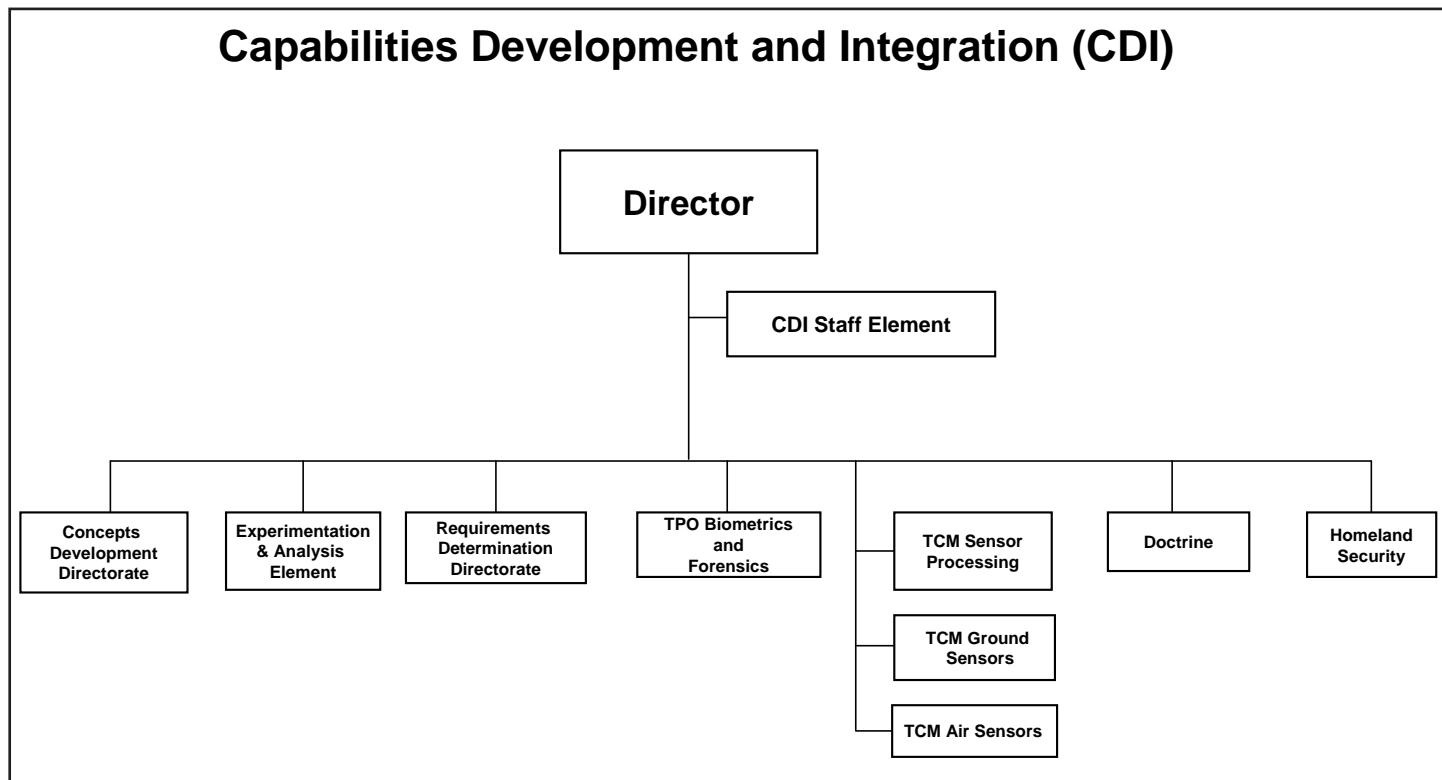
- ◆ Media—newspapers, magazines, radio, television, and computer-based information.
- ◆ Public data—government reports, official data such as budgets and demographics, hearings, legislative debates, press conferences, speeches, marine and aeronautical safety warnings, environmental impact statements, contract awards.
- ◆ Observation and reporting—unmanned aerial systems' flight data, radio monitors, and satellite observers, among many others, have provided significant information not otherwise available. The availability of worldwide satellite imagery, often of high resolution, on the Internet (i.e., Google Earth) has expanded open source capabilities into areas formerly available only to major intelligence services.

In 2002, FBIS came to the DAC to assist them in transforming their facility from an analog system, where all broadcasts were manually reordered on consumer VHS recorders, to a totally digital facility where all incoming feeds were digitally recorded, indexed, stored, and made available on web based

*(Continued on page 5)*

# ALWAYS OUT FRONT

Service rank. The major elements within CDI are depicted in an organization chart format below. Just as you do, the Soldiers and civilians (government and contractor) working within CDI support both the current fight while preparing for the future. The names of most of the major muscle groups within CDI give you an idea of the areas for which they are responsible: Concepts Development Directorate, Requirements Determination Directorate, Experimentation and Analysis Element, Doctrine, and Homeland Security.



Other elements within CDI are the U.S. Army Training and Doctrine Command (TRADOC) Capabilities Managers (TCMs) ‘tick-ems’ for Sensor Processing (TCM SP), Ground Sensors (TCM GS), Air Sensors (TCM AS), and the TRADOC Program Office for Biometrics and Forensics (TPO B and F). The TCMs and TPO work for you. They are your representatives and advocates to the Army and those whom the Army charges to design, build, and field the equipment (or capability) you employ to accomplish the MI mission.

This issue of MIPB includes an article based on the concept developed within CDI regarding Tactical Persistent Surveillance. Future issues of MIPB will include articles highlighting various missions and accomplishments of the TCMs and other elements within CDI. Keep an eye out for these articles. We too are working the challenges of today, while keeping watch over the horizon. 

**Always Out Front!**

## CSM FORUM

servers. The product was named “Mainship” and it has undergone several modifications over the past five years. Mainship is currently available to thousands of authorized users through the ‘OSC.gov’ network and has gathered in excess of 400 terabytes of data.

### **USAIC’s Digital Asset Management System**

Recognizing the importance of OSINT data in the intelligence process and the many sources to obtain this data, the U.S. Army Intelligence Center (USAIC) deployed the new Mainship digital asset management system at Fort Huachuca. Now students at the facility have the ability to train on the same system that the Director of National Intelligence Open Source Center, the Office of Naval Intelligence, the Defense Intelligence Agency, and the Federal Bureau of Investigation utilize on a daily basis to ingest, index, and retrieve relevant OSINT data from worldwide broadcast news to digital pictures retrieved from cell phones. The Mainship system has the ability to store the captured data as well as associated notes from analysts, maps, whitepapers, URL address, etc.

Moreover, USAIC is creating a simulated operational environment enhancing the Warfighter experience through the use of Mainship capability. The inspiration behind this *irreversible momentum* is derived from the direction provided by the then Multinational Force-Iraq Commander, General David Petraeus, when he stated, “It is largely recognized in both theaters of war that operationally the forces are much further ahead of schoolhouse and home station training.” How we train, what we train, and the systems we use today will be shaped by the day-to-day developments at the forward edge. These tools enable instructors to provide a truly enriched combat environment in the classroom for our Soldiers.

### **Mainship Family Features**

**News monitoring.** Mainship grew up on news monitoring. The Mainship family includes a variety of different 24/7 A/V recorders called Mainship Core™ and Mainship Edge™. Mainship Core encoders allow web users to search and playback content directly from the encoder utilizing a unique distributed capture and storage configuration. Mainship Edge encoders live at the “edge” of your collection workflow and play out through the Clipplay™ appliance. For critical content that needs to be re-

tained indefinitely, there is an option to transfer to Mainship Genesis™. The Mainship™ family allows scalability to meet your specific needs.

**Mainship Genesis.** The heart and soul of Mainship is the integrated web and database system known as Genesis™. Start with a simple solution and scale as your needs change. Genesis includes integrated users and group management along with dozens of other standard features such as proxy mapping and lightweight directory access protocol integration. Genesis grows with a simple licensing scheme based upon numbers of assets and users.

**Ultimate scalability.** Mainship’s unique disconnect architecture allows remote news capture and monitoring through its ability to run without being constantly connected to the Mainship Genesis system. Because Mainship is designed for enterprise applications, the system can be customized for both the number of users and the quantity of assets.

**Live streaming to the desktop.** In addition to the Mainship Edge and Core 24/7 recorders, Mainship also offers single and multi-channel live stream encoders to provide real-time access to live content. This allows the ability to schedule live streaming to any desktop on the network where a user with permissions is located. USAIC can alert students when particular “live venues” are going to be streamed so they can watch from their desktop.

**Robust player interface.** Mainship’s Rich Media Player interface allows users to dive in and move rapidly through a program by browsing through the scene changing thumbnails or synchronized and highlighted CC or speech recognized text within the transcript.

**Powerful search engine.** Based upon the latest Oracle Enterprise Database and Lucene query parsing technology, Mainship’s Genesis search system allows searching across multiple metadata values such as date, time, and keywords and also supports advanced “Google-like” techniques such as “sounds like” or “near” (find words within 15 or 20 words of each other). You get the idea.

**Clipplay-The integrated output appliance.** What good is an asset management system if you can’t get the content back out of the system? Mainship Clipplay is a powerful touchscreen appliance that allows users to fulfill media orders directly

# CSM FORUM

---

to CDs and DVDs from the Mainship collection. Users can also play video files as full-screen NTSC video for presentations and/or recording to VHS.

**Third party system integration.** Mainship's optional external application interface allows files and metadata to be moved between multiple systems passing both metadata and A/V files in both directions.

**Complete integration.** DAC recognized that the market was ready for a turn-key solution that was easy to use and included everything necessary in an enterprise asset management system including scheduling, streaming, on-demand playback, and long-tail archiving.

**Full range of options.** Mainship's five year development cycle has allowed DAC to develop a robust selection of optional features and capabilities. These capabilities are integrated in a tight, cohesive workflow that let users focus on things other than the complexities that can haunt a home-made system.

## **Mainship Genesis options:**

- ◆ Profile notification—This optional service allows users to create custom profile searches. When new content is captured that matches the profile, the user is notified by email and is provided a link to view the content immediately.
- ◆ Online editing—Don't deploy editing software to thousands of users. Do it all within Genesis. Intuitive online editing of programs allows users to create new assets or sub-clips of programs for other purposes.
- ◆ Media order—Integrated media workflow allows users to request a program in different formats such as MPEG1, Real, Flash, 3GPP, Quicktime, and many other formats. These programs can be delivered to the desktop or anyplace of the user's choosing.
- ◆ Document attachments and search—Do you have a need to keep documents such as scripts, PDF files and related images in the same system as your media assets? With the document attachment option, Mainship will ingest your textual and image documents, index them, and make

them searchable. Once ingested the documents can be linked to programs so a user can search for words found within the document or image file and be linked to the related video program. Now users can have video files **and** linked text and images together.

- ◆ Advanced scheduling option (ASO)—Mainship ASO allows users to create more detailed recording schedules. Rather than just 24/7, ASO allows users to record specific programs at specific times and lengths with more descriptive metadata.
- ◆ Advanced storage management (ASM)—Most media asset management systems force you to calculate this important part of the system manually. With Mainship's ASM option, you can delete, manually or automatically archive, and move files around based upon your storage architecture. ASM integrates particularly well with third party HSM/tape library solutions such as diskxtender from EMC and Xendata.

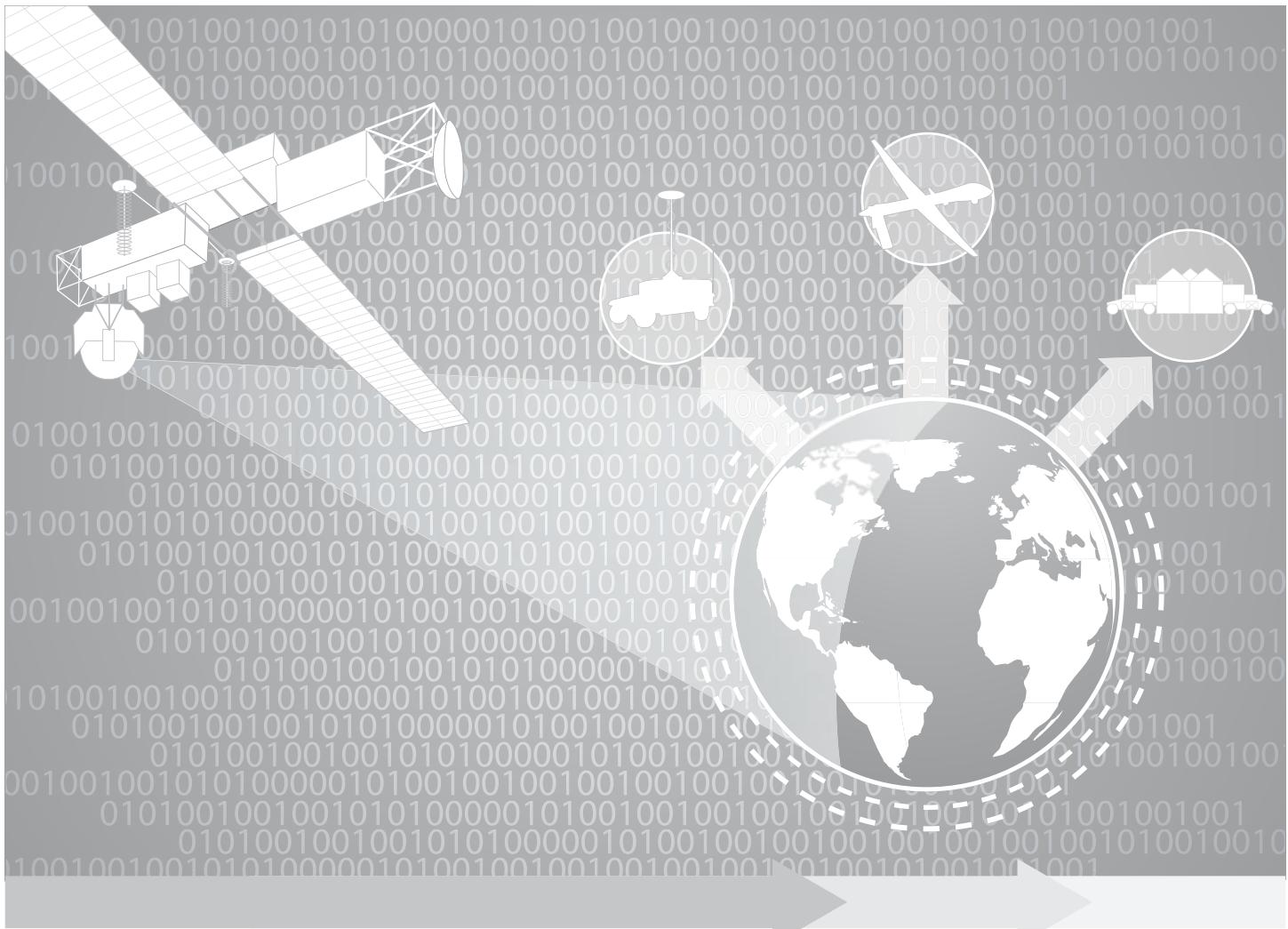
**Ingest Content from File.** Already have a large supply of digital media files such as MPEG and WMV? Use Mainship's Optional Hydra™ service to ingest files, including metadata, for searching later. The Hydra Ingestion service creates a low resolution proxy version of the video file and still maintains the high-resolution source file for editing, conversion to different formats, or burning to DVD/VHS.

**Live Foreign Language Conversion.** Mainship's new speech to screen (STS) technology provides real-time monitoring of broadcast foreign television programs. The current STS application is for Arabic; however, additional languages are planned for the future. The keyword alerting feature monitors your system-defined "keywords" and highlights those on the display screen to provide a quick alert to the occurrence of critical words and phrases. STS can run stand alone however, when connected to a Mainship Genesis system, users can search and review past programs.



*Captain Agustin Taveras (CIO/G6) and Joel Emry contributed to this column.*

## **NCOs Lead from the Front!**



# TACTICAL PERSISTENT SURVEILLANCE

---

by Colonel Sharon R. Hamilton, Mr. Richard L. Smith, and Mr. Martin C. McCleary

---

## Introduction

The purpose of this article is to present the key concepts associated with persistent surveillance, distill those ideas into a proposed Army definition, and identify current and future capabilities to achieve tactically focused persistent surveillance. We need an approved Army definition for tactical persistent surveillance (TPS) in order to establish a baseline from which to further refine and develop the associated doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF) implications.

The idea of persistent surveillance missions is not new. Beginning with the 2001 Quadrennial Defense Review (QDR), the term persistent surveillance was referenced, yet not defined. Since 2001, there have been numerous efforts within the Department of Defense (DOD) to define the term and its associated capabilities and limitations. Within the Army, agreement on a common definition for persistent surveillance has proven a challenge, and subsequent attempts at definition confused rather than clarified the meaning and the desired end state of persistent surveillance.

It may be helpful to first define what TPS is **not**. TPS is not:

- ◆ an “intelligence only” mission, it’s an Army combined arms mission.
- ◆ equal to an “unblinking eye” 24/7/365.

- ◆ the same as constant surveillance.
- ◆ a panacea that will eliminate mission uncertainty and risk.
- ◆ a replacement for detailed operational planning.
- ◆ solely a sensor capability issue.
- ◆ meant to imply simultaneous detailed surveillance of all objects of focus over the entire area of operations (AO).
- ◆ a new idea.

There is an informal consensus that the goal of persistent surveillance is to provide actionable intelligence at the right time, in the right format to answer a clearly focused, specified duration, priority intelligence requirement. Persistent surveillance requires:

- ◆ robust, survivable, assured network communication capability.
- ◆ networked enterprise to link and synchronize tactical through national sensor system employment, data accessibility, and analytic effort.
- ◆ enhanced system-level analytical and exploitation tools that fill gaps in our ability to see and understand the enemy.
- ◆ planning tools and control methodologies for coordinating and controlling multiple data collection, analysis and information processing systems.
- ◆ an ability to detect a change in the environment.

## **Definitions**

- ◆ **Joint Definition.** **Joint Publication 1-02** defines *persistent surveillance* as: “A collection strategy that emphasizes the ability of some collections systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in real or near real time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action.”
- ◆ **Proposed Army Definition.** Currently, there is no approved Army definition for persistent surveillance. Joint doctrine and Army concepts offer multiple definitions for persistence, surveillance, or persistent surveillance. TPS missions are much more than a collection strategy and cut across all disciplines, branches and services. The following definition is offered for consideration: TPS is the synchronization and integration of available, networked sensors and analysts across warfighting functions and operational environments (OEs), to provide commanders with combat information, actionable intelligence and situational understanding. TPS missions detect, characterize, locate, track, target, and assess specific objects or areas, in real or near real time despite target countermeasures or natural obstacles.

The terms used in this definition serve to simplify and focus this complex mission:

- ◆ **Tactical.** Constraining the definition to TPS provides focus of purpose to the immediate Army concerns of providing maximum support to the ground component.
- ◆ **Synchronization and Integration.** The inclusion of synchronization and integration reinforces the requirement that operations and intelligence functions be fully linked down to the lowest echelon and include sensors commonly associated with intelligence collection activities and those that are not. Total sensor visibility, dynamic cueing, manned and unmanned teaming, and seamless system networking are all elements of synchronization and integration.
- ◆ **The OE.** Persistent irregular or smaller scale conflict will characterize the future OE and require increasingly time critical, focused resolution of individual targets. We conduct tactical missions focused on individual targets at extended distances in open, complex, and urban terrain. We need the capability to conduct persistent surveillance operations across all spatial domains—sub-surface, surface, air, space, and cyberspace.

- ◆ **Warfighting functions.** Every system and individual connected to the network is a collector capable of supporting the persistent surveillance mission. No single sensor system, including personnel (Every Soldier as a Sensor) is a panacea for persistent surveillance.
- ◆ **Detect.** Threat detection and unambiguous identification requires more than good sensor data. Context information and historical background is equally important. You must know why and what you are looking for and in what spectrum a potential target operates. The continued development of signatures libraries across the entire electromagnetic, acoustic, and other spectrums is vital to the success of TPS.
- ◆ **Characterize.** Characterization is the ability to determine the nature of the detection and is linked to combat identification to include the ability to discern allegiance of the entity. Some characterization can be automated, some requires human involvement.
- ◆ **Locate.** Locate allows us to know precisely where the entity is in the OE. Detection and location are not synonymous.
- ◆ **Track.** Tracking is the ability to display or record the successive positions of a moving object despite natural obstacles or man made countermeasures.
- ◆ **Target.** Targeting allows us to link all necessary warfighting functions to prosecute the target—either lethally or non-lethally—as the commander and mission require.

## The Evolution of Persistent Surveillance

The strategic, joint, and service documents reviewed for this article primarily link persistent surveillance to operational and strategic concerns and typically focus upon space based and/or aerial platforms such as unmanned aerial systems (UAS). The published references (see complete list at the end of the article) inextricably link persistent surveillance to sensors supporting targeting and precision strike capabilities.

The key points of the reviewed documents are summarized below.

- ◆ The 2001 QDR introduced persistent surveillance as one of the six operational goals necessary to implement a new defense strategy.
- ◆ The 2006 QDR described persistent surveillance capability as “the ability of the future force to establish an unblinking eye over the battle space through persistent surveillance . . . future capabilities will support operations against any target, day or night, in any weather, and in denied or contested areas.”
- ◆ ISR efforts must be persistent across time; seamless across key geographic regions; take advantage of the most capable collection platforms; gather data across the information spectrum and benefit from cooperation and timely cross-cueing of national agency, overhead and sensitive reconnaissance assets.
- ◆ Persistent surveillance “ . . . needs to be integrated with those assets that fly, those that are on the ground and, indeed, with our **human intelligence** capabilities.”
- ◆ Tactical forces will benefit from the continued development of sensors operating in three dimensions that provide both temporary and persistent surveillance.
- ◆ While persistent surveillance is only achievable for specific periods of time against extremely critical targets, it is an essential capability for the future modular force.
- ◆ The 29 March 2007 *Joint Integrating Concept, Persistent Intelligence, Surveillance, and Reconnaissance (ISR) Planning and Direction*, shifts the terminology from persistent surveillance to persistent ISR to support “better unity of ISR efforts in support of the Joint Force Commander’s campaign plan.”

Since none of the capabilities described in the reviewed sources specifically point to tactical echelon support, the Army needs to define persistent surveillance to support tactical operations.

## Linkage between Persistent Surveillance and the AUTL

It is appropriate to focus our persistent surveillance discussion at the tactical level. A more tightly focused discussion on the performance of TPS missions does not diminish the essential interdependency of sensors at all echelons and in the joint environment.

**FM 7-15, Army Universal Task List (AUTL)**, provides a standard, doctrinal foundation and catalogue of the Army's tactical collective tasks. For the purposes of TPS, the most applicable AUTL task is Army tactical task (ART) 1.3.4 Conduct Surveillance. This task is a subtask of the larger ART 1.3 Conduct ISR.

Task 1.3.4 states that surveillance is the systematic observation of airspace, surface, or subsurface areas, places, persons, or things in the AO by visual, aural, electronic, photographic, or other means. Other means may include but are not limited to space-based systems, and using special chemical, biological, radiological, and nuclear; artillery; engineer; special operations forces, and air defense equipment. Surveillance involves observing an area to collect information.

Two key measures associated with this task are that surveillance assets collect required information and fulfill the duration of the surveillance until the priority intelligence requirement (PIR) is answered or the information is no longer of value.

## Persistent Surveillance Themes, Capabilities, and Limitations

The references provided at the end of the article, like most persistent surveillance discussions, focus almost exclusively on strategic and operational missions. Those references identify the following persistent surveillance capabilities and limitations.

These **nine** capabilities were highlighted in the aforementioned sources and predominantly focus on sensor and lethal solutions to support strategic and operational missions:

1. Deny enemies sanctuary by providing persistent surveillance, tracking, and rapid engagement with high-volume precision strike.
2. Find and strike protected enemy forces while limiting collateral damage.
3. Develop the means to deny sanctuary to potential adversaries for a specific mission, area, and time period.
4. Support long-range precision strike.
5. Extend across time, space, and information domains; resistant to determined denial and deception efforts.
6. Match the frequency of revisit with the time stability of the object that you are looking at—the speed with which things change.
7. Support operations against any target, day or night, in any weather, and in denied or contested areas.
8. Exploit the constellation of military and civilian space platforms for persistent surveillance.
9. Gain an understanding of the opponent and the OE continuously and in near real time to maneuver across strategic distances.

**Six** limitations were highlighted in the aforementioned sources:

1. Surveillance sensors (all services) are high demand/low density assets.
2. Commanders must prioritize and clearly define IRs and acknowledge risk in areas/objects not identified as priorities.
3. Achieved only for specific periods of time against extremely critical targets.
4. Dilutes efforts against other PIR and target priorities due to extended focus and allocation of sensors directed against one target.
5. Creates an ISR management challenge or requires a significant increase in force structure to employ sensors operating in three dimensions that provide both temporary and persistent surveillance.
6. Creates an analysis challenge—the vast increase in collected data and information will require an increase in the number of analysts.

## Making TPS Work—2007 to 2024 Assumptions

- ◆ Persistent conflict will result in an enduring environment of escalating local and regional conflicts.
- ◆ U.S. military operations will be subject to greater adversary ISR exploitation and targeting capability. Adversary ISR systems will access available commercial and military command and control (C2) and global positioning systems (GPS) to provide enhanced threat OE situational awareness.
- ◆ U.S. force protection will be increasingly challenged by adversary denial and deception.

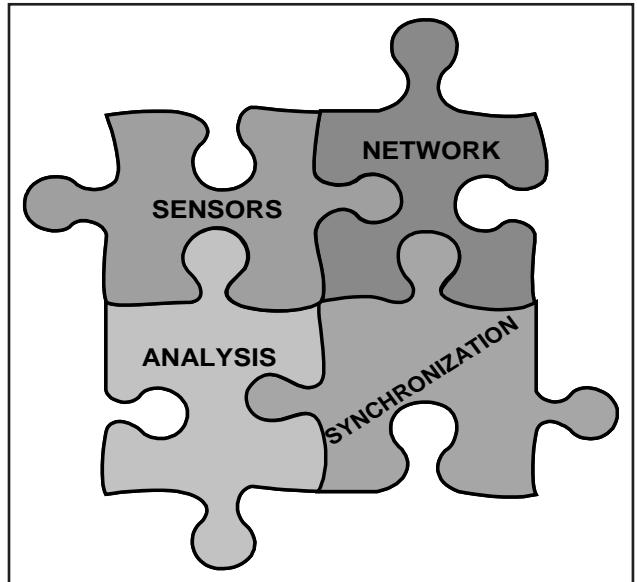
- ◆ Future modular forces will have the capability to conduct persistent surveillance in both permissive environments and denied areas.
- ◆ Assured communications are in place and survivable.
- ◆ An open sensor and analytic architecture, flexible enough to accept emerging technology, personnel changes and purpose-built plug-ins.
- ◆ Automation does not replace the requirement for analysts at the right echelon with appropriate skills, attributes, and tools.
- ◆ Federated analytical environment with system flexibility to conduct analysis operations in the OE and/or from a Home Station Operations Center (HSOC).
- ◆ Partially automated or assisted fusion Level 2 capability in 2024.
- ◆ Current programs of record (PORs) arrive on schedule and work in accordance with requirements Distributed Common Ground Station-Army (DCGS-A) and Aerial Common Sensor (ACS).
- ◆ Innovative and technologically advanced surveillance means identified and under development.
- ◆ Everything on the network becomes a sensor (i.e., Soldiers, laser range finders, smart weapons).
- ◆ Focus on the “sensor to decision maker to action” not just on “sensor to shooter.”

### Risks.

- ◆ Surveillance trade-offs and consequences are required to accomplish the persistent surveillance mission.
- ◆ Unanalyzed information due to imbalance between the information collected and overloaded processing and human analytical capability. This problem will increase as we continue to add sensors and sensor systems to the intelligence enterprise.
- ◆ Increased U.S. military budget pressures may result in diversion of resources necessary to accomplish the research, personnel support and system fielding for TPS.

### Requirements.

- ◆ The four elements required for effective TPS missions are: assured network connectivity, analytical support, integrated sensor capability, and ISR/RSTA synchronization.
- ◆ Resource commitment for an assured, robust communications network to support netted sensors, massive information flow and analyst reach to support decisions measured in seconds and minutes.
- ◆ A vertical and horizontal integration strategy to acquire and apply collection assets that integrates surveillance capabilities across all intelligence disciplines and national, theater, tactical, and commercial programs.
- ◆ Match requirements for processing, exploitation and dissemination tools with new sensor requirements.
- ◆ Commitment to research, development, and experimentation, as we identify and explore new signatures and survey baselines across all spectrums.
- ◆ New sensor fusion paradigm. Fully automated fusion is not a near-term probability as initially envisioned. This will require more analysts as we gain access to more information through sensor integration and synchronization, better sensor capability, better processing, and network expansion.
- ◆ Increased manned and unmanned sensor integration to provide the optimum coverage at the lowest overall cost and risk.
- ◆ Better exploitation and integration of existing knowledge to include: civil and non-government agencies; indigenous, allied and coalition sources; and cultural social, and religious factors.



**Figure 1. Elements of TPS.**

- ◆ Seamless C2 system. A C2 system that makes warfighting functions transparent to each other to facilitate the exchange of information. All surveillance assets would be visible and their availability to conduct surveillance missions clearly displayed. Dynamic re-tasking of assets and the resulting collection impacts are displayed for the commander.
- ◆ Analytic cadre capable of analyzing the data and extracting knowledge from TPS.

## **The Way Ahead: Ever evolving synchronization, assured network, analytical support, and innovative sensors.**

In the future modular force, Army intelligence will continue to synchronize multi-discipline collection, integrate processing and reporting across all warfighting functions, and improve access of data from all available sources. The future modular force will be day-night, all-weather sensor capable with access to a wide array of intelligence and analytic capabilities using a network-centric enabled enterprise environment. The TPS mission will be accomplished by continually enhancing the ISR support to an operation. As the operation matures, the ISR synchronization and integration, sensor availability and capability, and analytic capability matures at an equal pace to provide all the necessary elements of TPS (See Figure 2). The success of the future modular force brigade combat team (BCT) depends significantly upon the integration of ISR capabilities at all echelons, and the capability to provide tactical persistent surveillance and exploitation of the area of operations.

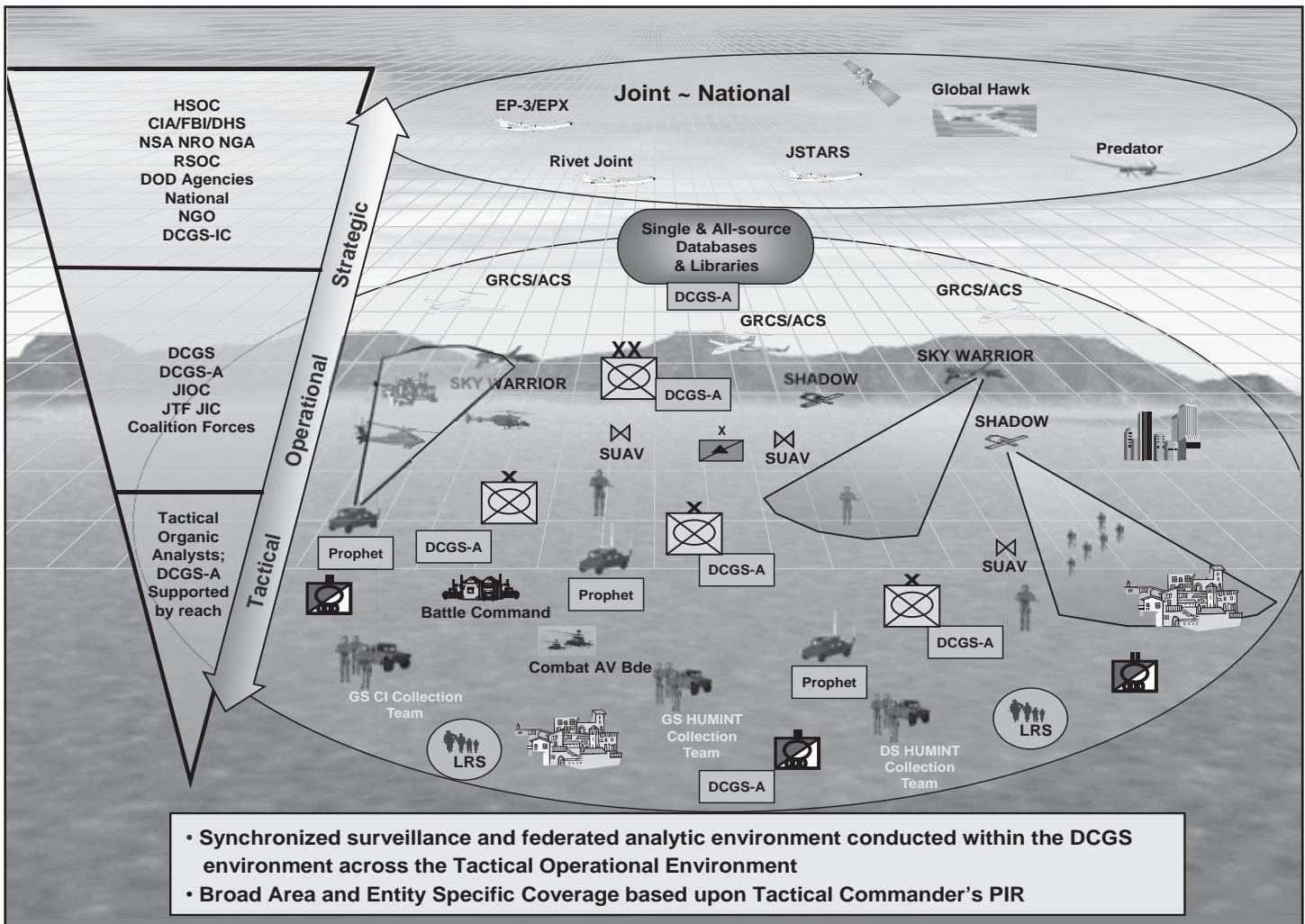


Figure 2. Tactical Persistent Surveillance.

## **Near-Term: Supporting the Current Fight**

In current doctrine, surveillance complements reconnaissance by cueing the commitment of reconnaissance assets against specific locations or targeted enemy units. Persistent surveillance supports the tac-

tical commander by maintaining contact to either prosecute a target or to continue surveillance to further develop information, signatures and other characteristics associated with the target. Effective TPS in the near term requires integrated, synchronized, sensor surveillance in conjunction with innovative processing, analysis, and dissemination. Current TPS capabilities and recommended near-term initiatives are listed below.

### **Synchronization.**

- ◆ DCGS-A V2/V3 provides greater access for analyst and commander to sensor data/reporting, with enhanced analysis tools, not found in current systems. DCGS-A V3 provides the brigade intelligence staff multi-functional collaborative capabilities and tools while improving the synchronization between the current systems.
- ◆ Sustain current collection and network architectures to support deep and austere intelligence requirements. Maintain ability for data exfiltration.
- ◆ Conduct a complete sensor capability analysis across all warfighting functions to identify critical gaps and seams in sensor coverage.
- ◆ Be informed by the success and failures of Task Forces ODIN and Lightning.
- ◆ Train and educate commanders, sensor operators and analysts.
- ◆ Improve employment of multiple intelligence disciplines: Human Intelligence (HUMINT); Signals Intelligence (SIGINT); Imagery Intelligence (IMINT); Measurement and Signatures Intelligence (MASINT); Technical Intelligence, Counterintelligence, etc.) against a specific surveillance target (individual object, system, or network) in order to:
  - ◆ maintain sensor contact with the target as environmental constraints or the target's behavior dictate.
  - ◆ gain a greater understanding of all aspects of the target.
- ◆ Focus collection capability to maximize situational awareness.
- ◆ Enhance collection management tools to allow the commander to visualize and direct ISR operations making ISR assets responsive to the commander's need for information.
- ◆ Pursue more extensive manned/unmanned teaming to employ unmanned platforms in high threat environments or to conduct repetitive tasks or tasks requiring long dwell times.

### **Network.**

- ◆ Warfighter Information Network-Tactical (WIN-T), TROJAN, Joint Network Node (JNN), Joint Tactical Terminal (JTT), satellite communications (SATCOM).
- ◆ Localized radio frequency to provide local direct support to units on the ground.
- ◆ Develop a robust, assured communication capability—necessary to link all sensors and analysts, support reach operations, enable the flow of information to commanders and leaders at all levels, provide capability to store and retrieve critical data.

### **Analytical support.**

- ◆ DCGS-A (V2/3) provides computer assisted correlation, link analysis tools, query support, information retrieval and visualization.
- ◆ Guardrail Ground Baseline (GGB): ground element of the Guardrail Common Sensor (GRCS) system that provides 24-hour processing capability of the Communications Intelligence (COMINT) and Electronic Intelligence (ELINT) data collected by all current and future SIGINT payloads of the RC-12 aircraft. Provides real-time geo-location and facilitates maneuver and direct engagement of discrete enemy formations and targets.
- ◆ Effectively leverage national and strategic enclaves to assist tactical decision processes.
- ◆ Maintain operational familiarity with HSOC and the supported tactical commander.
- ◆ Leverage national topographic products, in the detail required, to support tactical operations to include terrain profiling and mapping products.

- ◆ Pursue sensor grid and analytical support that dynamically evolves from forensic analysis to predictive analysis.
- ◆ Pursue pattern analysis system that processes feed from multiple sensors and compares that information against activity threshold values.
- ◆ Enhance analysis tools to provide greater access to sensor data/reporting.
- ◆ Research and development funded for fusion Levels 3-5 (ability to interpret, determine, predict, assess and review entire process of sensors, collectors, analysts, and staffs).

### **Sensors.**

- ◆ GRCS—provides day/night all-weather airborne SIGINT collection and analysis capability for assured, timely, accurate, and responsive actionable intelligence support and targetable information to tactical commanders across the full spectrum of military operations
- ◆ Aerial Reconnaissance-Low (ARL)—provides day/night all-weather airborne SIGINT collection and analysis capability; COMINT, ELINT, and MASINT collection capabilities simultaneously employed against separate targets and fused with IMINT sensor data acquired from unmanned aircraft systems (UAS) or other sensors to provide an integrated view of a single target; sensor to sensor cueing for immediate servicing of targets.
- ◆ UAS—short-range airborne reconnaissance system electro-optic/infrared (EO/IR) payload provides day/night, multi-sensor collection system; near real time intelligence data.
- ◆ MASINT—maintain and improve national collection capabilities to address scientific exploitation. Continue to leverage tactical MASINT capabilities in ground sensing technologies.
- ◆ HUMINT maintain operations to provide digital photos, video, scanned documents and interpreted text.
- ◆ Tethered aerostat surveillance systems to provide continuous broad area surveillance, threat detection and communications support to a wide deployment area.
- ◆ Identify currently employed effective quick reaction capability (QRC) surveillance capabilities to augment existing PORs.
- ◆ Enhance biometric capability to capture, access, and archive key personal data.
- ◆ Expand Human Terrain Team initiatives and their capability to archive and disseminate interrogation and source reports.
- ◆ Link unattended ground sensors (UGS) to provide extended, undetected collection data.
- ◆ Develop persistent detection capability to support force protection and intelligence.
- ◆ Pursue the ability to support urban military operations by observing structure compositions and dispositions.
- ◆ Pursue automatic detection, system cueing and correlation of sensors to provide terrain model enabled sensor data.
- ◆ Develop common geospatial reference for all networked entities.
- ◆ Integrate sensor suite with multi-sensor to enable Soldiers to detect, recognize, identify and geolocate distant targets while remaining outside the threat's acquisition and engagement envelope.

### **Mid-Term (2009-2014): Affecting Tomorrow's Fight Today**

Emerging technologies will continue to improve the capability of sensors at a faster pace than the ability to efficiently analyze and exploit the collected data. The anticipated technological advances will not replace human beings during this period. Advances predicted in automated, fused capabilities have not developed to the level initially anticipated. The information environment will continue to overwhelm the ability of human analysts to absorb all available data, detect patterns or develop an enhanced level of understanding about the OE. The fluid OE combined with ever-compressed decision cycle times will continue to stress decision makers searching for key, discrete, elements of information upon which to make good decisions. We can mitigate this situation to some degree in the following areas:

## **Synchronization.**

- ◆ Implement DCGS-A V4 designed to improve the ability to synchronize the management of information and intelligence, expand access to available theater and national resources, and build upon previous analytical capabilities.
- ◆ Synchronization, cueing, and modularity of sensors; maturing of sensor availability and capability in the OE; increased sensor duration, survivability and dwell.
- ◆ Develop ability to track targets in spite of natural obstacles or adversary countermeasures.
- ◆ Provide interactive access to ISR plans at all echelons; tailor able at all levels, with visibility of all collection asset locations, commanders' information needs, and collection results.
- ◆ Layer technology to align data from multiple sensors: EO; video; synthetic aperture radar (SAR); sonar, hyperspectral, and laser induced differential absorption radar (LIDAR) to a geo-coordinated position.
- ◆ Dynamically adjust the revisit rate of the collection capabilities to meet the commander's requirements.
- ◆ Enhance simulation environments and tools to familiarize and train commanders and staff with ISR capabilities before they have to use them in real operations.
- ◆ Robust research and development programs to accelerate the automated fusion of information.
- ◆ Exploit commercial technology center advances in collection and fusion (U.S. military battle labs, Communications-Electronics Research Development and Engineering Center (CERDEC), and Defense Advanced Research Projects Agency (DARPA).
- ◆ Pursue reinforcing platform architecture to integrate sensor data from multiple sensor platforms to provide on-demand intelligence to multiple users.

## **Network.**

- ◆ JTRS, JNN, TROJAN, JTT, Integrated Broadcast System (IBS)
- ◆ High Altitude Long Loiter (HALL) communications relay capability to move high volumes of data over tactically relevant distances on the move.

## **Analytical support.**

- ◆ DCGS-A V4 designed to provide computer assisted: link analysis tools, assisted query support, information retrieval and visualization, and object aggregation. Will introduce semi-computer controlled correlation and continue to provide user defined alert notification.
- ◆ Review and determine the appropriate skill and task set to enhance the ability for analysts to mature into situational awareness specialists.
- ◆ Review intelligence analyst allocation and distribution to mitigate some of the information overload.
- ◆ Pursue exploitation and analysis tools that receive direct feed from their respective sensor subsystem and that allow analysts to conduct real-time data assessment for immediate re-tasking or feedback to the tactical commander.
- ◆ Enhance reach capability and capacity to HSOC and analytical support centers.
- ◆ Pursue systems that receive multiple data feeds, fuse the data, and allow selective dynamic sensor re-tasking for immediate focus upon targeted activity.
- ◆ Pursue automated object recognition by computers.
- ◆ Migrate proven visualization capabilities to mitigate the information flow.
- ◆ Pursue Level 1 and 2 fusion to develop situational awareness and understanding object relationships to each other and the environment.
- ◆ Leverage the National Signatures Program (NSP) to accelerate standardized target signatures and feature vectors to provide reliable characterization and identification of specific OE objects.

## **Sensors.**

- ◆ Develop re-locatable entity tracking capability.
- ◆ Team UGS with selected upgrades of sensor suites on manned airborne platforms. Improve ground

sensing capabilities as Future Combat System (FCS) spin out technologies mature and are enhanced by the net centric architecture.

- ◆ Refine coherent change detection (CCD) capability that detects changes between sensor imaging passes and measures direction or magnitude of change.
- ◆ Continue netting of existing systems and the initial research and development necessary to develop sensors capable of detecting, either actively or passively, entities within new areas of the various spectrums.
- ◆ Enhance extended range/multi-purpose UAS to provide EO/IR and laser designator (EO/IR/LD), SAR, Ground Moving Target Indicator (GMTI) sensors, improved modular ground control stations (IMGCS), communications suite, and ground support equipment (GSE).
- ◆ Standardize the current QRC capability to use existing sensing technologies and achieve extended range data exfiltration enhanced by a standardized data structure and data archival system.
- ◆ See through the wall capability-to detect, locate, track and target individuals and vehicles in an urban OE.
- ◆ Pursue LIDAR sensors.
- ◆ Refine hyperspectral sensors.
- ◆ Refine High Resolution SAR imagery.

## **Long Term (2015+): Information Exploitation and Sensor Innovation is the Future Synchronization.**

- ◆ Field DCGS-A V5 designed to provide limited automated fusion while integrating with PORs, ACS, and other ground stations. It will operate on the enterprise network and be integrated with battle command capabilities.
- ◆ Identify and migrate proven technologies (sensing, processing, data exfiltration and fusion) to Army Material Command for accelerated exploitation and development.
- ◆ Pursue sensor resource management systems to electronically steer array radars. The radar's agile beams can be steered on a dwell-by-dwell basis to any point in the field of regard and have multiple modes: GMTI, high-range resolution, SAR, inverse SAR, interferometric SAR, CCD.

## **Network.**

- ◆ Enhance network assurance and refine capability to provide the reach, capacity, and survivability necessary for the Army to operate in all environments, reduce deployed footprint and conduct full spectrum operations.
- ◆ Evolve the transport layer capability to accommodate the exponential increase in data collected by improved sensor platforms and to link all sensors and all analysts at all echelons.
- ◆ Refine and implement network technology to achieve miniaturization, power management savings, extended data exfiltration, faster processing time, and data throughput (bandwidth).

## **Analytical support.**

- ◆ Achieve Level 2 automated fusion. This capability likely provides the largest technological hurdle we will face but is essential to successfully leverage (process and analyze) the vast amounts of information from future sensors. Automated fusion equates roughly to thinking machines with the ability to reason. Level 2 fusion will be a combination of automated and cognitive processes. The output of Level 2 fusion is a more complete set of battlefield objects that are aggregated and linked together either via observation or inference plus an assessment of current activities and behavior.
- ◆ Vastly improved information exploitation capabilities that free analysts and warfighters from processing data reports so that they can focus on evaluating potential threats.

## **Sensors.**

- ◆ Continue to expand the development of the NSP to incorporate the emerging sensing technologies. This will allow for adaptation to the asymmetric threat and enhance current capabilities.

- ◆ ACS designed to provide a day/night all-weather multi-intelligence airborne collection and analysis capability.
- ◆ Pursue ability to transition from a covert to an overt collection posture to accelerate the characterization and identification of targets.
- ◆ Pursue multiple means of sensor dispensing devices and platforms to maximize area coverage.
- ◆ Pursue sensing techniques that are not degraded by environmental conditions.
- ◆ Pursue a constellation of urban UASs with a high resolution sensor footprint that detect insurgents and their infrastructure and track tags.

## **Conclusion**

A critical aspect of TPS is the ability to rapidly bring to bear sensors, processing and analysis and to maintain sensor contact with targets in a rapidly changing, asymmetric, complex tactical environment. The tactical commander requires the ability to dynamically re-task and cue sensors and information feeds in *real time or near real time*. The sensors and analysts must be able to rapidly support both the generation and assessment of lethal and non-lethal effects. Success in the contemporary and future OE will be measured in seconds and minutes not hours, days or weeks.

Effective TPS in the near term requires employment of current capabilities in innovative ways. TPS relies on the integration and synchronization of sensors with dynamic processing, analysis, and dissemination capabilities. Ongoing refinement, testing, and field implementation of collection and asset management tools must continue to support the current fight. To achieve a reliable, effective TPS capability, we must devote resources, research and development to improve synchronization and integration tools, establish an assured network, improve sensor networking, improve analytical support, and develop innovative sensors.

The resources required to explore new sensor capabilities across all spectrums, dwell time, and counter-measure attenuation must be identified and committed. Equally important, the investment in our analysts must be sustained in quality as well as quantity. These analysts will be augmented by increased automated processing capabilities. Someday we will reach a fully automated fusion capability that allows us to reduce our reliance on human analysis, but this is a long way in the future. For the present and foreseeable future, all warfighting functions remain dependent on the human element to make sense of the increasingly vast quantities of information available from both current and future advanced sensor systems.

There is a risk that as the current operation concludes or decreases in intensity the available resources may decrease as DOD shifts emphasis to other areas of concern. In anticipation, we should recognize potential future resource limitations and allocate the available resources to best support our prioritized, anticipated needs.

The definition for TPS, if accepted, and reconciled with the current body of combined arms and intelligence doctrine, will allow the Army to establish a common doctrinal baseline from which to explore the DOTMLPF implications of persistent surveillance. A TPS definition and baseline brings us one step closer to an integrated, synchronized sensor system supported by an assured communications network and robust analytical support focused on the tactical commander's requirements.



### **References:**

DOD QDR 2001, 30 September 2001.

DOD QDR 2006, 6 February 2006.

President of the United States, National Security Strategy of the United States, September 2002.

Director of National Intelligence, National Intelligence Strategy of the United States, October 2005.

Chairman of the Joint Chiefs of Staff, National Military Strategy, 2004.

U.S. Army Training and Doctrine Command (TRADOC) FY 2008 Army Concept and Capability Development Plan (AC2DP).

TRADOC Pamphlet 525-3-1, The Army Operating Concept for Operational Maneuver 2015–2024, 2 October 2006.

TRADOC Pamphlet 525-3-2, The Army Operating Concept for Tactical Maneuver 2015–2024, 2 October 2006.

TRADOC Pamphlet 525-2-1, The U.S. Army Functional Concept for See 2015–2024, 30 April 2007.

TRADOC Pamphlet 525-3-6, The U.S. Army Functional Concept for Move 2015–2024, 30 April 2007.

TRADOC Pamphlet 525-3-5, The U.S. Army Functional Concept for Protect 2015–2024, 30 April 2007.

TRADOC Pamphlet 525-3-4, The U.S. Army Functional Concept for Strike 2015–2024, 30 April 2007.

TRADOC Pamphlet 525-4-1, The U.S. Army Functional Concept for Sustain 2015–2024, 30 April 2007.

Defense Authorization Request for FY 2005 Senate Committee On Armed Services: Strategic Forces Subcommittee, Dr. Stephen A. Cambone, Under Secretary of Defense for Intelligence testimony April 7, 2004.

Military Transformation: A Strategic Approach, Fall 2003.

JP 1-02, DOD Dictionary of Military and Associated Terms 12 April 2001, as amended through 1 March 2007.

FM 2-0, Intelligence, 17 May 2004.

FM 3-0, Operations (Post DRAG Draft).

FM 7-15, Army Universal Task List, 31 August 2003.

Joint Functional Component Command, Joint Integrating Concept v 1.0, “Persistent ISR Planning and Direction”, 29 March 2007.

Director of Combat Developments, USAIC & Fort Huachuca, Fusion White Paper, 6 July 2004.

Joint Forces Command, Persistent ISR Functional Area Analysis, 25 June 2007, V 0.19.

*Marty McCleary is currently the ISR Division Chief, Concepts Development Directorate, U.S. Army Intelligence Center and Fort Huachuca. Mr. McCleary is a retired Armor officer with 20 years of service.*

*Richard Smith is currently the Deputy Director, Concepts Development Directorate. Mr. Smith is a retired Army officer with 28 years service as an enlisted man, noncommissioned officer, and commissioned officer. Mr. Smith served in the Infantry, Artillery, and Military Intelligence career fields in the Marine Corps, National Guard, Army, and Army Reserve.*

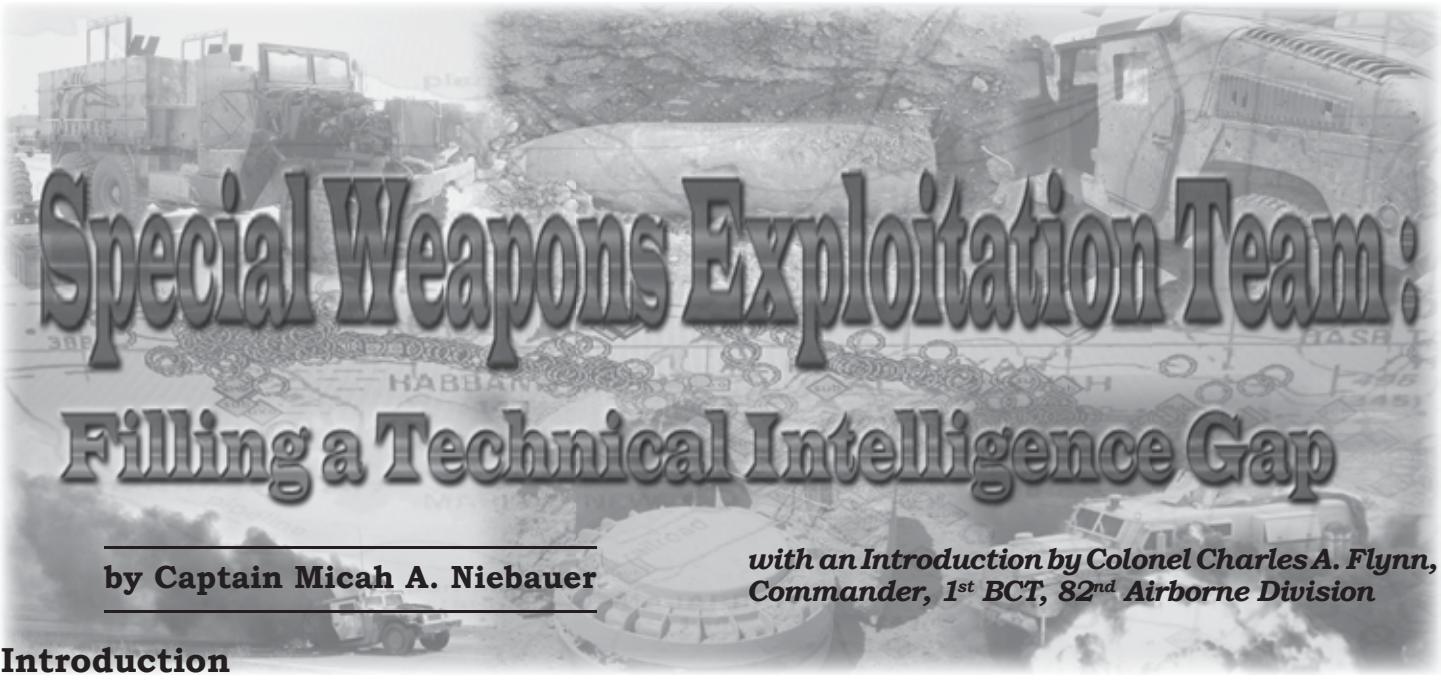
*Colonel Sharon Hamilton is currently Director, Concepts Development Directorate, Colonel Hamilton commanded the 344th MI Battalion and served in a variety of tactical, operational, and strategic MI positions during the past 23 years.*

## MI LEGACY

---



The Lens Stereoscope provided a three dimensional view of an image. It was low cost, compact, and portable



# Special Weapons Exploitation Team: Filling a Technical Intelligence Gap

---

by Captain Micah A. Niebauer

---

*with an Introduction by Colonel Charles A. Flynn,  
Commander, 1<sup>st</sup> BCT, 82<sup>nd</sup> Airborne Division*

## Introduction

War creates uncertainty and friction of enormous scale. Throughout history examples indicate that numerous nations and militaries struggled to match capabilities and resources as they attempted to anticipate the needs of the next fight. In fact, it could be argued that identifying your opponent's most effective weapon systems before an operation, battle, or war may be the single most difficult task. In the opening chapters of the War on Terror that pitted us against radical extremists employing the full range of asymmetrical threats, it can be argued that not only was the U.S. Army, and the broader Department of Defense (DOD), ill-prepared for improvised explosive devices (IEDs), we were completely surprised at its lethality and the various means of employment. An admission of this unpreparedness is displayed in the development of the Joint Counter IED Task Force in 2004, and its eventual expansion to JIEDDO with a 2008 budget of roughly \$4.4 billion.

In today's fight our opponent's weapon of choice is the IED—in whatever form of delivery. This weapon has become an insurgent or terrorist's modern low cost form of precision guided munitions. While its physical aim is to kill and maim, its broader aim is to achieve psychological effects against Troopers as these types of attacks cast an even wider net, gaining immediate enemy information operations successes at home as they grab media headlines. One small blast can strike fear across the globe, an IED can have enormous operational and strategic reach. Given those considerations, tactical units have tried

and been provided various Joint, interagency, organizational, and technical solutions. Some of these have been very helpful but given our unique missions set and operational environment, 1<sup>st</sup> Brigade Combat Team (BCT), 82<sup>nd</sup> Airborne Division was forced to do something different.

In July 2007, the 1/82 BCT began to develop and design a capability resident within the BCT to work for the Commander to counter and exploit a wide range of enemy attacks. This capability was designed using a group of Troopers with varying military occupational specialties (MOSSs), talents, and experiences. Team members had to be selected, sent to technical schooling, provided equipment, and given facilities for them to perform and meet the needs of the command and commander.

As you will see in this article, the Special Weapons Exploitation Team (SWET) is an internally resourced BCT capability that is responsive to the commander and his priority intelligence requirements. A SWET can be designed and developed by every BCT and we would advocate that position. Further, we'd argue that that this capability should be considered as an MTOE modification as we look to refine the original design of the BCT. The IED in its various forms will become more sophisticated as our opponents attempt to defeat our countermeasures, we are already seeing signs of this with deep buried and explosively formed penetrators. Therefore this well led, farseeing, and thinking countermeasure is better than any technical solution. Of that I'm convinced.

## **What is the Need?**

The increasing sophistication and rapid evolution of weapon systems at the tactical level makes the creation of Technical Intelligence Cells (TICs) a crucial priority for the U.S. Armed Forces. The institutionalization of TICs will empower the Army to counter the enemy's threats with a more effective strategy. To ensure the success of TICs, the Army should make teams a formal capability as far down as the battalion level, but definitely at the BCT. While the job of Technical Intelligence (TECHINT) at the tactical level is currently being conducted by Weapons Intelligence Teams (WIT) in the Iraq and Afghanistan Theaters of Operation, presently no such organization exists outside of Theater. This becomes a significant shortfall as we learn, sustain, retrain, and integrate forces and capabilities for the fight; we need to train and refine these capabilities continuously, not just upon arrival to the combat zone.

Shortly after arriving in Iraq and not having the support of a WIT, the 1/82 BCT formed an internal brigade WIT which was designated as the Special Weapons Exploitation Team (SWET). The SWET's impact not only benefited the brigade during this deployment, but will continue to play an integral role during home station training as well as all future deployments. As the Army approaches a decision whether to fund TICs, the experience of 1/82 BCT SWET provides evidence that TICs would give commanders a valuable asset. It places, within the BCT, a capability that can analyze enemy effects, but more importantly counter threat weapons/tactics in the complex combat environments of today and tomorrow.

## **Evolution of Technical Intelligence**

*"After the insurgency began in Operation Iraqi Freedom . . . the need arose at the tactical level for technical intelligence experts on IEDs to collect, analyze, and defeat these systems."*

**Joint Publication 1-02, DOD Dictionary of Military and Associated Terms**, defines TECHINT as "Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and material for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages." Since the onset of Operation Iraqi Freedom (OIF), the

Army's focus on TECHINT has shifted considerably from the Cold War days. During the Cold War, the Army's TECHINT focus dealt with the large, Soviet Bloc weapon systems. Developments of these systems took place over a significant amount of time and were large, national projects. Only one unit in the Army, the 203<sup>rd</sup> MI Battalion, provided TECHINT and that was deemed sufficient given the threat assessment at that time. After the insurgency began in OIF, the weapon of choice became the IED, a smaller and less complex weapon. Nonetheless, these weapon systems were continually evolving, and the need arose at the tactical level for TECHINT experts on IEDs to collect, analyze, and defeat these devices.

In early 2004, the National Ground Intelligence Center (NGIC) was tasked with countering the rising threat of IEDs, and created the Counter IED Targeting Program (CITP) to collect technical intelligence and conduct analysis of IEDs to support the targeting of insurgent networks. CITP in turn created six WITs and deployed them to Iraq to conduct initial exploitation and analysis of devices before sending recovered materials up to higher agencies for further examination. The first deployment of WITs was a success, and since then, the Army has put in a request for forces of one team per deployed brigade. While the first rotation of teams consisted of Army personnel, the five person teams since then have consisted of four Airmen and one Soldier. The teams include an Explosive Ordnance Disposal (EOD) Technician, two Intelligence Analysts, a Crime Scene Investigator, and a Combat Arms Soldier. The Airmen and Soldiers that make up these teams train together in the States before deploying on a twelve month rotation. Their reporting provides valuable information both to the brigades they support as well as to Theater and National level intelligence agencies. The successes of these teams in Iraq have laid the framework for a more permanent TECHINT solution in the Army.

## **Meeting an Operational Need**

*"Not having a WIT meant that the BCT rarely received valuable data from IED incidents . . ."*

After deploying to southern and western Iraq in support of OIF in June of 2007, 1/82 BCT (ABN) was tasked with the Theater Security mission. As a part of that mission we secured and escorted large convoys from Kuwait and Jordan into Theater. Due to its mission, 1/82 BCT was not assigned a

WIT and the closest equivalent, a British Weapons Intelligence Section, was located at such a great distance that it was often unable to respond to IED attacks. Moreover, not having a WIT meant that the brigade rarely received valuable data from IED incidents, to include construction, emplacement techniques, and likely enemy over watch locations. The 1/82 BCT leadership decided to create its own organic WIT called the SWET to help fill the inherent organizational deficiency in TECHINT.

## Special Weapons Exploitation Team

*"A distinctive aspect of the 1/82 SWET is that the BCT will retain the same knowledge and capability upon redeploying to Fort Bragg, North Carolina."*

1/82 BCT created the SWET with Soldiers of several MOSs from within the BCT. An Infantry officer was selected as Team Leader to provide tactical analysis of why attacks occurred in the locations they did. An MI Analyst was selected to fuse reports in with the rest of the BCT S2 section, helping to provide an All Source Intelligence report on every attack that was then disseminated throughout the intelligence community. One Sapper-qualified Engineer provided explosives knowledge and worked closely with the EOD Team. A Military Policeman (MP) was in charge of scene investigation, evidence handling, and gathering biometric data. Two civilian Law Enforcement Professionals (LEPs) employed by Military Professional Resources Inc. also conducted scene exploitation as well as helping with analysis and targeting efforts. An interpreter with a Secret clearance was assigned to the team which greatly aided in questioning local nationals on the scene to aid in the investigation. What made the team truly versatile was the addition of a security element that provided mobility for the SWET. Normally WITs are reliant on other units for transportation and are often limited in the time they have to investigate and gather evidence. Not only could the SWET respond to any attack without needing separate escorts, the BCT was able to use the team for a variety of missions. As many as 28 Soldiers were on the team at one time, making for a much more robust force than the five traditional members of a WIT.

Crucial to the success of the SWET was the ability for the core members to attend the Weapons Intelligence Course conducted by the 203<sup>rd</sup> MI Battalion at Aberdeen Proving Ground, Maryland. Members of NGIC were informed that 1/82 BCT was

attempting to stand up a WIT capability, and they provided the opportunity for 1/82 BCT to send five personnel to Aberdeen. The course taught the basic weapons intelligence mission, as well as sections on TECHINT and biometrics. The course fully enabled a diverse group of Soldiers to conduct the initial exploitation and analysis of insurgent attacks that had been missing in the brigade.



A Biometrics practical exercise during the Weapons Intelligence Course.

The SWET's mission set largely mirrors that of a traditional WIT, but with additional capabilities due to its size. The basic missions are grouped into three categories: reactive, proactive, and training. The reactive missions largely focus on IED attacks due to their frequency. Whenever there are IED discoveries or detonations, the SWET responds to the scene and secures it with the on-scene commander. In many cases, the on-scene unit is able to hand over security completely to the SWET and continue on its mission, allowing it to maintain its tempo. A second reactive mission is to locate and exploit indirect fire attacks. Not only does the team move to the points of impact and gather fragmentation from the rockets, but the team also has the capability to move to the points of origin and exploit evidence left by the insurgents. A third mission that the SWET conducts is exploitation of caches found by Coalition forces or turned in by the local populace. In all of these reactive missions, the focus is to

collect the evidence, conduct analysis of the event, report the findings, and then send the materials off to agencies that conduct more detailed analysis like the Combined Explosives Exploitation Cell.



Photographing the site of a recent IED detonation.

The proactive missions the SWET conducts include Tactical Site Exploitation during raids as well patrolling throughout the BCT's area of operation (AO). When conducting Tactical Site Exploitation, the SWET goes onto an objective once it is secure and gathers evidence from the scene. The Weapons Intelligence Course trained students on the proper way to assess, prioritize, and exploit the scene within the time constraints of the operation. With knowledge gained at the course, the team was able to quickly gather evidence, document it, and preserve it for further exploitation after the mission. Beyond conducting Tactical Site Exploitation, the SWET is also used to conduct route security patrols, sniper emplacements, as well as other intelligence, surveillance, and reconnaissance missions for the brigade. The team also participates in a number of programs run out of the Multi-National Corps-Iraq's Special Technical Operations section which has proven to be a complementary effort. It is apparent that SWET is a significant combat power multiplier to a BCT.

The final mission the SWET conducts is training for both Coalition Forces and Iraqi Security Forces (ISF). The training consists of IED awareness classes as well as site exploitation classes. All Coalition Forces receive IED training prior to arriving in the theater as well as some classes once they arrive, yet every area of the country has IEDs with unique features and different attack profiles. As these threats continue to evolve, the SWET is able to keep com-

manders and units informed of enemy weapons and tactics so that they are able to effectively counter them. Training takes place at quarterly conferences attended by leaders throughout the BCT, via daily battle update briefs when new threats emerge, as well as when new units arrive and want to know what they will face in their AOs. Of great significance is the training conducted with the ISF to help further increase its capabilities. The SWET works not only with the Iraqi Army EOD Team, but also conducts training for regular soldiers who face many of the same perils that U.S. soldiers face on a daily basis. These efforts effect great progress towards ISF and Coalition Force partnership objectives.



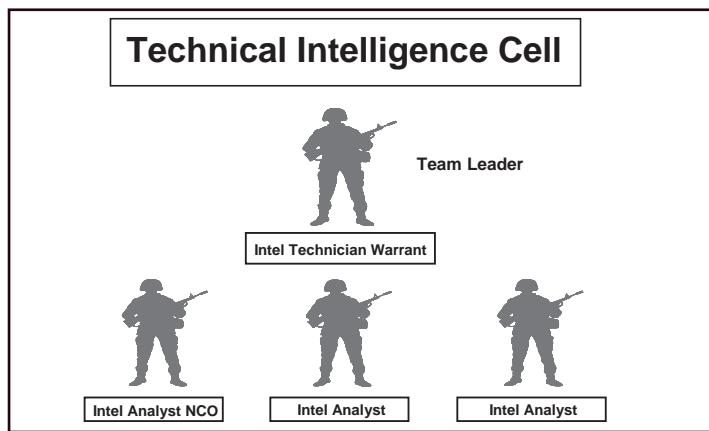
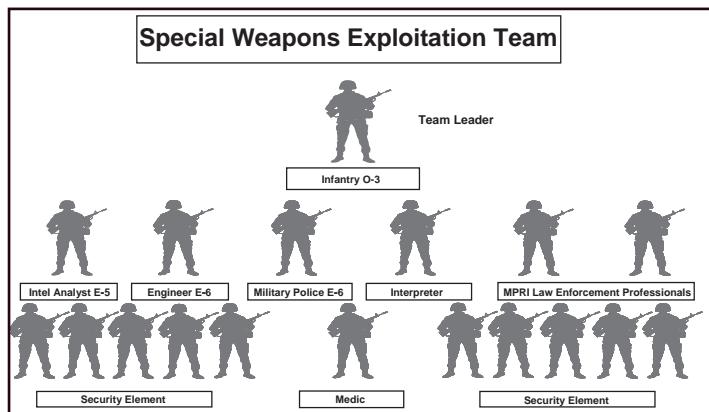
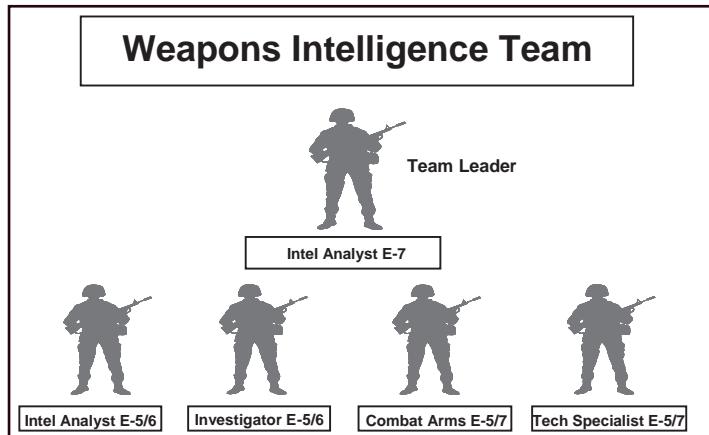
A class on IED Awareness is presented to an MP company in the 10<sup>th</sup> Iraqi Army Division.

## Maintaining this Capability is Critical

While these missions have many similarities to the WIT missions, a distinctive aspect of the 1/82 ABN SWET is that the BCT will retain the same knowledge and capability upon redeploying to Fort Bragg. Whereas normal WITs exist only temporarily in Iraq or Afghanistan, the planned permanence of the SWET in 1/82 ABN will provide many unparalleled and enduring benefits. Upon redeployment, the SWET capability will be retained within the BCT by keeping the WIT-trained members active in their positions—most as an additional duty at the BCT level. The skills they gained and the lessons learned will create an institutional body of knowledge. The SWET will not only be able to conduct training events as a team, but also plan training events for the entire BCT on site exploitation, biometrics, and IED awareness. The training will keep the skills of the SWET members sharp and also give them a rap-

port with the units they will be supporting. When major field training exercises or mission readiness exercises occur, the BCT will be able to reconstitute the team with a security element so they can train as they fight. Lastly, the SWET members will be able to stay linked to TECHINT intelligence reports coming out of theater and keep the unit informed of major developments in enemy tactics.

While 1/82 ABN's SWET is an internally resourced solution to an institutional shortage in the Army, there are currently plans well underway that could make similar teams a permanent asset in our military.



## Technical Intelligence Cells

*"A significant benefit TICs would bring about is the creation of a professional discipline of TECHINT in the Army."*

The U.S. Army Intelligence Center has proposed the establishment of TICs to create an enduring TECHINT capability at the brigade, division, and corps levels. Their mission would be to enable commanders to counter high-priority threat tactics and weapons systems and defeat the enemy's use of these weapons and tactics. Designed as a low density asset, the two primary functions will be expert TECHINT analysis and collection. TICs would be based out of the S2/G2 and comprised of three MI Analysts with a Warrant Officer in charge. Each echelon would have a different TECHINT focus—the lowest levels would focus on collection and initial analysis, while the higher echelons would provide further analysis and reach back to higher agencies for exploitation and support.

One major improvement that TICs will bring is that their focus will be on the greater TECHINT mission and not just IEDs. Currently, WIT training is centered on defeating IEDs as this weapon presents the greatest threat. As weapon systems change in our current or future conflicts, the success of TICs will depend on the ability to shift focus and deal with new and emerging threats. While the doctrine is still being developed, these teams would focus on the methodology and process of TECHINT and apply them to the weapons and tactics they face.

Another significant benefit TICs would bring about is the creation of a professional discipline of TECHINT in the Army. Currently there is no official training or career path in this field. By giving Soldiers either a skill qualification identifier or possibly creating an MOS, the Army would be able to track personnel with TECHINT training and give them assignments that would enhance their abilities and develop a professional cadre of analysts.

While the proposed size would prevent a TIC from conducting missions on its own, TICs could follow the 1/82 ABN SWET model and attach a small security element to the team while deployed or during major training events. It would take little more than an Infantry Rifle Squad's worth of people to supplement the team, and as a result the brigade would gain a versatile, highly trained unit that can conduct self-sustained reactive, proactive, and training missions.

## The Way Ahead

***"As the Army begins to train and field TICs, other units should consider taking advantage of the Weapons Intelligence Course."***

As this article is being written, 1/82 ABN's deployment is nearly complete and their replacements, 4/1 CAV, are in their final stages of preparation. When the 4/1 CAV's leadership came to Iraq in early 2008 for a Pre-Deployment Site Survey, they observed the value that the SWET provided 1/82 ABN and decided to stand up their own team. NGIC and the 203<sup>rd</sup> MI Battalion were extremely accommodating and resourced slots for 4/1 CAV to attend the spring Weapons Intelligence Course, fully qualifying them for the job. Their team will also include a security element, providing them with freedom of movement on the battlefield. The two teams have been in communication for a number of months and all of the 1/82 ABN SWET reports have been shared to facilitate a smooth transition. Both units are greatly benefiting from an innovative concept.

The Organizational and Operational Concept for TICs has already been approved by the commander of the U.S. Army Training and Doctrine Command. It is currently awaiting final approval during the Total Army Analysis for Fiscal Years 2010 through 2015 which takes place in July. If the Army decides to create TICs as an enduring capability, it would take approximately four years to fill the positions in every BCT, division, and corps in the Army. In anticipation for the increased demand and permanence of TECHINT, the training course is scheduled to move in the fall of 2008 from Aberdeen Proving Ground to Fort Huachuca, Arizona, and would be conducted twice a year.

As the Army begins to train and field TICs, other units should consider taking advantage of the Weapons Intelligence Course. The move to Fort Huachuca should enable the school to accept additional students. Some divisions have already sent personnel who were able to return and establish training for their subordinate BCTs. The training would be beneficial even for a BCT that receives a WIT in theater; some areas in Iraq maintain such a large volume of attacks that one WIT can not possibly respond to every event. A BCT's organic team could complement a WIT by either responding to insurgent attacks or providing dedicated Tactical Site Exploitation on missions for the BCT.

Beyond the current wars in Iraq and Afghanistan, there will be an enduring need for the capability that TICs can provide in gathering, assessing, and reporting critical information. Weapon systems used at the tactical level will continue to become more technically advanced, whether they are IEDs, rifles, or optics. Some brigade commanders have already assessed the need for these teams and have formed their own with internal resources. The SWET concept is a superb model to replicate. The approval and institutionalization of TICs or SWET Teams is a must, as these elements provide the tactical commander and the Army with a solution to fill a much needed capabilities gap which is required today and will undoubtedly be a necessity in the future.

*Captain Micah A. Niebauer is currently the Special Weapons Exploitation Team OIC for 1BCT, 82d Airborne Division. After graduating in 2003 from Wheaton College, Illinois, he worked for six months in the U.S. Department of State's Bureau of Political/Military Affairs, Office of International Security Operations. He has served as an Infantry Platoon Leader and Executive Officer for C Company, 2<sup>nd</sup> Battalion, 504<sup>th</sup> Parachute Infantry Regiment. He has deployed in support of Operation Enduring Freedom and Operation Iraqi Freedom. Captain Niebauer may be contacted at micah.a.niebauer@us.army.mil.*

*Colonel Charles A. Flynn was commissioned and came on active duty in 1986 after graduating from the University of Rhode Island. His military education includes the Infantry Basic and Advanced Courses, the U.S. Naval Command and Staff College, and the Joint Advanced Warfighting School, JFSC where he earned two Masters Degrees in National Security and Strategic Affairs and Joint Campaign Planning and Strategy. His extensive service includes Platoon Leader, Company XO; Assistant S3, 3rd Infantry Regiment; Battalion S4, 4-325th Airborne Infantry Regiment and Brigade S4, 2nd Brigade, 82nd Airborne Division and Operation Desert Shield/Desert Storm. He was the Commander, Alpha Company, 4-325th Airborne Infantry Regiment. He served with the 75<sup>th</sup> Ranger Regiment in positions to include Battalion S1, Battalion S3 Training Officer, and Commander, Alpha Company, 2nd Battalion, 75th Ranger Regiment. COL Flynn served in the 25<sup>th</sup> Infantry Division (Light) as G3, Chief of Operations; Battalion S3, 1-27th Infantry, and S3, 2nd Brigade. Other positions include Joint Plans and Operations Observer/Trainer, Deployable Training Team, Joint Warfighting Center, USJFCOM and Battalion Commander, 2-504th Parachute Infantry Regiment and deployed to Operations Enduring Freedom and Iraqi Freedom. COL Flynn's follow on assignment was Division G3, 82d Airborne Division. He is currently the Commander, 1<sup>st</sup> BCT, 82<sup>nd</sup> Airborne in Iraq.*



# COLLECTION MANAGEMENT IN THE COIN: A 3<sup>rd</sup> Infantry Division Perspective

## Introduction

As the 3<sup>rd</sup> Infantry Division established a new headquarters as the Multi-National Division Center (MND-C) for Operation Iraqi Freedom (OIF) V surge operations, we attacked problems with new insight and a fresh approach. As a new headquarters we had the opportunity to do things differently instead of simply falling in on already established procedures. When we arrived we, of course, met with and adopted many of the practices of Multi-National Division-Baghdad as we were assuming a large section of their operating environment (OE).

At first we wanted the transition to appear seamless to the brigades that would now have a different higher headquarters and it was a good place to start. We could have simply stayed there, maintaining the status quo, but then where would we have gone? Clearly we would not have made the significant advances that placed our Division in the forefront of the surge operations and the positive impact it had by reducing attacks by 60 percent in six months. Within the first 30 days our Commander, Major General Rick Lynch applied a directional focus on the collection management process calling it *Persistent Stare Operations*. This was a very different approach to collection management and intelligence, surveillance, and reconnaissance (ISR) operations.

## The Persistent Stare

The concept in its infancy was simple. MG Lynch stated, "I want to take every asset I can and focus

by Chief Warrant Officer Two Martin Schwerzler

on one area for 72 hours." While that sounds like an easy order to follow there were many traditionalists in the collection management field who would and did criticize this idea as a waste of resources and improper management of assets. We, the Division Collection Management and Dissemination Section (CM&D), initially believed the Commander would only do this once and let it go, moving on to another idea; however it was more than successful and the proof is the results of our rolling operations which had the same basic ISR strategy expanded to a Division operation lasting for a month.

One example is our first division surge operation, *Operation Marne Torch*, in northern Arab Jabour which started on June 15 and ended in July resulting in 89 enemy killed in action; 349 detainees; 61 caches found, and 1,279 structures cleared. Another is *Operation Marne Courageous* in the Owsat region which started on 15 November and ended on 15 December resulting in 57 detainees; 9 improvised explosive devices (IEDs) found; 12 caches found, and 217 structures cleared. Initially the brigades were unaccustomed to this level of support. Corps Collection Managers felt marginalized and left out of the decision making process as they were told to support the *Persistent Stare*. It is a different approach and people's natural inclination is to resist change and keep the status quo.

## **Plan or Plan to Fail**

When we first began planning and coordinating for *Persistent Stare* support, we discovered that there were many hurdles to jump to make it possible and effective. With multiple full motion video (FMV) platforms, it is easy to fill the sky over one area; the difficulty comes in planning, receiving, viewing, and exploiting collection. While planning we did not want two FMV assets looking at the same thing at the same time, so there needed to be a geographical separation. For FMV assets, there are a multitude of planning considerations when you have only one asset and the complexity is exponential when you are juggling multiple assets in one area. Some of the planning considerations are:

- ◆ How will the video feed be received?
- ◆ Does it require a special receiver?
- ◆ What resolution of imagery can travel across a unit's communication path?
- ◆ How will the asset be controlled?

Once a unit has all of the aforementioned issues worked out, it must now overcome the exploitation hurdle. Special attention to the effective planning of the exploitation is necessary; because if it all fails here, the rest of the planning and coordination is wasted. Tailoring of exploitation and control of the assets is critical due to the differences in the capabilities, manning, communication paths, and overall proficiency level of the unit being supported. Sometimes it meant that the Division ISR Cell controlled an asset. Division ISR, a Division-level four person section in the Division Operations Cell, maintained situational awareness of all unmanned aerial sensor (UAS) missions within the MND-C OE and responded to immediate requirements for FMV assistance. But the cell was not normally the primary controller of an FMV asset as that is the responsibility of the brigade or battalion.

The Persistent Surveillance and Detection System of Systems (PSDS2) (a contractor managed asset), a complex collection of various video feeds, video exploitation software, and still image capture software, occasionally fulfilled additional exploitation support. Again, the PSDS2 monitored most of the brigade FMV but was not normally the primary exploiter as that was the responsibility of the controlling brigade or battalion. A brigade's manning, equipment status, location, and experience level, determined whether it was capable of handling it all. The Division ISR stood by as a secondary or incorporating some of the resources previously mentioned. Other assets

were fixed and unchangeable as they were Theater planned, controlled and focused in general support to multiple MNDs; therefore spreading the support across a broader coverage and not wholly focused on one operation. For those assets we ensured they understood our requirement and that it received the appropriate level of emphasis.

## **The 100K Stare**

As a focal point, we always tried to maintain an area smaller than 100 square kilometers; the smaller the better. When MG Lynch started this concept, he simply asked brigade commanders where their problem areas were. Everyone quickly knew exactly where their worst areas were—typically high casualty producing areas, IED hotspots, and where the enemy was obviously making a stand. This meant the areas were target rich for us to select named areas of interest (NAIs) and to target for clearance teams and future operations to eliminate the threat. After our Division had cycled through several iterations and each brigade had been the focus of the *Persistent Stare*, it began to transition to a deliberate Division level focus.

Our planners and Intelligence sections determined where the enemy was, where he was going, and designed Division level operations to keep him on the run through a relentless pursuit with ISR chasing the enemy to focus combat power. It almost became a routine and methodical application of the simple tenets of stacking ISR assets and focusing on a limited area. In stacking the ISR assets we also used the principle of *mixed collection* which provides multiple intelligence disciplines looking at the same targets in order to build a more complete picture. In maintaining this operational and intelligence tempo, we incorporated many external agencies for assistance in sifting through the data collected to extrapolate every bit of intelligence related to an area.

## **Help from the Outside**

Outside agencies such as, the National Air and Space Intelligence Center (NASIC), the National Geospatial-Intelligence Agency (NGA), or the U.S. Air Force's Distributed Common Ground Station Analysis and Reporting Teams (DCGS DART) can provide a fresh look at data. NASIC focuses on the use and exploitation of air and space intelligence collection platforms; consequently, it possesses many experts on the wide variety of Measurement and Signatures Intelligence (MASINT) to provide specialized and correlated intelligence products. NGA focuses on the use and exploi-

tation of Imagery Intelligence (IMINT) by providing strategic level analysis conducted by experts in their respective fields and producing extensive in depth analytical products. The DCGS DART purpose is to improve the quality, responsiveness, and relevance of the intelligence analysis DCGS provides to its customers via the multiple ISR platforms that it operates, manages, or exploits in a near real-time manner. These are experts in various disciplines which no tactical organization could possibly have and incorporation of these resources is necessary when conducting a massive data collection effort.

In order for these agencies to be successful in supporting an operation, they have to be included from the planning stage. They need the priority intelligence requirements, NAIs, operational graphics, enemy situation, task and purpose, a general idea of what type of products to produce, and specific deadlines for delivery. Because these agencies are not in the immediate area they will not be familiar with the situation like a ground unit.

When you simply consider the outside agency as you would any other section of your unit, you get the best support. We sent everything to them from the initial NAI and warning order to the daily collection plans as they developed. Open discussions between the experts, liaison officers, and our CM&D section allowed familiarity with various capabilities of an organization, made cross cueing transparent and fluid, and built solid relationships of trust and interdependence and a cohesive team effort. While building these relationships with higher and external units, it is equally important to note the communication with the subordinate units.

## The End Result

As the *Persistent Stare* concept matured into a standard way of doing business, the brigades became an equally important part of the planning effort. Another simple maxim is that as you go down the chain of command the individual knows more about the terrain and the enemy. So as we developed the plan we invited the S2 and the Collection Manager from the brigade to be part of the planning and briefing of the plan to the commanding general (CG), usually during one of his weekly Analysis and Control Element Updates. This provided firsthand data regarding ground truth and an invaluable resource when the CG wanted a soldier's perspective from someone who had walked the ground. Additionally, it provided an open forum to discuss collection strategies, ensure the right assets

are on task and supporting, resolve any conflicts in scheduling, come to agreement on NAIs, and ensure synchronization of the plan across all echelons.

An additional benefit of the *Persistent Stare* is that there are multiple intelligence disciplines looking at a given area. Too often in normal operations we will support with one asset, typically a UAS, leaving us with more questions and a single source reporting on what is happening. When we stack multiple assets, we benefit from seeing and hearing the enemy, while passively observing activities through IMINT and MASINT for a more complete picture. A MASINT report may tell us that there was activity at a given location, we can then go back to see if there had been any moving target indicators within the given area, and query to find out if a UAS flew over the area. This is just one example of the benefit of stacking assets. Outside agencies and National reach back can produce many products based on the data collected. Once they are included in the plan, the data feeds their analysis and products. Ground commanders can then see and have access to the same analytic products once reserved for executive level briefings and assessments truly leveraging a hefty resource for a battalion or brigade commander to assist his operations and decision making.

The final benefit of a *Persistent Stare* is the brigade's benefit from the weight of a Division emphasis on their problem. In the collection management arena, combat operations take precedence over everything. When you start competing for limited resources the priority is stacked in the favor of Divisions when Corps is prioritizing. With these Division focused operations; it is easy to recognize requirements through all collection management echelons up to the U.S. Central Command level instead of being lost in a myriad of brigade and battalion level operation names. Finally, one need only look at the record and see the total number of attacks dwindle from 615 in June to 249 in December 2007, or see almost a 400 percent increase in the number of caches found between June and December 2007, to realize that *Persistent Stare Operations* in MND-C for OIF V was successful.

CW2 Martin Schwerzler has been assigned to the 3<sup>rd</sup> Infantry Division G2 as the Requirements Manager since September 2004 and served during OIF 3 and 5 in that capacity. He has also served in 101<sup>st</sup> ABN DIV (AASLT) and V Corps G2 sections in various intelligence and leadership positions. He instructed at Fort Huachuca, Arizona for the 96H CGS Operators Course and will be assigned to 3<sup>rd</sup> MI at NGIC in the Sustainment Training Section. He can be contacted at martin.schwerzler@us.army.mil.



# RED TEAMING AND THE INTELLIGENCE PROFESSIONAL: THE ENVIRONMENT AND THE CHALLENGE

by Nicholas R. Marsella

## Introduction

Today's battlefields are complex. Current operations range from those conducted in complex urban settings to those in sparsely populated harsh and inaccessible terrain. Elusive enemies operate in areas with populations having complex tribal, ethnic, and religious differences. Enemies attempt to coerce or control the population while wearing down U.S. resolve.

Future challenges will be no less complex. The challenges found in future operational environments are best described as operations that will be conducted: "among local populations with unfamiliar cultures, often in the midst of humanitarian crisis . . . in urban settings or harsh, inaccessible lawless areas . . . with an absence of local security or an effective local government . . . containing competing factions locked in internal conflict . . . against extremists, full spectrum and networked enemies embedded in the local population and possessing a wide range of advanced technologies and military capabilities including possible weapons of mass destruction (WMD) . . . employing adaptive and asymmetric combinations of traditional, irregular and criminal tactics . . . tied to a sophisticated information campaign . . . and conducted under the unblinking eye of an omnipresent

media, potentially giving local events global significance."<sup>1</sup>

Threats will range from traditional nation-state military forces to challenges posed by non-state actors. Adversaries may seek to possess WMD and attempt technological breakthroughs, gain access to niche technologies, or develop techniques to negate our technological capabilities.

The U.S. Army must be prepared to respond to each of these types of challenges—most often working in a Joint and multinational environment. Forces must be prepared to conduct "full spectrum operations"—simultaneously conducting combat and stability operations with units smoothly transitioning to new tasks to accomplish the mission. Commanders and their staffs must quickly identify and adapt to unanticipated challenges and opportunities. In an era of what the Chief of Staff of the Army has described as one of "persistent conflict," it will require us to think critically and creatively while being able to see things from other points of view.

For the intelligence professional, as a key member of the staff, the current and future operational environments present a huge challenge given the diversity of threats and their complexity. One of the best descriptions of

the challenges facing the intelligence professional is found in the 1997 version of the U.S. Marine Corps capstone manual on Intelligence, which states:

*"We expect a great deal from intelligence. We ask intelligence to describe in detail places we have never seen, to identify customs and attitudes of societies fundamentally different from our own, to assess the capabilities of unique and unfamiliar military or paramilitary forces, and to forecast how these societies and forces will act in the future. Most notably, we want intelligence to enter the thought process of an enemy commander and predict, with certainty, what course of action he intends to pursue, possibly even before he knows himself what he is going to do."<sup>2</sup>*

## Fighting and Winning in the Cognitive Dimension

To meet these challenges, the Intelligence Community (IC) **has, is, and will** continue to adapt. Better collection, improved dissemination, new means of visualizing the information about the environment—mostly technologically driven—are being worked. **Yet, what delineates intelligence from information is the work of the analyst and the assessment made by the "2."**

Successful commanders and their intelligence professionals must first **fight and win** in what is termed in joint doctrine as the "**cognitive dimension.**" As described in **Joint Publication 3-0, Joint Operations**, this is the dimension in which commanders and staff think, perceive, visualize, and decide, and as the doctrine highlights—"battles and campaigns can be lost in."<sup>3</sup> Clausewitz noted there will always be "fog and friction" on the battlefield, but fog and friction should not begin in faulty thinking, preconceived or biased views, resulting in flawed plans and intelligence estimates.

To reduce this "fog of war," we must understand the critical variables found in the operational environment, such as culture, as well as understanding the subtle relationships among the variables. Intelligence analysts must consider and account for the perspectives and the impacts of the enemy and others while simultaneously guarding against group-think, mirror imaging or using flawed assumptions to discover options not only for the enemy, but also opportunities for our commanders. **In essence, we must think critically, creatively and be able to see things differently in these increasingly complex, lethal, and ambiguous environments.**

One means to help commanders, their planners and intelligence staffs in "thinking" about the operational environment and discovering and examining alternative views is facilitated through the concept of Red Teaming. Traditionally, Red Teaming has narrowly been defined as modeling the enemy during a war game or training exercise, and while not incorrect, the term has recently taken on a much broader meaning. For the Military Intelligence (MI) community, Red Teaming is both a staff function and a process.

## Red Teaming

Historically the services, government, and industry have employed some form of Red Teaming—each having their own unique definition of the concept as well as differing perceptions of how to apply it to their endeavors. As noted by the *Defense Science Board (DSB) 2003 Study on Red Teaming*:

*"Red Teams and Red Teaming processes have long been used as tools by the management of both government and commercial enterprises. Their purpose is to reduce the enterprise's risk and increase its opportunities . . . . Red Teams are established by an enterprise to challenge aspects of that very enterprise's plans, programs, assumptions, etc."<sup>4</sup>*

In essence, Red Teams help the organization anticipate change before it is driven to it by challenging aspects of plans and operations developed by the organization.

Within the IC, Red Teaming has long been used—but with mixed success. Since 9/11, a number of intelligence related reports and studies recommended reinforcing Red Teaming within the IC. For example, the Robb-Silberman Report, *President's Commission on the Intelligence Capabilities Regarding Weapons of Mass Destruction 2005*, recommended the use of "Red Teaming" as both an analytical technique and as an additive organizational structure to improve our understanding and modeling of the enemy and to improve analysis.<sup>5</sup> This report reinforced long standing intelligence practices such as analysis of competing hypotheses, alternative analysis, and other analytical techniques. Other studies such as U.S. Joint Forces Command's *Iraqi Perspective Study* illustrated the need to approach the battlefield through the perspective of the enemy goals, intent and culture—an old lesson continually rediscovered by intelligence professionals.<sup>6</sup>

From the Army perspective, as a key issue relevant to Army Intelligence Transformation, the MI

leadership in 2007 identified “Red Teaming” as a key enabler and a nontraditional analytical skill needing to be trained.<sup>7</sup>

From the doctrinal standpoint, the June 2007 update to **JP 2-0, Joint Intelligence**, recommends using the concept of Red Teaming as a means to better understand the adversary and visualize the relevant aspects of the operational environment. JP 2-0 states:

*“Red Teams are organizational elements comprised of trained, educated, and practiced experts that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. Red Teams assist joint operation planning by validating assumptions about the adversary, participating in the wargaming of “friendly and adversary courses of action (COAs) and providing a check on the natural tendency of friendly forces to “mirror image” the adversary . . . ”<sup>8</sup>*

As a function, trained and educated Red Teams formed from or added to an intelligence staff, whether permanent or on an “ad hoc” basis, serve as **catalysts** to help the J2/G2/S2 escape the gravitational pull of our own western military culture and organizational procedures by continually questioning and offering alternative perspectives about the enemy COAs while also accounting for the many “others” influencing the environment.

Within the Joint community, Red Teams have been formally added as an organizational element within the newly created combatant command level Joint Intelligence Operations Centers (JIOCs). Initial reports of their additive value have been good. For example, a U.S. Pacific Command JIOC branch leader recently noted that Red Teams allow them “to tap the expertise of critical and creative thinkers, . . . to encourage consideration of overlooked possibilities, challenge assumptions and present issues in a cultural context or from a different perspective.”<sup>9</sup>

But the idea of Red Teaming is more than a job title, it is a process embedded in intelligence theory and doctrine and practiced by the best intelligence staffs and their analysts. Red Teaming demands the entire J2/G2/S2 staff continually examine its own thinking—being self critical. It is drilling down on whether the assumptions made are correct or merely wishful thinking. It is self questioning to ensure the estimate doesn’t reflect bias, groupthink, or mirror imaging of our own values, culture, and military theory.

Red Teaming enables the analysts to discern the difference between the known, unknown, and the possible. As Director of National Intelligence Mike McConnell noted on the advice given to him by then Joint Chiefs of Staff Colin Powell: “The rules are, as an intelligence officer, . . . is to tell me what you know, tell me what you don’t know, then you’re allowed to tell me what you think, but you always keep those three separated.”<sup>10</sup> The process of Red Teaming helps the analysts ensure this differentiation occurs, while expanding the range of the “possible” meanings and options available to the adversary and other major entities in the operational environment.

## **Army Red Teaming for Decision Support**

In 2005, the U.S. Army began to experiment with the concept of Red Teaming as a shift in our own Army organization culture, and move it beyond its linkage solely to the intelligence warfighting function. The concept was to expand what is already a requirement in our planning doctrine, as found in **FM 5-0, Army Planning and Orders Production**, by providing an independent capability to help the commander and staffs think through the problem, offering alternative perspectives, and helping to examine the group’s decision making process.<sup>11</sup> As the concept was refined, three major tasks emerged for this newly created special staff element to accomplish:

- ◆ Provide alternatives during planning and operations by participating in each phase of the planning process by assisting in problem framing; challenging the planning assumptions being used; identifying friendly and enemy vulnerabilities and opportunities not captured, and helping the staff to “think” about the assessment system to ensure we are measuring the right things.
- ◆ Anticipate and help the staff to account for the cultural perceptions of partners, adversaries, and other to include the potential operational implications and consequences of our and their actions.
- ◆ Conduct independent critical reviews and analysis to identify potential weaknesses and vulnerabilities before the enemy does.

The concept is to embed a small “Red Team” as a “special staff element” responsible to the commander/chief of staff, but working with the “staff.” As a division chief of staff noted: “These Red Teams serve as the designated critics charged with productively challenging ideas and decisions, bringing

fresh perspectives, and ensuring the cultural factors are injected into the decision cycle.”<sup>12</sup>

Pending final Department of the Army approval, we will in the next few years, document Red Teams as part of Army, corps and division headquarters tables of equipment. In the meantime, to support deploying forces, Red Teams are being created either “out of hide” or using reserve personnel, currently supporting Army units in Operations Iraqi Freedom/Enduring Freedom. At the brigade combat team (BCT) headquarters, in lieu of adding more personnel to the headquarters, two members of the staff will be trained as Red Teamers and will use the skills primarily in their duties as the Plans Officer and the Assistant S2. Human Resources Command has created and begun awarding the Additional Skill Identifier (ASI) 7G–Red Team Leader and 7J–Red Team Member to those graduating from Red Team education and training programs.

Critical to the success of any Red Team is the selection of the right people with the right personality, skills, and experiences. Personnel must be effective and tactful communicators, negotiators and listeners. Experienced officers must lead the team in grades comparable to the primary staff officer’s grade (e.g., Red Team Leader is a colonel/06 at the Corps level) to facilitate dialogue. They must have team members (normally majors) with the right set of experiences and skills specifically Areas of Concentration Foreign Area (48), Strategist (59) and Military Intelligence (35).

Success for the Red Team is defined by aiding the command in viewing problems and potential solutions from various perspectives in “real time” to be of value and without being a critic or “Monday morning quarterback.” An effective Red Team buys the unit improved horizontal integration; production of the “what if” questions others often hesitate to ask; and better accounting for the variables found in the operational environment in our plans.

## Impacts on the Army IC

First, G2s will interact with the Red Team serving as a special staff element within our formations. These small Red Teams will primarily interact with the plans and future operations staffs, and do not augment the G2 staff. Unless otherwise directed by the commander, the relationship between the Red Team and the G2 is one best categorized as “mutual support,” the G2 providing access to available information

and the Red Team providing insights and alternatives to the G2 based on the Red Teams own sources of information and subject matter experts with a different interpretation of the data.

Secondly, MI personnel will serve as members on a Red Team. In fact, the ASI 7J–Red Team Member is being added to each BCT Assistant S2 position, requiring the officer to attend Red Team training. At the Army, corps and division Headquarters, an MI officer will serve as a member of the Red Team.

Lastly, every analyst would benefit from the thinking skills associated with Red Teaming. Within our career courses, the concept of Red Teaming will be introduced and whenever possible, we should afford the senior analyst time to participate in this training.

## Educating and Training Red Teams

*To enable success, Red Team personnel must receive education and training different in scope and content to enable them to think differently to reach alternative conclusions and alternative perspectives.*

In 2006, the newly established University of Foreign Military and Cultural Studies (UFMCS) at Fort Leavenworth, Kansas began educating and training Red Team leaders and members using a diverse “graduate level” curriculum organized along five major themes:

- ◆ Critical and creative thinking.
- ◆ Red Team techniques to include communication, negotiations and group dynamics.
- ◆ Anthropology and understanding the impacts to and how to apply culture to understand the operational environment.
- ◆ Understanding the trends and variables found in the operational environment.
- ◆ Western, non-western, and non-military (competitive) theory.

## The Bottom Line—Red Teaming Is Value Added

Whether you view Red Teaming as an additive structure, a concept or an analytical tool, history continually produces the lesson for the need to look at situations and problems differently. History notes we should expand our thinking while shedding bias and fixed mindset, while avoiding mirror imaging, and considering alternative COAs from the perspectives and mindsets of our adversaries and others.

Two key catastrophic events from our history illustrate the point that a lesson that isn't learned is not a lesson at all. The catastrophic events on December 7, 1941 and September 11, 2001, separated by 60 years, had many similarities. In these events, history (and subsequent investigations), clearly demonstrated we were captured by our own mindsets and biases and unable to comprehend that an adversary would take the actions it took. As one author noted, "The fatal flaw was that we believed that their logic had to be our logic."<sup>13</sup>

A properly trained Red Team with the right people will provide timely value added input to challenge the unit or staff's thinking and assumptions, while identifying vulnerabilities, opportunities, consequences, and alternative perspectives not captured. As Sun Tsu wisely counseled, "victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur."



#### **Endnotes**

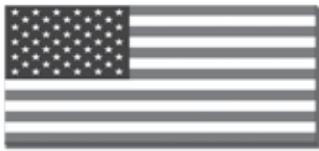
1. Extracted from the U.S. Army Training and Doctrine Command (TRADOC) G2 (Futures) unclassified briefing, "The Future Operational Environment: An Era of Persistent Conflict," May 2008.
2. U.S. Marine Corps, "The Nature of Intelligence," MCDP 2 Intelligence, 17 June 1997, 17.
3. JP 3-0, Joint Operations, 17 September 2006, II-21.
4. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Defense Science Board Task Force, The Role and Status of DOD Red Teaming Activities, September 2003, 2.
5. Report to the President of the United States, 31 March 2005, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 170. The report is commonly referred to as the "Robb-Silberman Report," named after the two co-Chairmen.
6. Kevin M. Woods with Michael R. Pease, Mark E. Stout, Williamson Murray and James G. Lacy, *Iraqi Perspectives Project: A View of Operation Iraqi Freedom from Saddam's Senior Leadership*. USJFCOM Joint Center for Operational Analysis, 2006. An abridged version of this study is found at "Saddam's Delusions: The View from the Inside" in *Foreign Affairs*, May/June 2006.
7. Association of the United States Army, Torchbearer National Security Report-Key Issues Relevant to Army Intelligence Transformation, July 2007.
8. JP 2-0, Joint Intelligence, 22 June 2007. This updated manual highlights the uses of "red teams" to support intelligence analysis, COA development and wargaming. While the JP 2-0 definition identifies the task to validate assumptions (a difficult task and the purpose of the ISR system) it is more appropriate to use the word to "challenge" assumptions" used by the intelligence staff in order to ensure only those needed are used and those used meet the test of being logical, and appropriate.
9. CAPT Tyler Akers, USNR, "Taking Joint Intelligence Operations to the Next Level," Joint Forces Quarterly, Issue 47, 4<sup>th</sup> Quarter 2007, 70.
10. Remarks and Q&A by the Director of National Intelligence, Mr. Mike McConnell on *Strengthening Analytic Practice: Lessons from the World of Journalism*, 13 November 2007.
11. Red teaming is defined as a "function executed by trained, educated, and practiced team members that provide commanders an independent capability to fully explore alternatives in plans, operations, concepts, and capabilities in the context of the operational environment and from the perspectives of our adversaries, and others. This definition is included in various sources and is found in the U.S. Army Posture Statement 2008, TRADOC Pamphlet 525-3-3, US Army Functional Concept for Battle Command 2015-2024, and is also found in JP 2-0.
12. Colonel Allen Batschelet, and Majors Mike Runey and Barry Hafer, "Risking Critique: Critical Review and Alternative Perspectives on the Battlefield," Armed Forces Journal at <http://www.armyjournal.com/2007/11/3072814>.
13. David Abshire, *Lessons for the 21<sup>st</sup> Century: Vulnerability and Surprise: September 11, 2001 and December 7, 1941*, (Washington D.C., Center for the Study of the Presidency, March 2002). Also a similar comparison of 9/11 and 7 December 41 is found at Combat Studies Institute Press, *Staff Ride Handbook for the Attack on Pearl Harbor, 7 December 1941: A Study of Defending America*.

## **MI LEGACY** —



SD-1 Surveillance Drone was a radio controlled plane used from 1957 to 1961 primarily for photo surveillance.





# Coalition Intelligence in OIF: A Year in Iraq with Multinational Division-Central South



by Lieutenant Colonel Robert M. Wilkinson

## Introduction

Performing as a Military Intelligence (MI) professional in a combat environment can be one of the most challenging experiences of one's career. Doing so as a member of a foreign-led Coalition division staff can be intriguing, exciting, challenging and frustrating—sometimes all at the same time. Success in this sort of international environment requires patience, perseverance and innovation. If you are destined to serve with a Coalition headquarters, here is what you need to know in order to be better prepared.

## Doctrinal Terms

In order to properly describe our craft, we use doctrinal terms to be sure that all involved have a common understanding. I offer these definitions according to **JP 1-02, DOD Dictionary of Military and Associated Terms** in order to clarify the terms I will use in this article. An **alliance** is the result of formal agreements (i.e., treaties) between two or more nations for broad, long-term objectives that further the common interests of its members. The North Atlantic Treaty Organization (NATO) is probably the best example of a permanent alliance to which the U.S. belongs. A **Coalition** is an ad hoc arrangement between two or more nations for a common action. The War on Terrorism Coalition is an ad hoc arrangement. **Multinational** is an umbrella term that includes both allied and Coalition and implies anything dealing with multiple international military partners.

These may seem like subtle distinctions, however, the differences are immense. Imagine the difference between a long-standing alliance where the terms of reference, doctrine, procedures, and standards have been worked out over many years and a Coalition

where little or no time has been devoted to interoperability and mutual understanding due to the urgency of the mission. This is the first point of reference that you must understand if you are destined to serve in a Coalition environment—it will not be easy to get things done until you realize that the American way of doing business is only one of several options.

## Background

Under the auspices of the State Partnership Program (SPP), former Warsaw Pact and Soviet Republics are paired with U.S. Army National Guard (NG) states for training and mentorship. From April 2007 until April 2008, I served in a small contingent of Army NG Soldiers supporting Poland by State Department request. Chicago, Illinois has the second largest concentration of Poles outside of Warsaw, so it only stands to reason that Illinois was partnered with Poland under the SPP. I was part of the fifth iteration of Illinois Soldiers augmenting the Polish division in Operation Iraqi Freedom (OIF).

For more than five years, the Polish Army has been the lead nation for Multinational Division-Central South (MND-CS) formerly in Babylon, now headquartered in the southern Iraqi city of Diwaniyah. During this time, the division was comprised of troop contributions from Armenia, Bosnia-Herzegovina, Bulgaria, Denmark, El Salvador, Kazakhstan, Latvia, Lithuania, Mongolia, Romania, Slovakia, and Ukraine in addition to Poland and the U.S. At one time, the division's area of operations spanned from the Iranian to Saudi Arabian borders between MND-Center and the British-led MND-Southeast. However, the current configuration of MND-CS only encompasses Al Qadisiyah province. MND-CS decreased in size as sev-

eral nations have withdrawn from Iraq since the OIF Coalition began in 2003. Current troop contributions come from Poland, Bosnia-Herzegovina, Mongolia, Latvia, Romania, Ukraine and the U.S. Poland's troop contribution to OIF is slated to end in October 2008; however, it is significantly increasing its presence in Afghanistan for Operation Enduring Freedom (OEF).



(R to L) General David Petraeus, MNF-I commander, Major General Tadeusz Buk, MND-CS 9th Rotation Commander and Lieutenant General Ray Odierno, MNC-I commander look on as the 9th rotation of Coalition soldiers pass in review for the transfer of authority to Rotation 10 (January 2008).

As American Soldiers, U.S. policy precluded us from being under command of other nations, therefore, our official duty descriptions stated that we were under the operational control of MND-Center acting as liaisons to MND-CS. In reality, we were embedded members of the division staff and our Coalition partners relied heavily upon us to guide the staff and closely advise the command group. There was already a liaison team from the higher headquarters, Multinational Corps-Iraq (MNC-I), which accomplished the typical liaison mission. My U.S. colleagues and I served in PMO-Detainee Operations, G2, G3, G4, and G9 staff sections. Our detachment commander served as the Assistant Division Commander for Support. My duties included being the Deputy G2 and G2X for MND-CS. In addition to acting as staff members, MNC-I expected our team to influence and shape the direction of the division, to ensure compliance with Corps and Theater directives, to improve the quality and timeliness of staff products, and to accurately report combat information and intelligence through U.S. systems.

My duties as Deputy G2 included directing, leading, and managing the analysis and production efforts of a very small, multicultural staff (15 officers and one noncommissioned officer (NCO)). I was frequently in front of a podium or a computer projector briefing dis-

tinguished visitors and high-level commanders as well as representing the G2 or the commander at meetings requiring a native English speaker. Regular trips were required to coordinate and collaborate with my MI peers at MNC-I and Multinational Force-Iraq (MNF-I) headquarters on behalf of the Polish division commander and staff. In addition, as the senior U.S. intelligence officer on the staff, I received all of the requests for information from higher and adjacent units.

As the G2X, I directed and managed interrogations, document and media exploitation (DOMEX), Human Intelligence (HUMINT) collection operations and Counterintelligence (CI) matters. These duties presented me with the biggest challenges and the widest gaps to fill. For example, because there was no releasable source registry database, it was virtually impossible to de-conflict American HUMINT operations from those of the other nations. Polish and Romanian collectors, just like American collectors, were reluctant to reveal the identities of their sources to collectors of other nationalities. To find a solution, I devised a crude source registry and rudimentary system of de-confliction using source phone numbers as the lowest common denominator with which we could attempt de-confliction.

My 2X duties also required that I coordinate closely with the Polish Ministry of Defense intelligence organizations operating in the MND-CS area of responsibility. The relationship between the MNC-I C2X, Field Office Iraq, MNC-I CI coordinating authority (CICA), sub-control office (SCO) and MND-CS flowed through me as well. Several investigations during my tenure required constant coordination between the U.S. and Polish CI assets as well as foreign disclosure challenges. I met on several occasions with senior officers from the Romanian Intelligence Directorate on matters of training and operations affecting their HUMINT collectors in OIF.

## What to Expect

**Language issues.** If you have never operated in an alliance or Coalition before, the first thing you need to accept is that language will be the biggest barrier to overcome. As Americans we learn to speak our own brand of English which varies regionally and culturally depending on where (and sometimes when) we grew up. As military professionals, we learn to abbreviate our communications using acronyms, keywords, terms and phrases which are not always well known outside our own military circles. Even though

the “official” language of OIF was English, every troop contributing nation tends to stick to their native language for ease and brevity. In order to communicate effectively, everyone has to learn how to speak slowly and correctly while avoiding euphemisms, colloquialisms, and non-standard military terminology.

Remember that a Coalition, unlike an alliance, is an ad hoc organization made up of countries that have not worked out all the details of their relationship. Unless you are lucky enough to have training in the proper language, it is best to slow down and think through what you are going to say ahead of time. On one occasion, my counterpart described how his international counterparts were struggling with a newly-learned task using a simple American phrase—“It is a bit like batting left-handed.” Based on what he thought he heard, a non-U.S. commander angrily replied, “What is wrong with my lieutenants?!” My colleague’s southern Illinois drawl and fast manner of speaking often led to simple misunderstandings which wasted valuable time and energy.

Many of the nations I worked with were members of NATO (some very recent). Often times, NATO or European military doctrinal terms (such as the abbreviation “coy” meaning company) would confound the already difficult process of separating accents and less than perfect pronunciation from the subject matter itself. Learn the terminology and phraseology used by your international peers and once you find the words that are interchangeable with your own, then use their words in order to facilitate mutual understanding.

Even though English was supposed to be the mandated language for OIF partner nations, the level of expertise varies widely between the enlisted and officer ranks. In fact, the older, more senior officers and NCOs were usually the least well-versed in the English language. One of the best things I did during my tour was to purchase a Polish-English dictionary to better understand the commonly used words in their native language. Ask them to teach you words in their language. Something as simple as saying “enjoy your meal” in Polish goes a long way toward earning trust and confidence from your counterparts.

Do not be offended when they switch to their native language during periods of intense discussion or stress. We called it “channel two,” as if they had suddenly switched to a different radio frequency. A patient approach to that situation will almost always

result in an apology and an explanation of what happened. Befriend someone with good English skills and ask them to give you the play by play translation.

**Cultural differences.** Different militaries have different standards for grooming, appearance, physical fitness, military dress, and personal hygiene. Beards are common among the soldiers of many Coalition countries. These differences are not necessarily bad, rather they are just different. If your colleagues are celebrating a particular cultural event, take part in the festivities. This not only shows respect, but it will often break down barriers. Obviously, we must not cross the line when it comes to general orders, regulations, and rules pertaining to forbidden activities; however, there are ways to show your respect and interest in cultural differences without getting yourself in trouble.

Good order and discipline have different applications and meanings to your Coalition partners. Where the U.S.-led units and bases will have very specific rules about uniforms, behavior and activities, a Coalition-led unit or base might not. One has to learn to live with those distinctions without breaching your own standards or degrading your own safety.



Romanian officers from the G2 staff pose for a group photo at the conclusion of their six month rotation at MND-CS headquarters.

**Military Training and Operational Experiences.** Many of the Coalition officers I served with were multi-tour veterans of OIF, the Balkan operations (KFOR, SFOR, IFOR) and OEF. And yet, they did not have the depth of MI knowledge and expertise that I had. The main reason for this disparity is that very few foreign militaries have a stand-alone intelligence corps. In the case of the Polish Army, the majority of the officers I worked with were reconnaissance officers, which is

roughly the equivalent to our cavalry branch. This meant that their core competencies involved confirming or denying information by direct observation. This proved useful because the most abundant intelligence, surveillance, and reconnaissance (ISR) assets we had at our disposal were Russian-made Mi-24, Mi-8 and Polish-manufactured W-3W helicopters.

Most of the foreign army officers lacked a mid-level or intermediate officer training experience like our captain career courses (CCCs) and intermediate level education (ILE) system. Once they completed initial entry officer training or a military academy, most foreign officers are not likely to receive further military education until late in their careers when they reached the senior staff/colonel-level. In my own experience, the most competent officers I worked with were those who were lucky enough to attend training at U.S. schools such as officer basic courses, CCCs or ILE. This did not mean that the other officers were less capable, but rather that they did not have the benefit of recent military education. Also, the U.S.-trained officers were well-versed in the doctrine and procedures most familiar to me, which naturally made it easier for me to work with them.

Given these types of constraints, you have to remember to not try to do all the work yourself because you feel you cannot trust others to meet your standards. You must learn to leverage the competencies wherever you can find them. I found it was better to aid and mentor them as they developed their own expertise. Certainly, it is a great deal easier to edit the intelligence summary every day than to write it all by yourself.

**Managing Expectations and Obligations.** You have probably heard that perspective is what matters. From your perspective, foreign military personnel could have a different work ethic and varying degrees of motivation. If you are in a leadership position, is up to you to find ways to get them to do the work that needs to be done and to respond in a timely manner to your requests. Sometimes, sheer personality or what I like to call “brute” personality is all you have in your tool box to motivate and lead foreign Soldiers. Remember, from their point of view, you might be setting the bar too high or asking more of them than their own peers do. Be prepared to accept a certain amount of resistance until you have earned the respect of your peers and subordinates. Once they realize that they benefit and learn from working with you, they will also seek to excel at their duties.

**Rank Structure.** Foreign armies do not place as much trust and confidence in their NCO Corps. This puts U.S. Soldiers at a disadvantage because the foreign headquarters can be very rank-heavy and officer-centric. In the case of MND-CS, two thirds of the force were officers, many of who had been frocked one or two grades for the mission. We had colonels who were actually lieutenant colonels or majors in some cases. The Poles referred to those officers as “desert colonels,” meaning they were temporarily frocked for the mission. Section leaders and primary staff officers sometimes lacked the depth of experience that we associate with a certain rank or grade. Another issue is foreign officers, especially those from former-Eastern Bloc countries, tend to discount the words and deeds of U.S. NCOs. This was particularly challenging for the sergeants on our team who were used to having a great deal more respect, authority and responsibility. The only solution for that dilemma is to work hard and earn their trust.

**Foreign Disclosure Challenges.** As an MI professional, you will most likely be working with U.S.-only systems which contain plenty of information that is not releasable to every nation in your Coalition. For example, the default caveat for secret level information being produced by ISR assets is quite often too restrictive for your needs. Be persistent when asking the foreign disclosure officer or originator to provide new products for broader release recognizing that what you need is usually not the default setting and it requires extra effort to get what you need. The more you educate the adjacent and higher units about your particular information requirements and maximum caveats, the easier this process will become. I built bridges to my counterparts at MND-C and MND-SE to ensure that I was getting all the intelligence products they produced under the releasable to multinational Coalition force-Iraq caveat (REL MCFI).

**Interoperability Problems.** Each nation contributing to a Coalition must bring their support elements to the fight. This means that the lead nation must provide a sufficient number of communication systems for all of the troop-contributing nations in that headquarters. In our case, MND-CS provided two types of telephones for internal communications (one tactical and one commercially-purchased phone solution) along with a commercial Internet provider and one national classified network administered and operated

in Polish. As a member of the U.S. team supported by MNC-I assets, I had the defense switch network (DSN) access, secure and non-secure voice over Internet protocol (VOIP) phones, and U.S. NIPR and SIPR networks available to me. The two separate sets of communications systems did not interface at all, except perhaps the DSN and Polish contracted phone system which could communicate after an elaborate series of dialing protocols and connections.

The one common computer system for all to use was the Combined Enterprise Regional Information Exchange Network System (CENTRIXS) computer network, which had several major drawbacks. Our adjacent and higher U.S. units did not like to use the CENTRIXS network because it represented a third (and in the intelligence field, a fourth) network to populate, monitor and manage. Most of the intelligence products issued by adjacent or higher U.S. units were classified above the level which could be distributed on CENTRIXS. Those products which were available at the appropriate level were not always distributed on CENTRIXS in a timely manner.

Another challenge for us was the lack of funding, supplies and replacement parts for our Coalition partners. The U.S. dollars available in abundance for American units to use were not always available for our Coalition partners to use. We had to be very careful when applying for contingency funding to apply it properly according to U.S. law and fiscal policy. Our international partners do not have the fully developed expeditionary logistical systems and lacked funding for country-specific major end items when they reached the end of their lifespan, were damaged in combat or required repairs.

Radio communications were difficult between U.S. and Polish units until we learned how to configure our radios to be compatible with theirs. It took several intense discussions to realize that the Polish ground and air units operated with their squelch off; requiring U.S. units to change their standard operating procedures accordingly.

**Shorter tours of duty.** Almost all of the nations involved in MND-CS were on a six-month rotation schedule. This meant that when I replaced my predecessor, I was falling in on a staff that had already been working together for three months. They were completely entrenched and set in their ways, which presented a greater challenge for me to establish my credibility and to achieve their acceptance. The sec-

ond group arrived and relied extensively on our U.S. team to guide them through the first few months. By the end of their tour, we were working together like a well-oiled machine, only to have to end the relationship prematurely. The third iteration of international soldiers also relied on us as well, although they knew we would be replaced in a few short weeks.



Polish Army Bronze medals were awarded to select Coalition officers on the MND-CS staff from Armenia, Mongolia, Latvia, Lithuania, Ukraine and the U.S. for their contributions to MND-CS (author on the far right).

## Conclusions

This deployment was my seventh multicultural military experience and the most challenging period thus far in my twenty-five year career. This was also one of the best tours of my life because I made life long friends and I will always be welcome to visit Poland, Romania, and several other countries.

Serving in a Coalition-led environment requires diplomacy, tact, and sensitivity. However, you also must be firm when it comes to adherence to policies and procedures. And you must maintain a flexible approach to problem-solving. There are many pitfalls to serving in a multinational environment which must be carefully managed in order to be successful. Be patient, learn from your partners, and embrace diversity as strengths.

LTC Bob Wilkinson enlisted in 1983 and was commissioned as an aviator in the Army Reserve in 1986. He has served as a platoon leader, XO, company commander, intelligence liaison officer, brigade S2, and operations officer in the U.S. Army Reserve and Army National Guard. He has four officer branch designations: Military Intelligence, Aviation, Transportation and Chemical. He is a graduate of the MI Officer Tactician Course, MI Captains Career Course, Command and General Staff College and attended the Joint C4I Staff Operations Course at the Joint Forces Staff College. LTC Wilkinson currently serves as a detachment commander in the Army Reserve Operations Activity (AROA).

## Part 2: 3<sup>rd</sup> Regional BTT—Initial Operational Employment on the Iraq/Iran Border Wasit Province

by Lieutenant Colonel Michael P. Spears

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

*This is a continuation of an article started in the April June 2008 issue of MIPB. Previously, LTC Spears discussed his experiences as a member of the Wasit Province BTT (March 2006–2007) regarding the training the team received prior to deployment; the team's relationship with Coalition forces; Camp Delta operations, and support issues. Here he discusses the team's relationship with the ISF to include training the Iraqi division intelligence personnel; POE and other border operations; support issues, and some recommendations.*

### Mentoring, Advising and Training

*"They're learning how to conduct searches, and they have a ways to go." Further training . . . has focused on computers, tactical checkpoints, logistics, communications, intelligence, the military decision making process, marksmanship, tactical operation centers and patrolling. "We spent about a month working with them and talking to them about how to do an operation (Regional team member)." <sup>14</sup>*

Teaching an eight week basic intelligence course was our first success and came about when the Iraqi division intelligence officer asked us to teach a basic course to the division, brigade, and battalion intelligence personnel. IAG did not provide any programs of instruction to assist us in training our counterparts. Reaching out to the U.S. Army Intelligence Center, we asked for anything it might have. With its assistance, and combining resources from the four teams, we conducted the course over eight weeks at Camp Delta. The G2 led by example, attending the course himself and later asked us to teach an advanced class to his senior personnel. Before we had



Training Iraqi Intelligence students.

a chance to conduct it, he was unexpectedly transferred and replaced with a Sunni officer from Diyala province. Fearing for his life, he rarely came to Shia' province headquarters location.

### Logistics in Iraq (Team Support and Support to the Iraqi's Logistics Classes)

*In 2007, a U.S. general officer, commanding a new offensive north of Baghdad, said his Iraqi partners may be too weak to hold onto the gains.*

**“They’re not quite up to the job yet.” His counterpart south of Baghdad seemed to agree saying, “There’s got to be more ISF . . . and they’re not quite up to the job yet . . . . Iraqi troops are short on uniforms, weapons, ammunition, trucks and radios.”<sup>15</sup>**

What they do not mention is the failure of the Iraqi Ministries of Interior (MoI) and Oil (MoO) to work out procedures to supply their units with fuel and prevent its diversion to the black market. The Ukrainian team briefed us that the Iraqi MoI under budgeted the actual cost of fuel for their units. MoI was supposed to transfer 2.5 million Iraqi dinars (IRD) each month to a fuel account. However, often the money is not transferred, and no transfer meant no fuel. Even so, 2.5 million IRD will only purchase between 10 to 16.7 thousand liters, during one three-day exercise they used five thousand liters alone. For the Border Police, fuel is a pacing item, without it the unit cannot perform its mission, generate electricity, or communicate.

Logistics tasks and equipping the Iraqi forces was one of the most important functions the team accomplished. Since we did not have a qualified Logistics officer, our Fires officer filled that role and worked any issue involving acquiring, managing, receiving, storing, issuing, and maintaining visibility and control of all classes of supply required to equip and sustain the Border Enforcement Division and the subordinate units. In effect, this meant working with the Multi-National Security Transition Command to obtain equipment for the ‘approved’ organizational structure.

Distributing the equipment was more of a challenge and it was always questionable whether the Iraqis would show up to accept it as coordinated. If so, would they have sufficient transportation and labor to load it? We stopped by the 2nd Brigade headquarters a month after a large delivery of equipment intended for the brigade and its subordinate units. The equipment was still stored throughout the headquarters. When asked why they had not distributed the equipment to their battalions and companies, they replied it was a gift for the brigade. Had we not checked, these items could have remained unused or possibly ended up on the black market. Maintenance on the Iraqi side was almost non-existent. A brand new trailer mounted generator apparently had a flat during the 86km trip from Delta to

the brigade. Rather than fixing it, the Iraqi’s continued to pull the trailer until the tire caught fire and fused to the rim; it was in the same condition when I saw Iraqi soldiers moving the trailer weeks later.

In addition, the units on the ground did not match the authorized modified table of equipment (MTOE). In our case, the division commander created a “Special Forces Battalion.” While he had the MoI approve the MTOE, he claimed he had no orders to implement it. This was a major issue throughout our tour; Iraqi Department of Border Enforcement (DBE) leadership didn’t approve or disseminate guiding documents and directives to subordinate commands in a timely manner.

Even so, our Fires/Logistics officer worked on comparing the “approved” MTOE to actual personnel on the ground. This sounds like an easy task, but determining who is actually in the roles is quite difficult. Merely tracking the duty status of an individual is next to impossible as Iraqi border enforcement personnel may take 10 to 15 days off each month. It makes it extremely difficult to train and maintain a professional force when you must hire 2 to 3 times the force you need and retain only 40 percent.

## **Border and POE Operations**

***The Coalition Provisional Authority view on border security in 2004 was “Foreign terrorists are present in Iraq. The numbers are not known with precision, but recent attacks and their continuing presence underscores the importance of improving security at Iraq’s borders. We are accelerating border security efforts . . [to] assure that when we turn over sovereignty . . the government will have the equipment, staff, training and materials necessary to operate each of its 20 major border-crossing points. We will monitor, limit and control the number of people crossing into Iraq and . . will begin deploying a system called PISCES—to positively ID everyone entering or leaving Iraq.”<sup>16, 17</sup>***

A port of entry or POE is similar to a crossing point between the U.S. and Canada or Mexico and conducts basic immigration customs and other related law enforcement services. In March 2006, two years after the Coalition Provisional Authority’s statements, the first U.S. BTT entered the picture; the Wasit Province POE record keeping system was



POE on Iraq/Iran border.

still bundles of loose-leaf paper subject to loss and corruption. Further, the lack of basic utilities and telephone service along the border made using a computer system, such as PISCES, nearly impossible without sufficient fuel to operate generators and available secure communications. Even obtaining basic information about border activity was not easy. The POE Director refused a request from the Ukrainian team for regular reports regarding the number of people and vehicles entering through the POE, unless he received an order from the MoI di-



Record Keeping at Wasit Province POE.

recting him to do so. We were eventually able to get this information after we placed a U.S. transition team at the POE. It was still difficult, this is a country with no viable databases or the ability to check data and no national requirements that direct and enforce the collection and reporting of information including biometric data on those who cross their border.

After Saddam's fall, Iranian Shiites saw their chance to visit their sacred sites in the holy cities of Najaf and Karbala. Our POE, while small, is the

busiest border crossing point on the Iraq-Iran border and the closest legal entry point for these cities. Daily pedestrian traffic alone, not including commercial traffic, varied between 1,200 and 2,000 Iranian "tourists" (70 percent of whom are women). U.S. officials believe, but Iraqi officials deny, that supplies and personnel move from the Iran to Iraqi border using these routes and it is difficult to distinguish legitimate visitors from Iranian government operatives providing aid to insurgents.<sup>18</sup> Often it was not possible to search females crossing from



Pilgrims at the border.

Iran, because there were no female employees on duty. Due to cultural taboos, a man wearing a full-length black robe disguised as a woman could easily slip through.

In what had to be a smuggler's dream, transloading of commercial traffic from Iran occurred behind a wall in Iran and without Iraqi personnel present. This arrangement makes it easy to hide something beneath the load. Once on the Iraqi side, the border



Vehicle inspection.

personnel did nothing more than a cursory inspection. If asked to download a vehicle for inspection they would refuse, claiming they did not have the workers or equipment. It was unusual to see cargo in boxes or loaded on pallets. Faced with a truck-load of melons, you would have to download each by hand in order to check for hidden items. Even after providing the POE with backscatter radar systems and training, inspections of any kind really only happened when U.S. personnel were present to observe. When asked, POE personnel claimed they inspected everything, but they never seemed to find anything reflecting the influence of corruption and reach of the militias. Those in the ISF who would not cooperate with these Shia militias were threatened, targeted, and eventually transferred or killed.<sup>19</sup>

***Recently, the 3ID commander, pointed to suspected Iranian support of insurgents in Iraq, noting his troops have found numerous rocket-propelled grenades and other ordnance, including powerful explosive formed penetrator (EFP) munitions, with Iranian markings. They are being trucked in into Iraq from the border in Wasit province.***<sup>20</sup>

Near the end of my research, I came across a September 2007 report from the Wall Street Journal that reported the Pentagon was preparing to build a military base near the Iraq-Iran border to try to curtail the flow of advanced Iranian weaponry to Shiite militants across Iraq. The 3<sup>rd</sup> Infantry Division Commander also said they were planning to build fortified checkpoints on major highways leading from the Iranian border to Baghdad. “We’ve got a major problem with Iranian munitions streaming into Iraq. This Iranian interference is troubling and we have to stop it.” Reading the article, I began to smile as a project we worked was finally bearing fruit. We had continuously recommended in our weekly updates to the IAG that we should build a fort with sufficient forces that would allow us to live on the border, collect intelligence, and interdict the smuggling routes and illegal activity. Before we left, our plans for such a fort were well on their way to approval and we left it to our replacements to carry the ball the rest of the way. The article notes that the new outpost will have quarters for at least 200 Soldiers. “Iran . . .will have to rethink how they do things, and the smugglers will have to rethink how they do things.”. . . However, we cannot rely simply

on technology, our teams provided backscatter machines to the POE and trained the Iraqis in its use but these machines have limitations.<sup>21</sup>

Lieutenant General Odierno noted in mid 2007, “It’s clear to us that there are networks that are smuggling weapons, both EFP IEDs as well as mortar and other capabilities from Iran into Iraq . . . there are networks that have been established directly to extremists here in Iraq . . .we believe some training is also going on inside of Iran . . .we continue to go after their networks with the Iraqi security force . . . and we will continue to do so until they stop bringing these weapons.”<sup>22</sup>

## **The Region Border Enforcement Division**

***George Tenet writes that the greatest disappointment of postwar Iraq was trying to create an Iraqi army. By 2004, it was clear the training effort was going badly and the discipline of the units was poor, often dissolving in battle. We failed to understand the Iraqi cultural and its Army . . . Iraqi officials seemed to understand we were building an army with no logistics or support and no respected leadership above the battalion, nor any effective command and control capability.***<sup>23</sup>

In May 2007 the Commander, MNF-I, wrote, “Capable ISF are critical to our effort to secure the Iraqi people . . . In watching the development of ISF over time, it has been very clear that unit leadership is the key element in achieving success in operations.”<sup>24</sup> The question is, how can we successfully train and sustain a force that lacks professionalism, cannot provide its own security, and is unable to retain its recruits; fewer than 40 percent of the trained recruits are still on the job today. This lack of capability in the ISF is the primary reason the target date for transferring authority in all 18 provinces continues to slip, compounded by equipment problems due to combat loss, theft, attrition, and poor maintenance. A ‘significant portion’ of U.S. issued equipment is now unusable.<sup>25</sup>

Enforcing the security of Iraq’s borders is the responsibility of the DBE, a unit of the Iraqi MoI. For us that translated to the Regional Border Enforcement Division and its two brigades located in Diyala and Wasit provinces. A former NATO commander observed that sectarianism, corruption, and Shiite

militias' influence are pervasive in the Interior Ministry.<sup>26</sup> Though the MoI claims he plans on removing corrupt leaders and instituting policies to eliminate corruption,<sup>27</sup> even the former chief of Iraq's Public Integrity Commission stated, "slogans about fighting corruption are only for propaganda."<sup>28</sup>

When we first arrived, the Wasit POE reported directly to the DBE. In effect, there was no unified commander responsible for border security, a fissure that enhanced corruption and illegal activities. The MoI later placed the POE under Regional Division. Additionally the Division Commander, a Shia', rarely visited the Sunni units in Diyala or resourced them appropriately. It did not take long to determine that the Region Border Police were poorly trained, undermanned, and lacked equipment. Many were hired because they were related to someone or had links to militias. Hence, they became senior officers overnight without any education or experience. One commander in the 1<sup>st</sup> Brigade was a "middle school graduate." Throughout our tour, we tried to model "what right looks like" and stressed the importance of a strong NCO Corps and the military decision making process, but we were unable to break their tradition of centralizing authority and power. "As Iraqi leaders observed NCOs within transition teams . . . they often commented that the American military is close-knit, with officers and NCOs working together."<sup>29</sup> In Iraq and the 3<sup>rd</sup> Region, we are just not there, yet.

## Evaluating the Iraqi Forces

*In January of 2006, a White House Press release noted that the coalition is helping to increase the border police to defend Iraq's frontiers and stop foreign terrorists from crossing into the country. Manning entrances by land, sea, and air ports across the country . . . the Coalition is embedding border police transition teams with Iraqi units . . . . Iraqi border forces are growing increasingly capable and taking on more responsibility.<sup>30</sup>*

In early 2007, as our team prepared to turn over the mission to our replacements, our Border Enforcement Division and its subordinates were clearly unable and unwilling to accomplish their mission. The IAG Commander seemed to echo this when he said, "Given the focus on Iraq's army and police to meet immediate security threats, the country's border guards remain a work in progress."<sup>31</sup>

We evaluated Iraqi units using a training readiness assessment (TRA), similar to a unit status report. The problem was the TRA questions required a simple yes or no and were so general that they tended to force the answer towards yes. For instance, if you ask, 'Does the unit have the ability to collect and disseminate information?' rather than, 'Can they disseminate information in a timely manner to the appropriate levels in order to action it (actionable intelligence)?' you'll get different answers. Our Iraqi units certainly could collect and disseminate information; they did so most often using couriers. We received copies of their reports 30 to 45 days after an event happened. Their use of computers to move information rapidly from point to point was almost non-existent primarily due to infrastructure, and without fuel to run the generators, they could only use the few on hand intermittently. What ISF units need is an assessment that helps them develop a vision for their unit and communicates issues to their chain of command.<sup>32</sup> If the goal was to declare a unit that could barely crawl as able to run (as in a crawl-walk-run model) then the TRA evaluation model was a success. But because the units were not increasingly capable and responsible, the evaluation was hardly the ground truth.

Americans may identify their cultural and ethnic backgrounds when asked. For instance one might be an Irish-American, however, we as individuals strongly identify with our nation and when national security is at risk or we are attacked, we are first and only Americans. In Iraq one is a member of a tribe, Shia', Sunni, militia, and an Iraqi last, if at all. The only way we will make a difference is if we instill in the Iraqi forces a sense of duty and professionalism as well as a true sense that they are Iraqi's first. This is something an evaluation will not fix.

## Intelligence Issues and the Fight for Knowledge

*How are EFPs coming into Iraq? "Iran's Revolutionary Guard Corps has established smuggling routes to transport men and supplies into Iraq."*<sup>33</sup>

The truth is that the Border Enforcement Division is not capable of executing intelligence-based operations. Regardless of the discipline you care to discuss, there are serious disconnects from the National to tactical to individual Soldier level that unless addressed will affect its ability to effectively perform

the mission and combat the corruption. Intelligence drives operations, but that requires an effective organizational design. In our headquarters, the operations, communications, and intelligence functions all occupied separate offices on opposite sides of the castle, much like boxers in their individual corners. Without an organizational structure to collect, analyze, report, or respond, you are executing or reacting to events while wearing a blindfold.

A transition team is an exceptional asset and well situated to fill information gaps in their AOR, however, our BTT went unused in this role. Compounding this, there were no standing border information or Theater priority intelligence requirements put out to the teams. Nor did the teams have appropriate tools or a reporting channel. A simple resolution would have been to provide the team with the Biometrics Automated Toolset that would have yielded big dividends by allowing the BTT to collect and report biometric data on the ISF. Further, MNF-I could share the products with Iraqi leadership to aid U.S., Coalition, and Iraqi efforts to identify nepotism, corruption, illegal activities, and links to Anti-Iraqi and Anti-Coalition Forces.

Still, we tried to report. Soon after arriving at Delta, we worked out a procedure with the 2X Cell at MNC-I to report information in an intelligence information report (IIR) format using the theater reporting tool called CIDNE (the acronym pronounced as ‘Sidney’ stands for Combined Information Data Network Exchange.) We set up a procedure so the teams could write IIRs and submit them to the regional team reports officer account. We reviewed and edited the draft IIRs prior to sending them to MNC-I. This worked well and allowed us to report information until a staff rotation at MNC-I. Eventually we worked it out again, but it was clear that collection capability of the transition teams was not valued.

Every Soldier comes across bits of information that may make no sense to him. We refer to this as *Every Soldier is a Sensor*, a doctrinal concept that reaches down to the individual Soldier to generate reporting that when entered into appropriate systems and fused produces actionable intelligence. By extension so is every unit or team. It is clear that neither the senior leadership in theater nor the teams understood the greater role they played in the ‘fight for knowledge’<sup>34</sup> or the development of ‘Dominant Battlespace Knowledge’.<sup>35,36</sup> Some refer to this as

‘operationalizing intelligence’,<sup>37</sup> but without formal reporting requirements or reporting channels we failed to enable this key Intelligence Operations tool for transition teams. Nor has the Iraqi government or MoI created an organization capable of directing, gathering or providing dominant battlespace knowledge to its forces.”<sup>38</sup>

## The Fight for Knowledge: Task Force Phantom

***Serving on a military transition team may be the most important job in Iraq today, with members working with Iraqi units to realize President Bush’s promise: “As the Iraqis stand up. We’ll stand down.”<sup>39</sup>***

Multiple new articles by reporters, both military and civilian, document the flow of weapons and trainers from Iraq. A senior U.S. commander claimed in one, that 50 officers of the Revolutionary Guard’s elite Qods Force were training militants in Iraq. The Christian Science Monitor reported that Iranian EFPs are used to attack U.S. forces and some captured homemade video shows preparations for Shiite militant attacks using 107-mm rockets . . . . there was “no doubt” the rockets—still with some packing grease, color-coded and with English lettering for export were made in Iran.”<sup>40</sup> The questions are how did they get there, and who are the key players who are involved in the smuggling.

Answering these questions requires intelligence, surveillance, and reconnaissance (ISR) assets combined with direct action units, such as Task Force (TF) Phantom. Late in our tour, we participated in an operation to close the POEs throughout Iraq for 72 hours. Originally, our POE was supposed to close permanently, but the Shia dominated government, provincial governor, and border officials linked to Badr Corps (SCIRI) and Madhi Militia (Muqtada al-Sadr) would not let this cash cow close. Even so, in what we viewed as recognition of the Iraq-Iran Border problem, MNC-I gave TF Phantom a mix of ISR collectors, analyst, aviation, and long-range surveillance troops, a warning order to move from the Syrian to the Iranian Border and to conduct operations out of Camp Delta.

The TF was equipped with sensors that could detect vehicles and people and transmit the data for analysis<sup>41</sup> as well as airborne systems capable of sending imagery in real time to teams on the

ground. In one Syrian operation, TF Phantom targeted twelve specific targets linked to cross-border trafficking of bomb-making materials and provided the actionable intelligence that 3<sup>rd</sup> Armored Cavalry Regiment needed to interdict the targets and verify movements of men and materiel from Syria to Iraq. Following the “Fight for Knowledge” construct, the TF continued to gather information after the operation ended looking for changes or new activity to drive future operations. When it came to high tech devices and equipment, our teams had radios, weapons and personal locator devices, but as noted earlier we had limited ability to report information, much less receive intelligence while on the border. TF Phantom would have provided that link; had this unit actually relocated to the operational area, our ability to identify and target illegal activities including IEDs flowing into Iraq would have been significant.<sup>42</sup>

## Conclusions

**Camp Liberty, Iraq (November 2007). Senior military commanders now portray the intransigence of Iraq's Shiite-dominated government as the key threat facing the U.S. effort in Iraq.<sup>43</sup>**

Iraq is a complex society and we would do well to remember the lessons from the first Russian battle for Grozny, Chechnya in 1994. The lack of knowledge concerning historical, national, religious, geographical, and other human factors seriously influenced operations and caused serious errors when dealing with the Chechens who, once insulted or mistreated, became supporters or active fighters themselves.<sup>44</sup> We must understand the fight for knowledge and the role teams play in information collection.<sup>45</sup>

Eleven-man teams are too small to execute this mission. We became well paid security guards whenever our team leader wanted to visit another border fort. The CALL report recommended the addition of 4 to 6 personnel for use as gunners and drivers to enhance the team’s capability. However, I believe that an 11 to 12 man infantry squad would be more appropriate, provide the necessary security, and allow individual advisors to break away from the team.

What is the future role of the conventional force in advisory operations? Recently, the Army Action Plan for Stability Operations directed the U.S. Army

Training and Doctrine Command to assess and make recommendations on the appropriate roles and missions of general-purpose forces to conduct Foreign Internal Defense (FID) training . . . to ensure general purpose force doctrine includes; nation assistance; peace operations, foreign humanitarian assistance and pursue the establishment of additional skill identifiers/specialty skill identifiers as appropriate. This is critical for past team members, so that the Army can identify advisors for future missions. Further, advising host nation ministries and training of security forces (police, military, and border guards) must be included.<sup>46</sup>

This is an unconventional mission, and the use of conventional forces without proper training is a recipe for disaster. Advisor training must focus on the critical FID mission, using classroom learning and role playing. The training now conducted at Fort Riley, Kansas is a good start, but our training never came close. Advisors should understand how we build, document, and train forces. They should receive language training, and instruction in cultural awareness, history, including intensive understanding of their AOR and the personalities from provincial governors to local sheiks. One model might be the course sponsored by the U.S. Institute for Military Assistance, JFK Special Warfare Center, Fort Bragg, North Carolina.

Advisors should have a three to four year tour of duty focused on a specific unit. After an intensive six month course, teams should rotate at six month intervals. Thus, an Iraqi unit would get to know two teams and their personalities for a three year period and build a solid long-term relationship that transcends one year tours. The team leader should have previous command in theater at the battalion or brigade level or service on a previous team.

If we are to have any success in training and advising the security forces of Iraq, it is critical that transition teams fall under the operational control (OPCON) of an organization that understands the mission and has the ability to command, control, and fully support these teams. Clearly, the IAG was not up to the task, and recently had its role changed to receiving, training and onward movement of the teams with command and control going to the local BCT in an AOR. While this may work in some cases, it has resulted in other teams being diverted to other missions by the command to which they were OPCON.

In November 2007, Iraq's most influential Shiite politician and leader of the Supreme Islamic Iraq Council said that the U.S. had not backed up claims that Iran is fueling violence.<sup>47</sup> However, in the same month a group of Shiite Muslims from Southern Iraq signed a petition condemning Iran for fomenting violence in Iraq.<sup>48</sup> However, experience and a recent National Intelligence Estimate suggest that the militias, Iranian backed or not, have significant influence in the DBE and other security forces.<sup>49</sup>

Recently an American platoon pinned down by fire called for backup. Less than a mile away, a powerful Shiite parliament member stood inside the office of the Iraqi Army commander and prevented the Iraqi Army from responding.<sup>50</sup> It is clear that, "A dysfunctional Iraqi government has made minimal progress toward unifying the country's religious and ethnic sects and the number of combat ready Iraqi army units dropped over the summer."<sup>51,52</sup>

I agree with General (Retired) Colin Powell, we broke it, but in fixing what we broke, let's not use an assessment tool for ISF tilted to produce a result that suggests they are capable of manning, training, and resourcing a force to successfully perform the border security mission.

For those who get the opportunity to advise, train and mentor another nation's Army I will tell you regardless of the frustrations, it is professionally, as well as personally rewarding. Let's set the standard high and man, train, equip the teams appropriately, and shoot for success. General (Retired) Wesley Clark recently noted, "Nation-building, however ideologically repulsive some may find it, is a capability that a superpower sometimes needs."<sup>53</sup>

## Endnotes

14. J. Kent, "ISF Look to Develop NCO Corps," *Victory Times*, Vol. II, Issue 124, 2 November 2006.

15. "Generals Ask if Iraqis Can Hold U.S.'s Gains," Associated Press, accessed 25 June 2007 at <http://www.msnbc.msn.com/id/19409402/>.

16. The Coalition Provisional Authority Press Releases, "Bremer Announces Iraqi Border Security Initiative," accessed 8 August 2007 at [http://www.cpa-iraq.org/pressreleases/20040315\\_Border-Remarks\\_31503.html](http://www.cpa-iraq.org/pressreleases/20040315_Border-Remarks_31503.html).

17. The Coalition Provisional Authority Press Releases, "Border Crossing Points between Iraq and Iran to be Reduced to Three," accessed 8 August 2007 at [http://www.cpa-iraq.org/pressreleases/20040315\\_iran\\_border.html](http://www.cpa-iraq.org/pressreleases/20040315_iran_border.html).

18. Michael Isikoff and Mark Hosenball, "Deadly Triggers, Is Iran Providing Devices that Help Insurgents Detonate IEDs in Iraq?"

*Newsweek*, 24 January 2007 accessed 12 August 2007 at <http://www.msnbc.msn.com/id/16795765/site/newsweek>.

19. Major David Voorhies, "MiTT HAPPENS: *Insight into Advising the Iraqi Army*," Combined Arms Tactics Directorate, USAIC, 20 April 2007 accessed 21 September 2007 at <https://www.us.army.mil/suite/doc/8725802>.

20. Gerry J. Gilmore, "Commander Says Iraq Surge Operations Have 'Significant' Impact Saturday," *American Forces Press Service*, 14 July 2007, MNF-I Web Site accessed 8 August 2007 at [http://www.mnf-iraq.com/index.php?option=com\\_content&task=view&id=12841&Itemid=1](http://www.mnf-iraq.com/index.php?option=com_content&task=view&id=12841&Itemid=1)

21. *Wall Street Journal Report: U.S. Plans Base near Iraq-Iran Border, Installation Reportedly Intended to Curtail Flow of Arms to Shiite Militants*, 10 September 2007, accessed on 10 September 2007 at <http://www.msnbc.msn.com/id/20687880/>.

22. Briefing by LTG Ray Odierno, CG, MNC-I and Staff Lt. Gen. Aboud Ganbar, Commander of Baghdad Operations, Fardh Al-Qanoon. *Topic: Current Operations*, 26 July 2007, accessed on 9 August 2007 at [http://www.mnf-iraq.com/index.php?option=com\\_content&task=view&id=13047&Itemid=1](http://www.mnf-iraq.com/index.php?option=com_content&task=view&id=13047&Itemid=1)

23. George Tenet with Bill Harlow, "At the Center of the Storm," (New York: Harper Collins Publishers, 2007).

24. David H. Petraeus, General, USA, Memorandum for Iraqi Security Force Transition Team Members; Subject: Commander's Guidance and Expectations. 8 May 2007.

25. "Another Delay in Returning Iraq to Local Control, Pentagon Report Highlights Difficulties in Developing Iraq Police Forces," Associated Press, 20 September 2007 accessed at <http://www.msnbc.msn.com/id/20883940>.

26. Jim Michaels, "Study: ISF at Least a Year from Taking Control," *USA Today*, 6 September 2007.

27. Report to Congress, Submitted pursuant to U.S. Policy in Iraq Act, Section 1227 (c) of the National Defense Authorization Act for Fiscal Year 2006 (PL 109-163), 5 January 2007, accessed on 11 August 2007 at <http://www.state.gov/p/ne/a/rls/rpt/1227/80963.htm>.

28. Alissa J. Rubin, "The Struggle for Iraq: Blaming Politics, Iraqi Anti-graft Official Vows to Quit," *New York Times*, 7 September 2007.

29. J. Kent, "BTT Helping to Keep Iraq Safe," *Victory Times*, Vol. II, Issue 108, 26 September 2006.

30. Fact Sheet: Progress and the Work Ahead in Iraq, Office of the Press Secretary, The White House, 10 January 2006, accessed 11 Aug 2007 at <http://www.whitehouse.gov/news/releases/2006/01/20060110.html>.

31. Bureau of International Information Programs, U.S. Department of State, "Coalition Helps Iraqis Build Strong National Defense," 29 August 2006, accessed 12 Aug 2007 at <http://london.usembassy.gov/iraq396.html>.

32. *Report of the Oversight and Investigations Subcommittee, "Stand Up and Be Counted: The Continuing Challenge of Building the ISF"*, U.S. House of Representatives, 2007 accessed 6 August 2007 at [http://armedservices.house.gov/pdfs/OI\\_ISFreport062707/OI\\_Report\\_FINAL.pdf](http://armedservices.house.gov/pdfs/OI_ISFreport062707/OI_Report_FINAL.pdf).

33. Jed Babbin, "Intrusive Facts," *Real Clear Politics*, 14 December 2006, accessed 3 June 2007 at [http://www.realclearpolitics.com/articles/2006/12/intrusive\\_facts.html](http://www.realclearpolitics.com/articles/2006/12/intrusive_facts.html).
34. Deputy Undersecretary of Defense (Science and Technology), *Nine Sub-Capabilities of ISR*, (Washington D.C.: Department of Defense, 2004), cited in "What Do We Mean by Urban Dominance?" *Military Intelligence Professional Bulletin*, April-June 2005, Michael Spears.
35. Arthur K. Cebrowski, Vice Admiral (Ret.), Director, Office of Force Transformation, Office of the Secretary of Defense in a statement "*Elements of Defense Transformation*" before the House Armed Services Committee, 26 February 2004.
36. Elements of Defense Transformation, 13 December 2004 at [http://www.ofot.osd.milllibrarylibrary.cfm?libcol=6#document\\_383](http://www.ofot.osd.milllibrarylibrary.cfm?libcol=6#document_383).
37. Stephen A. Cambone, Undersecretary of Defense for Intelligence in a statement before the Senate Armed Services Committee Strategic Forces Subcommittee, 7 April 2004.
38. Keith B. Alexander, Lieutenant General, DA G2, in a statement before the Senate Armed Services Committee, Strategic Forces Subcommittee, 7 April 2004.
39. Jim Garamone, "Transition Teams Coach, Mentor Iraqi Units," *DefenseLink*, 13 May 2006, accessed 3 June 2007 at <http://www.defenselink.mil/news/newsarticle.aspx?id=15767>.
40. Scott Peterson, "An Intensifying US Campaign Against Iran," *The Christian Science Monitor*, 24 August 2007, accessed 24 August 2007 at <http://ebird.afis.mil/ebfiles/e20070824538568.html>.
41. Robert P. Whalen, Jr., Lieutenant Colonel, USA, "Everything Old is New Again: Task Force Phantom in the Iraq War," *Military Review*, May-June 2007.
42. Michael R. Gordon and Bernard E. Trainor, General, *COBRA II, The Inside Story of the Invasion and Occupation of Iraq*, (New York: Random House, Inc. 2006)
43. Thomas E. Ricks, "Iraqis Wasting an Opportunity, U.S. Officers Say" *Washington Post*, 15 November 2007, accessed 15 November 2007 at <http://www.msnbc.msn.com/id/21781092/>.
44. Michael Spears, Michael, "What do We Mean by Urban Dominance?" *Military Intelligence Professional Bulletin*, April-June 2005.
45. Newton L. Gingrich with Mark Kester, "From Stabilizing to Transforming Societies, the Key to American Security," *The Fletcher Forum of World Affairs*, Summer 2004: 28, 2.
46. Department of the Army, HQDA G35 Strategy, Plans and Policy, "*Army Action Plan for Stability Operations*" Army Campaign Plan Decision Point 105 Approved 2 August 2007, 8.
47. "Leading Shiite Disputes U.S. Claim That Iran Is Feeding Violence," *Arizona Daily Star*, 26 November 2007.
48. Amit R. Paley and Sudarsan Raghavan, "Shiites in S. Iraq Rebuke Tehran Petition: Calls for U.N. Probe into Iran's Influence, Sheiks Say". *The Washington Post*, 22 November 2007, A25.
49. "U.S. Report Sees Precarious Iraqi Government," *Associated Press*, accessed on 23 August 2007 at <http://www.msnbc.msn.com/id/20408600/>.
50. Joshua Partlow, "Tactics on the Ground: Building Up the Iraqi Army," *The Washington Post*, 4 September 2007.
51. Kathy Kiely, "Critical GAO Review Starts Series of Reports on Iraq," *USA Today*, 5 September 2007
52. National Intelligence Council, National Intelligence Estimate, "*Prospects for Iraq's Stability: Some Security Progress but Political Reconciliation Elusive*," August 2007.
53. Wesley Clark, General (Ret.), "The Next War," *The Washington Post*, 16 September 2007.

## 2009 Army Intelligence CSM/SGM Conference



The Headquarters, Department of the Army, Deputy Chief of Staff G2 Sergeant Major, the MI Corps Command Sergeant Major, and the U.S. Army Intelligence and Security Command Sergeant Major cordially invite you to attend the 2009 Army Intelligence Command Sergeants Major/Sergeants Major Conference, 3 to 6 March 2009, at Fort Huachuca, Arizona. We welcome your support for this conference as we strive to support our Global MI Missions and Organizations.



The theme for this year's conference is "The Future of Intelligence is Now—Technology Advancing Intelligence Capabilities." The conference is open to all MI CSMs/SGMs (Active, Retired, Army Reserve, and National Guard), Division CSMs, Special Mission Units CSM/SGMs, all BSTB CSMs (MOS immaterial), and all MICO 1SGs.

More messages to the field, as well as the stand up of the conference website (available on 7 November 2008 on the Intelligence Knowledge Network (IKN) at <https://icon.army.mil>, Upcoming Events) will occur over the next few weeks. The point of contact is SGM Phil Sharper at COM: 520-538-1211; DSN: 879-1211 or [phillip.sharper@us.army.mil](mailto:phillip.sharper@us.army.mil) or [phillip.sharper@conus.army.mil](mailto:phillip.sharper@conus.army.mil).

# Synthesis: Intelligence Support for Disaster



by Lieutenant Colonel Robert A. Blew, U.S. Army, Retired

## Introduction

The conditions created by combat are similar to disaster. Both require a wide range of capabilities to which to respond and recover. Indeed, war is arguably the worst type of man-made disaster. For this reason, the Department of Defense (DOD) is a major part of the overall plan for national disaster, the National Response Framework (NRF).<sup>1</sup> The capabilities of DOD are so diverse that it's one of only two federal departments that has a role in each of the NRF Emergency Support Functional (ESF) areas, and is the lead for ESF9, Search and Rescue.

The U.S. military has a long history in disaster relief, as well as other Defense Support to Civil Authorities (DSCA) missions. However, one key capability is used haphazardly—its abilities to support Disaster Intelligence (DISINT). Though ESF9 implies Intelligence, there is little understanding of how knowledge is disrupted during a calamity, of secondary disasters caused by information loss, and how to comprehend non-human adversity. It is not generally known how to apply the Intelligence Cycle of tasking, collection, processing and dissemination for the purpose of saving lives and infrastructure.

Current policy is that Intelligence supports the functions of disaster response. "Intelligence/Investigation is an optional sixth functional area that is activated on a case-by-case basis."<sup>2</sup> In the National Incident Management System (NIMS), Intelligence isn't ignored but is part of the NIMS Planning Function. This has the advantage that Intelligence is integrated in the Incident Command and Staff. However, when DOD provides DISINT support, it is probably a meta-disaster that requires a separate Intelligence function. In any case DOD personnel remain in the DOD chain of command and operational control.

## Disaster's Effects on Information

Information is fragile, as susceptible to damage and change as landscape, structures, and lives. Meaning and interpretation change after disaster. An assumption is that some facts are immutable. There is a sense of unreality after catastrophe—Terra Firma is not so firma, but can be like ocean waves. Water does not always seek its lowest level, it can flow far and deep up on land. Insubstantial air can pick up and carry heavy items long distances, or drive fragile straw through telephone poles. Even if the world looks the same, everything has changed.

From an Intelligence perspective, certainties are invalidated by disaster and need verification. A short distance from one place to another can be so altered that knowledge of locations, layouts and routes is useless. People may realize that what they know is no longer true, but are temporarily unable to adapt to all the emerging reality, resisting even at the risk of life. If the disaster is dynamic, change will continue requiring continual monitoring.

Lives depend on quickly collecting and analyzing information, then providing it in a usable form. Decisions for priorities must have accurate situational awareness. Instructions must be understood by users. Those who can help, and those who need help, will not have the same priorities or vocabulary. One of the purposes of NIMS is to standardize terminology for emergency responders. This is similar to military Joint Operations terminology, but for Interagency communication among federal, state, local, non-governmental and international organizations. This does not include non-emergency personnel, ad hoc response and victims.

After a disaster there are surfeits and deficits of information, few filters to screen for relevance, lim-

ited cues on questions to ask, and contrast to discriminate credibility. This is when misinformation enters information flow. Confusion is exacerbated by rumor from official and unofficial sources. These delusive “facts” become accepted by traumatized decision makers. Once adopted as true, false information is self verifying making it difficult to discredit.

The conditions of uncertainty further erode reasoning. Actions have undesired results, cognition is paralyzed; procedures are followed blindly. Discerning patterns in the chaos is problematic. How does one neutralize a foe that is ruthless in destroying lives yet arbitrary in its victims? How does one predict events that are both slow degradation and sudden calamity? Precursors are unrecognized, or indicate multiple possibilities. Evidence is untrustworthy when reliability and validation aren’t established.

The loss/irrelevance of records, plans, accountability, retrieval, and storage create opportunities that can be exploited, especially if likely contingencies are anticipated. Intentional and unintentional fraud happens when massive funds and resources are rushed in and distributed. Understandably, saving lives is more important than paper work.

Disasters create vulnerabilities, adding hazards to an already stunned population. These secondary threats may go unrecognized until too late to mitigate. Initiating an incident to draw in responders is an ambush tactic. Fears do not have to be real to cause panic. Rumors, scapegoating, looting, barricading, hoarding, stress, mass exodus and convergence, and vigilantes can cause more damage than the original disaster.

This stressful situation is fraught with error, with constantly changing priorities. It’s an overwhelming information management task to track the massive and rapid tempo of needs, questions, and solutions. Add to this, determining who needs what information, how to deliver, updating and correcting, while keeping back other information until needed. All this is done continuously without respite to regroup. DSCA can provide personnel to allow rest and more breadth to deal with the volume.

Information is never independent. Impacts to one cascades to other information. Isolated information is worthless. How information interrelates gives value. Gaps may not be apparent, resulting in false correlations. These include combining unrelated information and failure to link related information. Complete may seem incomplete while incomplete

appears complete. Adding to this chaos, desirable results may be achieved by inaccurate information. These create false lessons learned, setting the stage for future disasters. Unlike an incident that is limited in duration, the effects of disaster endure long after, spreading globally. In an incident Intelligence is for resolution. In disaster Intelligence is for accommodation to emerging circumstances.

Disaster scrambles context and sequence, as changing the place of one word in a sentence changes or reverses meaning, or renders it meaningless. Problems are considered solved that are not. Effort is wasted sending unneeded help. Solutions are withdrawn too soon or not sent soon enough. Putting data in order is labor intensive, delaying priorities and planning which may be based on invalid information. Direct observation is required to adjust implementing plans. Intelligence is best when part is actively in the field, reaching back for the strategic picture, not only passively isolated in fusion centers.

In this disrupted information environment, it is difficult to be noticed. What was valuable information before may not be afterwards, but still treated so due to habit. Calm factual objective reporting may mean critical problems aren’t acted on. Accuracy is sacrificed as exaggeration becomes necessary to gain significance above other needs.

After the disaster it’s a given there will be criticism. Why was information unknown or shared? Why were critical reports not acted upon? Why were decisions made that hindsight concludes were wrong? Intelligence disasters are defined as lack of information prior to an event. Blame is placed, despite restrictions that interfered with Intelligence processes.

Those who are involved in counterinsurgency (COIN) and counterterrorism Intelligence will recognize the similarities between the complexities and ambiguities of those and meta-disasters. Undoubtedly many who work in Emergency Planning Intelligence positions initially learned their craft in the military, which gives the advantage that they will know what to ask DSCA for.

## **What DSCA DISINT Support Provides**

Disasters require Intelligence to understand the situation and shape solutions. Job Books for the NIMS Planning Section Intelligence positions list duties familiar to DOD Intelligence. In a pinch an in-route review of these would help to work with NIMS staff, though prior instruction in DISINT is preferred.<sup>3</sup>

The basic questions DISINT answers are similar to military ones. What, where, and when is the mission? How many are hurt and how? What are the needs for food, water, shelter, medical care, and transportation? Where are the needs and resources, how to connect the two and when needed by? What interferes with the mission? What infrastructure is damaged? What can be saved? What needs to be repaired and what can wait?

DOD support to the NRF is secondary to its Homeland Defense (HLD) mission. The Secretary of Defense approves DSCA to assure it does not compromise HLD. Furthermore, the authority to provide Intelligence support is separate and must include guidelines. Unlike other military operations, assets diverted to Homeland Security are kept to the minimum and returned as quickly as possible to HLD. Concurrently disasters impact the military. Enemy attack or natural disaster can threaten national security and neutralize military forces.

Large numbers of personnel are needed to survey and validate information, but they do not have to be in Intelligence. For some assessments preventive medicine, engineer, food service, chemical, National Guard Civil Support Teams, etc. have better backgrounds. All Soldiers receive basic instruction in observation and reporting. They also have equipment to operate in dangerous environments, and training to function under stress. With an orientation in NIMS and Interagency DISINT checklists, assigned personnel can perform basic tasks.

Not all DOD personnel will be from a disaster area. They are not immune to emotional impacts of the situation, but are less likely to have agendas from local affiliations, and more apt to be neutral and objective. On the other hand, advantage can be taken of those who have local knowledge and skills not usually of military use, but needed for relief efforts. This all assures that military assistance is interpreted as help to accept, not something suspicious to resist.

Secure communication may be unavailable or limited. Intelligence can provide dissemination, and links to share information between those who have with those who need. Usually needed information exists, such as satellite imagery, but locating and distributing it is a problem. Sophisticated analysis isn't required, but the ability to identify who "needs to have" is. Just passing information is insufficient. Sometimes a user will not understand

relevance and need an explanation. However, providing too much Intelligence is the same as giving none. This can be as simple as reporting an approaching storm and mentioning that it will interfere with operations and threaten victims without shelter. Sifting for what is needed, and maintaining the rest until needed, is a major task. This is simplified due to directives against collecting on U.S. citizens, so DOD Intelligence does not store and database what is collected.

A common Interagency practice is mutual aid, similar to mutual support of military forces. It is prohibitively expensive for each jurisdiction to have every emergency capability. With a network of agreements one can concentrate resources where needed, while still covering other locations. Agreements between agencies spread interlinking capability, and the burden. Similar agreements can be done for DSCA DISINT.

Normally National Guards provide military capabilities for domestic needs, while also being a reserve for Federal active forces. In today's world active services need to back the reserves that are deployed. Under DOD Directive 3025.16, "Emergency Preparedness Liaison Officers (EPLOs),"<sup>4</sup> there is a system to support the NRF and perform local coordination.

The emergency phases are Prepare, Respond, Recover and Mitigate.<sup>5</sup> Intelligence prepares by gathering baseline data, entering mutual aid agreements, and familiarizing with NIMS per Homeland Security Presidential Directive 5, "Management of Domestic Incidents".<sup>6</sup> DSCA DISINT is part of response to gain situational awareness, consolidate sustainment, and then transition back to civil authority. Intelligence contributes to prior preparation and post mitigation by analysis of vulnerabilities and lessons learned. The migration/prepare phase is when continuity and resilience are improved. This threat reduction decreases the need for future DSCA.

Operations Security (OPSEC) applies to DSCA. OPSEC is protecting sensitive information that can be identified by observing behavior. A disaster can reveal how DOD will respond to future incidents; identify unit missions and special skills; classified means of information collection; weaknesses in preparedness, and vulnerabilities. For this reason it's necessary in some cases to "write for release" or designate with Controlled Unclassified Information (CUI).<sup>7</sup> What could be used against national security is noted and recommendations made.

## Operations Security (OPSEC) PUBLIC SAFETY AWARENESS CARD

OPSEC: Five-step risk-management analytical process used by military and security professionals to protect sensitive information that adversaries could use to their advantage and your disadvantage.

### OPSEC PROCESS:

- Identify Critical Information
- Analyze Threat
- Analyze Vulnerability
- Assess Risk
- Apply Countermeasures

### ADVERSARY:

Can be any individual or group who is collecting information about you and your organization and intends to use this information to defeat your operations or plan an attack against you and your resources. This can include gangs, terrorists, extremists, organized criminals, drug traffickers and computer hackers.

Examples of Critical Information that should be protected:

- Current and Future Operations
- Current and Future Investigations
- Usernames and Passwords
- Official Access/Identification cards
- Travel Itineraries
- Agency/Special Teams Capabilities and Limitations
- Personal Identification Information
- Entry/Exit/Check Point Security Procedures
- Budget Information
- Lessons Learned and After Action Reports (AAR)
- Critical communications via phone or radios
- Desktops, Laptops, Disks and Flash Drives

Version 1, Page 1, February 2007, August Vernon [fdtac@yahoo.com](mailto:fdtac@yahoo.com)

*Response sheet is for training and informational purposes only. Please utilize local guidelines and procedures.*

**OPSEC Public Safety Awareness Card is available at <http://www.wiaai.com/Operations%20Security.pdf>.**

Monitoring military disaster effectiveness is vital. Minimizing DSCA requires constant review that only needed capabilities are provided to the right place at the right time and duration, rotating assets in and out as the situation evolves. Measures of effectiveness (MOE) are tailored to gauge effects and unintended consequences. The tendency is to create matrices of easily defined and measured effort. It is gratifying to report amount of supplies and man hours, but what is needed are end states. End states are fluid, ill defined, and not conducive to measurement. DISINT MOE isn't for those providing help, but those assisted.

DSCA support can be categorized as *Supplement, Augment, Exclusive, and Replace*. *Supplement* is providing more of what exists, such as personnel. *Augment* is improvements on existing resources, like an unmanned aerial system for continuous imagery. *Exclusive* capabilities are those that are unique to DOD. Exclusive assets are potentially classified, and Intelligence from them needs to be sanitized. The last type of support is to *replace* those assets that have been lost, damaged or otherwise unavailable.

Duration and size of support provided must be considered. Configuring, numbers engaged, deployment, disengagement, return, reconfigure, and transition back is time unavailable for HLD. The ideal is minimal time and amount, but providing

## Operations Security (OPSEC) PUBLIC SAFETY AWARENESS CARD

### Examples of VULNERABILITIES:

- Unsecured e-mail accounts
- Use of home e-mail for official business
- No trash management plans to stop "dumpster diving"
- No shredding of sensitive documents or plans
- Information posted in agency procedures and guidelines
- Units with no radio encryption
- Extensive amounts of photos of public safety equipment and people available
- Leaving mission briefs and sensitive documents in your car
- Web Cams (Official and Unofficial)
- Chat groups
- Discussing information with friends and family
- Releasing unscreened information to the media

### BENEFITS:

Can benefit Law Enforcement, Fire, EMS, Emergency Management and other agencies. The effective use of an OPSEC program will help ensure that agencies and special teams will be able to conduct their activities:

- No injuries or loss of life to response personnel
- Protect personnel's families
- Safe and secure arrest of "bad guys"
- Protection of vital information and plans
- Protection of infrastructure
- Ensuring the safety and security of a planned events

### INFORMATION:

For additional information reference OPSEC for Public Safety please visit the Interagency OPSEC Support Staff [www.ioss.gov](http://www.ioss.gov)

Version 1, Page 2, February 2007, August Vernon [fdtac@yahoo.com](mailto:fdtac@yahoo.com)

*Response sheet is for training and informational purposes only. Please utilize local guidelines and procedures.*

too little or withdrawing too soon can have more negative impact than no support at all. There are always costs even if minimized. Like war, the possibility exists that a person or equipment may not return. One way to assure minimum support and cost is to provide rapid support. For example controlling a fire (fight) is easiest early on, suppressing it while it is still small. Waiting until a conflagration means more time, funds, resources, and lives lost. DISINT can assist EPLOs to determine which incidents will expand.

One caution is that disaster scenes blend with crime scenes. Intelligence support to save lives is generally acceptable, but supporting law enforcement and investigations is another matter. A toxic plume spreading toward a city is a disaster. If the plume is from an industrial accident then there is criminal liability. If the plume is a terrorist act then the disaster and crime scene blend on an international scale. Both meta-crime and disaster scenes need security, which requires Intelligence.

Disaster rips away concealment. The aftermath exposes lost, hidden, and secret information. Criminal activity can be exposed by ESF9, or incidentally revealed during analysis. A disaster may lead to civil unrest that requires force to quell rioting, looting, securing government facilities, protect limited resources

and civil rights. These are all areas that Intelligence would have a role, but may be perceived negatively.

## **DISINT Benefits to DOD**

In a perfect world Intelligence for National Security, HLD and Law Enforcement are isolated from DISINT. But then a perfect world would not need military and police forces, have war and crime, or suffer from disasters. Given this reality, rather than avoid involvement, DOD should prepare to support, and position itself to benefit from involvement. One of the benefits is cross fertilization of various Intelligence fields.

At the beginning of the article similarities between disasters and combat were noted. A serendipity is that skills honed for one applies to the other. The fog of war impacts information the same as the fog of disaster. What better training than disasters to prepare against a ruthless enemy that acts irrationally, creates conditions of uncertainty, and is literally inhuman and uncivilized. In addition, this real world experience occurs when conditions are not optimal, urgency is immediate, there is no script, and immediate solutions are required without full information. This applies to the full spectrum of military operations, not just COIN. In today's world, missions take place among civilian populations and infrastructure. Disaster support is a benevolent activity in that context.

Maintaining DOD Intelligence is critical and expensive. Since the capability must exist, it makes financial sense to leverage for other appropriate purposes. Intelligence skills must be practiced or they deteriorate, and take years to develop. It does not make sense to let investments deteriorate from lack of use, or limit to a single purpose.

Interagency operations are the norm. No single agency can do everything, or operate without considering other stakeholders. Working with other agencies allows developing expertise in a smaller set of skills, sharing costs, and gaining synergy from mutual support. This is beyond coordination to avoid inadvertent interference, this requires collaboration to unify effort.

Real disasters, training exercises, and special events provide opportunity to work with agencies that will be encountered again. Major disasters can destroy the means to respond, changing an emergency into a disaster requiring outside help. For situations where developed solutions and procedures do not apply, one must have an Interagency network. If DSCA isn't engaged there are still strategic lessons for Defense Critical Infrastructure Protection.

Intelligence shies from publicity, preferring anonymity. What is known is from failures, with speculations based on fear of the unknown. Such biased information vacuums foster negative rumor. The perception of Intelligence would be more positive if there are activities that can be public.

## **Conclusion**

This article does not address DISINT techniques, the history of DSCA, and the layers of disaster operations. Nor did it cover legitimate and fanciful concerns about Intelligence for humanitarian purposes, other DSCA Intelligence, interoperability, dual use, and information fusion. The intent is to introduce DSCA DISINT for the NRF. It gives an idea of why it's needed, possible support, and the eclectic benefits to DOD Intelligence.

Disasters will happen. Some will require DSCA, and a portion of DOD will be in a disaster area, if not the target. Disaster degrades HLD, especially if unprepared. Support to DISINT is part of HLD. When DOD is required for a disaster, it will be multiple overwhelming incidents. Such situations threaten national security, the ability to protect the nation, and increases vulnerability to further attacks or disasters. It behooves DOD Intelligence to develop its roles in NRF and NIMS, to include minor events. As in war, waiting till it begins is too late. 

## **Endnotes**

1. The NRF is available at <http://www.fema.gov/emergency/nrf/mainindex.htm>.
2. NIMS, IV. Command and Management, item A. Incident Command System, page 44. The same phrase is in previous versions at <http://www.fema.gov/pdf/emergency/nrf/nrf-nims.pdf>.
3. Job books are available on the NRF website under "Planning Functions" at <http://www.learningservices.us/fema/taskbooks/showCadres.cfm?ID=11>.
4. Go to <http://www.dtic.mil/whs/directives/corres/html/302516.htm>.
5. The Understand, Shape, Engage, Consolidate, Transition model in RAND's MG 428/2-JFCOM, "People Make the City," at <http://www.rand.org/pubs/monographs/MG428.2/> is more appropriate for the Intelligence Cycle.
6. See items (9) (18) (19) at <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html>.
7. Presidential Memo, Designation and Sharing CUI at <http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html>.

*Robert Blew began his Army Reserve career in Intelligence as a team commander, instructor, and operations officer. After a stint with a Combat Engineer battalion as the S1, then Company Commander, he switched to Civil Affairs. His service includes Civil Military Officer, Medical Intelligence; Weapons of Mass Destruction Consequence Management Instructor at a Medical brigade and various Intelligence assignments. Mr. Blew holds an MA in Anthropology. He may be contacted at Robert.Blew@us.army.mil.*

# Secessionist Jihad: The Taliban's Struggle for Pashtunistan



## We Got it Wrong from the Start

In the days immediately following the 9/11 attacks, U.S. President George W. Bush convened his inner circle of foreign policy and military advisors at Camp David to determine the best way for the nation to respond. Recognizing the public mood, and wishing to differentiate his administration from the previous one, Bush pushed his team to develop a plan which would accomplish more than just “pound sand” with cruise missiles—he wanted action and tangible results. The evidence soon indicated that Osama Bin Laden’s Al-Qaeda (AQ) terrorist organization was the responsible party, and that it had planned, trained for and mounted the attack from the safe haven of Taliban-led Afghanistan. In a very straightforward way, the U.S. told the Taliban government that if it did not hand over Osama Bin Laden and the AQ organization, it would attack Afghanistan and replace the Taliban with a regime that would cooperate.<sup>1</sup>

And thus, the U.S. went to war against what they viewed as an Islamic Jihadist group which had seized control of a sovereign state and taken to harboring Islamic terrorists. As other invaders over the millennia had found before them, taking control of Afghanistan was relatively easy—but keeping control of it was another, more difficult task. By late November 2001,

by Major Michael D. Holmes

only two months after operations began, the Taliban had fled Kabul and the coalition of tribes and ethnic groups called the Northern Alliance swept into the southern strongholds of their Taliban enemies, supported by the Central Intelligence Agency, U.S. Special Forces and U.S. airpower.

But as we enter the seventh year of conflict in Afghanistan, the Taliban is resurgent. While it is far from controlling the country, the Taliban certainly controls intermittent stretches of southeast Afghanistan and threatens to establish footholds in any southern area not actually held and patrolled by a U.S. or NATO soldier. The Taliban is far from defeated. Why?

One of the reasons for our failure to subdue the Taliban insurgency may be that we have not identified the proper causes behind it. We have labeled the Taliban a jihadist movement and ascribed motives to them based on religious *traditionalist* goals, in part because that is what the Taliban itself has stated. But had we looked deeper, we might have found that the root causes behind the enduring and resilient nature of the Taliban have very little to do with religion, and much to do with an ancient ethnic struggle between the Pashtun people, and virtually everyone else in the region. And much like the enduring struggles of the former Yugoslavia, religion has become a blanket for what, in reality, is an ethnic and cultural struggle between tribes in a zero-sum game to control territory.

What is also clear, and in little dispute, is that the U.S. took great pains to avoid a confrontation with Afghanistan's neighbor, Pakistan. The U.S. government viewed the Taliban as a religious group, closely allied to AQ and other Jihadist organizations, which had taken power in Afghanistan through a blend of popular support and military action. And while it was clear that a significant portion of the Taliban's support came from Pakistan, the U.S. plan to support its ally, Pervez Musharraf, and his military regime in return for their support, established both a precedent and a penchant for viewing the conflict through the very western lens of a statist mindset and as a religious conflict with Jihadist Islam.

But has this been correct? Has our western perception of nation-state sovereignty and the very real religious nature of the wider "War on Terror" blinded us to a fundamental truth about the nature of the Taliban in the lesser regional struggle against terror in Central Asia? And has this led us to base our warfighting strategy on a false paradigm?

By mentally segregating the Taliban as an "Afghan" problem, by not addressing their roots of support inside the border with Pakistan, and by ignoring the obvious truth of their largely homogeneous ethnic composition, I believe that we have misdiagnosed not only the nature of their insurgency, but also the best way to deal with that insurgency. This approach has put us on the path of treating the symptom, but not the disease.

As a result of this imprecision, we have applied a series of remedies designed to combat religious extremism (but not ethnic separatism) with lackluster results. However, had we correctly identified the ethnic nature of this conflict early on, and applied remedies designed to counter and combat an ethnic secessionist insurgency, and in so doing faced that transnational nature of "Pashtunistan," we would very likely have been more effective in combating them.

Up to this point, we have viewed the Taliban as a Jihadist Muslim insurgency, composed largely of Pashtun tribesmen. I argue that what we should be doing is viewing and, more importantly, treating the Taliban as a Pashtun ethnic insurgency, composed largely of Jihadist Muslims.

## **In Counterinsurgency, the Why May be More Important than the How**

People are moved to fight for very deep-seated reasons; this is especially true of insurgencies. We

know from recent psychological studies of current and former terrorists and insurgents that most of them viewed themselves as soldiers fighting for a cause, very much the same as institutional soldiers of state-owned armies do, and with the same convictions and types of motivations. In the same way, the population which supports insurgents is also supporting that cause. Usually, both segments are trying to effect a change in their political or cultural conditions, a change from the current conditions which they can no longer tolerate peaceably.<sup>2</sup>

We also know that the goal of the insurgent is not necessarily to win a military victory. More importantly, the insurgent must gain and maintain the support of the population to win. If he can do this, he will eventually prevail. The same therefore goes for the counterinsurgent. In this type of warfare the real goal is to win the people, the insurgent cannot live without it, and the ruling government cannot remain in power if they do not have it.<sup>3</sup> It is that simple.

What this means to both sides is that they are in a popularity contest for the favor of the people. The insurgent has decided to take up arms because he thinks that is the best way for him to achieve his goals. Often, if he starts to see success in achieving those goals, or if those goals become impossible or unwinnable, he can be persuaded to disarm and work towards a peaceful solution. There are plenty of recent examples of this, from the decommissioning of the Irish Republican Army to the dissolution of the European leftist terrorist groups after the fall of communism.<sup>4</sup>

For the counterinsurgent, it also means that one can choose to combat an insurgency in one of two basic ways, one may impose and maintain the strictest of police-state regimes and allow no freedoms which would permit the insurgents to operate; or one might compromise with the insurgents and give in to their demands, at least enough to make it no longer worth the effort of armed struggle.<sup>5</sup> The first choice is difficult to achieve and requires massive resources. It is also anathema to liberal society and in the modern western world, it is simply not done. Which leaves us with the second option—compromise.

Keeping in mind that it is not necessarily the insurgent himself with whom we must find the compromise but the people who would support him, the option of compromise does not mean giving in to the demands of the insurgents themselves. More cor-

rectly, it means working with the population which is at play, and finding workable and acceptable ways to address the complaints which have driven them to insurgency. Successfully finding the happy medium between allaying their frustrations enough to forego supporting the insurgency, and yet still remain in power, means stealing a march on the insurgents, and cutting them off from their base of support. At this point, not only can they no longer win, but if they continue the struggle the population itself may eventually turn against them and take active measures to help you destroy them so that they can get some peace. This is the dynamic currently at play in Al-Anbar province and many other areas of Iraq, where AQ and other sectarian groups are finding that the population is turning against them and supporting the coalition forces.

So, to forge a political compromise with the affected population, one must know what is causing them to rebel or at least support a rebellion. As in any negotiation, a proper understanding of the fundamental problems is necessary to effectively address the key concerns, those most central to the core problem, and find the best solutions. Without this understanding, one runs the risk of giving too much. But more crucially, one may never address the real sources of discontent, and end up losing everything.

It is in this regard that the U.S., and the rest of the world, has failed in Afghanistan. We have not correctly determined the root causes of instability which have propelled several millions of people to support the Taliban. We might want to start over again with the fundamentals.

## **Scoping the Problem: Who Are the Taliban?**

As President Bush's cabinet and advisors well knew, the Taliban was the *de facto* government of Afghanistan. However, they missed the significance of the Taliban's almost wholly Pashtun membership, certainly at its leadership and inner core. Similarly, while the Pakistani roots of the Taliban were well known, the decision to treat it as an Afghan problem, and as an Islamic Jihadist group rather than a secessionist insurgency, focused our counterinsurgency efforts on the wrong things.

That the Taliban is a homogenous organization made up largely of Pashtuns, is not in itself a controversial statement—it is simply a fact.<sup>6</sup> But recognizing

how this fundamentally shifts not only the underlying goals and base of popular support for the movement seems to be more difficult. This is exacerbated by the fact that the Taliban members and even their leadership do not seem to comprehend the issue either.

Bard O'Neill has categorized nine different types of insurgencies based on the root causes behind them. This taxonomy is an important step in counterinsurgency warfare because it allows us to adapt our strategy to the specific type of insurgent threat we face. Two of these categories are the *Traditionalist* and the *Secessionist* models.

*Traditionalist* insurgencies focus on "primordial and sacred values, rooted in ancestral ties and religion", to impose a government system based on these ancient values, usually one characterized by passive participation by the masses and reliance upon an inherited or clerical elite for the major functions and decisions of government.<sup>7</sup> The Islamic Jihad groups—AQ, Jemaah Islamiyah, Abu Sayyaf, *et al.*, fall into this category, as do many of the Shia groups and the government of Iran (as well as the inherited monarchies of the Middle East). On the face of it, so does the Taliban.

One might easily classify the Taliban as a *traditionalist* insurgency at first glance. Everything it has said and published as either manifesto or edict would support such a claim; its goals and the government it established support it further. But looking at their actions once in power; the ethnic homogeneity of its ruling elite, and the history which gave rise to the movement, leads one to an overridingly strong case that the Taliban is actually a *secessionist* insurgency which has cloaked itself in the *traditionalist* mantel for very practical reasons.

*Secessionist* insurgencies seek to separate from their current state and establish new states based upon their political, ethnic, religious or whatever other feature they feel sets them apart from their current political peers. Some of the more notable insurgencies in history have been *secessionist*, to include our own American Revolution, the 1999 war in Kosovo, and the Liberation Tigers of Tamil Eelam in Sri Lanka.<sup>8</sup>

Given this definition, one might say that the Taliban could not possibly be *secessionist*. Everything it advocates speaks to a traditionalist mindset. It has actively advocated the unity of the Islamic *umma*; it does not wish to separate from Afghanistan, but to unite it

under its banner, and nowhere in its creed does it advocate power for one group over another, but rather passionately it struggles for the greater Jihad and the unity of all under the banner of Mohammed.<sup>9</sup>

All of this is true, but it ignores the greater and deeper sources of discontent that fuel the Pashtun people's support for this jihad; the transnational make up of the Taliban, and the dimension of their exclusion from the Pakistani elite. To understand this, one must view Central Asia from a tribal, ethnic and historical perspective, without the artificiality of political boundaries.

## Pashtuns and Pashtunwali: Defining a People

The Pashtuns define themselves not by language, but by adherence to an ancient code of conduct dating back to the pre-Islamic era.<sup>10</sup> To anyone having dealt with Albanians and familiar with their *Kanun* of Lek Dukagjin, this *Pashtunwali*, or "Way of the Pashtuns" is strikingly familiar. Like the Albanian *Kanun*, it might be described as the glue which binds this disparate people together as an ethnic group, and the beginnings of an insight into the ethnic dimension of our war in Afghanistan.



The Pashtun people are by some measures the world's largest tribal society, some 6 million native speakers, who have seldom in their long history had anything holding them together except for their language, a close relative of Farsi-Persian. They are mostly concentrated in southern Afghanistan and northwest Pakistan. See geographical location shaded in white on map above.

As a tribal people, Pashtuns are far more ready to subscribe their loyalty to their tribe over any ties to a

nation, much less a nation ruled by people from a different ethnic group or tribe.<sup>11</sup> A brief glance at the map shows that while most Pashtuns reside within the borders of Afghanistan, there is a fair-sized and reasonably compact Pashtun area largely within the boundaries of Pakistan's Northwest Frontier Province (NWFP).

Looking at the raw numbers gives another, starker view. Pashtun speakers comprise 35 percent of the Afghan population and are the largest, single ethnic grouping in that country. In Pakistan however, they are only 8 percent and are a clear minority.<sup>12</sup>

History provides an explanation. The origins of Afghanistan and the Pashtuns are inextricably tied, and equally indistinct. From the earliest times, the two have often been synonymous<sup>13</sup> and the history of one was to a great degree the history of the other. Afghanistan as we know it today was founded in 1747 by a Pashtun warlord named Ahmad Shah Abdali (he later changed his name, and that of his clan to Durrani), who united the disparate Pashtun clans under his banner to conquer all of present day Afghanistan, Pakistan, parts of Iran, and southward to Delhi.

This acme of Afghan/Pashtun power was short lived as it ran headlong into the birth of the British Empire in India.<sup>14</sup> For the next 190 years, the Afghans, and virtually everyone else in South Asia, began losing ground to first the British East India Company, then the British Empire proper. As the British expanded north and west, following the western rim of the Himalayan Mountains, they began having difficulties with the Muslim tribes of the "Northwest Frontier". People they called the "Pathans" and often subcategorized as Afridis, Yousafzai or a host of other names (most, by the way, Pashtun clan names) proved a constant source of instability.

In an effort to stabilize the frontier and prevent Russia from expanding and threatening India, Britain invaded Afghanistan three times. None of these expeditions ended well. By 1893, Britain gave up hope of controlling these tribal people. Lord Roberts himself called the region "ungovernable," and commissioned a survey of that land which they could control, and that which they could not.<sup>15</sup> The resultant "Durand Line" more or less describes the southern boundary of Afghanistan today.

Like many arbitrary surveys of the colonial age, Sykes-Picot comes to mind as another example. The

Durand Line was drawn by westerners, to the demands of western governments, with no regard to the facts or rights of the indigenous peoples. It cut across the heart of Pashtun tribal areas and while it allowed for a majority Pashtun ethnicity in Afghanistan, it created a minority Pashtun area in that part of India which would later become Pakistan. This gave rise to the problem of secession.

While Pashtuns in Afghanistan have long been a major political power if not a clear majority, their kin in Pakistan have been excluded from power by the largely Urdu and Punjabi speaking city dwellers in Karachi and Islamabad.<sup>16</sup> Although given a large degree of autonomy within the boundaries of the NWFP, some Pakistani Pashtuns have reacted to their minority status by demanding their own state—"Pashtunistan".

So there is an urge for independence and for a state of their own that is strong within the tribal culture of the Pashtuns. It drove them to found Afghanistan in 1747 and it is now driving some to seek a new country carved out of Pakistan. But how did this become translated into an Islamic Jihadist call for religious reform? There seems too large a gap between the impulse for secession, and the call for jihad.

But not really. Viewed from the context of tribal culture and a strong desire to be seen as a separate people, the turn to religion was an almost natural response. Tribal societies do not have strong leadership models, they exist in a "headless" state, and the Pashtuns are no exception to this.<sup>17</sup> As they turned inward and began looking for ways to unify the disparate and often hostile clans, the native religion and traditional practices were a natural choice.<sup>18</sup>

As a tool to unite the Pashtun people, religion worked well. But it also had perhaps the unintended (there is no evidence to the contrary) consequence of covering the real reason behind the discontent—the urge for separatism—and spilling over into the larger, non-Pashtun but religiously observant Muslim population in the region. This was further confused and muddled by historical events in Afghanistan which allowed the discontent of the Pakistani Pashtuns to spill over the border and helped unite the greater Pashtun tribe even further.

While the Pakistani Pashtuns struggled with their minority status following partition in 1947, their cousins in Afghanistan had grown accustomed to being the ruling elite. Since the founding of the kingdom in 1747, Pashtuns had filled virtually all Afghan

leadership positions. But in 1973, Shah Mohammed Zahir, a Pashtun, was overthrown and Afghanistan began its spiral downward to its current failed status with a series of increasingly leftist and socialist governments. On the way downward, the Pashtuns were replaced as the power elite by Tajiks and other northern tribes eager for their turn at the wheel. This climaxed with the 1979 Soviet invasion and the imposition of the Communist regime.

These events had the effect of pushing the Afghan Pashtuns in much the same way as their cousins across the border. Dispossessed of the power they once held, and dominated by people they viewed as godless heathens, the Afghan Pashtuns turned inward to find their identity and unity in religion. Whether this came as a result of, or in parallel with, the natural retreat to Pakistan and their cousins to the south is immaterial to this discussion. What is important is that the war with the Soviets united the Pashtuns as few things had since the British left, and gave a physical outlet to their secessionist urges.<sup>19</sup> It also greatly confused the issue of religion as the cause of the insurgency.

As the Muslim world reacted to the Soviet invasion, dollars and dinars began to flow, and people as well. It was an almost geographic certainty that the entry point for this assistance from the *umma* would be through Pakistan, and through Pashtun hands. The other peoples who comprised the remainder of the Afghan resistance had ethnic homelands that were either already under Soviet domination, or in Iran, which was not only Shia, but also in no economic shape to be of assistance to anyone throughout the 1980s. Pakistan was the only neighboring country through which people, money and materiel could pass, and the doorway was through the NWFP and the Pashtun tribal lands.

As the Muslim fighters and financiers became acquainted with these people who had so strongly embraced Islam as their rallying point, it was easy for them to confuse the issue of ethnic nationalism with Islamic Jihad. Just as we have done, the Arabs and others took the Pashtun piety at face value, and not for the unifying rally point it actually was. Not that this mattered at the time, they were, after all, solely in the fight to repel the godless invaders and sort out the details later.

As long as there was the common Soviet enemy, there was cooperation. But after the Soviets left,

cracks began to appear in the coalition of tribes and ethnic groups as they began to struggle for power. And it was in this maelstrom that the natural advantages of size and the unity that language, culture and the appeal to the common religion began to once again favor the Afghan Pashtuns. Given their secure bases in Pashtun areas across the border, and their large ethnic population within Afghanistan, the Taliban (as the Pashtun religious reformers now came to be known) with its agenda of government inspired and led by the Quran also had great appeal to the non-Pashtun Muslims who, like everyone else, took the religious face of the movement as the Truth and ignored the heavily Pashtun composition of the leadership. But as the Taliban swept into power, often hailed as liberators by the non-Pashtuns, the cracks began to appear in the heretofore wholly religious façade.

While I believe it is quite possible that even now, the Taliban leadership itself believes the movement to be religious and not at all about ethnic power or secession, the reality of its ethnic membership, monolingual administration and the very real tribal urges to keep important decisions and positions within the trusted group, all converged to insure that only Pashtuns had positions of power and control within the government, even in non-Pashtun areas.<sup>20</sup> By the end of the Taliban's reign, Afghanistan had once again separated along ethnic lines, with the Northern Alliance composed of Tajiks, Uzbeks and other northern ethnic groups opposing the Pashtun Taliban for political control.

Taliban activity is now largely restricted to the Pashtun areas of southern Afghanistan, and particularly the border region with Pakistan's NWFP, from which it can stage and train for missions and operations inside Afghanistan. The Taliban is a transnational Pashtun ethnic group which uses its bases in safe areas within Pakistan as sanctuary to continue their fight for a homeland encompassing Afghanistan and parts of Pakistan, and essentially to re-establish the Empire created by Ahmad Shah Durrani in 1747. And as for their paradoxical claims of Islamic Jihad? While I have no doubt that they themselves believe it, the Islam they wish to impose has more to do with their Pashtun traditions and serves more as a unifying force for the Pashtuns themselves than it does anything else.

There is no denying the religious component of the Taliban, it is indeed a jihadist organization to its

very core. It describes itself as such; its members proclaim it as such and ascribe to neither ethnocentric nor nationalist goals. It is easy to see why AQ and other jihadist organizations interact with it so closely, and why so many western observers have chosen to classify it as a *traditionalist* insurgency. But in reality, the Taliban movement began as an ethnic based response to the domination the Pashtun people were feeling from other ethnic groups in Pakistan, and the loss of control they were experiencing to other groups in Afghanistan. So, what do we do about it?

## **Treating the Cause Rather than the Symptom**

If we acknowledge the true reasons behind the Taliban's continued struggle and the Pashtun people's support for it, then we can better combat it. But this requires a change not only in how we deal with the Pashtun people in finding a path to compromise, but also in how we conduct our military operations. The most fundamental change to consider is our policy towards the Taliban sanctuaries within Pakistan. This is not a new suggestion, but in recognizing the transnational and ethnic nature of the Pashtun struggle, it is one with renewed urgency.

Throughout history, insurgent movements which operated from secure bases outside the area of combat operations had a far greater chance of success than those without such security. This only stands to reason: a secure base provides breathing room where they can ignore their logistical security to focus all of their combat power at the time and place of their choosing. This is a significant advantage over the defender who must defend everywhere at once.<sup>21</sup> It was this dynamic which Wellington used with the Spanish Guerrillas to defeat Napoleon in the Peninsular campaign, and that the Viet Cong used so effectively against us in Viet Nam. It was also the way that the Taliban and its allies fought the Soviets. So, to ignore the history of this is staggering.

While the political realities of Pakistan dictated a cautious course, it is after all a nuclear power and politically unstable, those realities have recently changed. And the fact is that one source of Pakistani instability is the question of Pashtunistan and the secessionist movement boiling over from the NWFP. Joining in common cause with the new government currently forming in Jalalabad to restore order to

the country by helping them to suppress the Taliban activities within their borders might be doable if we can demonstrate its utility. If we do nothing to deny the Taliban their safe areas, then we are likely to be in Afghanistan, like the Soviets, for a long time with very little to show for it.

More basic than this, and more volatile, is the question of Pashtunistan itself. If we are going to treat the cause of the disease, should we address the Pashtun peoples' evident desire for a homeland of their own?

As a point of discussion, a start point for negotiations with the Pashtuns themselves, we should consider the prospect of creating a Pashtunistan which reflects the tribal boundaries. This would be a new state, carved from parts of both Afghanistan and Pakistan. Parts, I might add, over which neither we nor the Pakistani's exert much control. Like the British in 1893, we might draw a line separating that which we can control, from that which we cannot. Unlike the British, we would draw it with regard to tribal and cultural lines, and not with a more tactical or geo-political motive for the preservation of our own empire. This new area would be composed largely of ethnic Pashtuns, similar to what we have created in Kurdistan or Bosnia, and it would therefore very likely have the consent of the population on the ground. This would not be easy or acceptable to all parties, but with the current advantages of precedence, common sense, political change in Pakistan and military strength on the ground, we probably have the best conditions we will ever have in our lifetimes of making it work.

The alternative to this is allowing Afghanistan to pursue the failed course it has since 1747 as a collection of squabbling ethnic groups with nothing in common but hatred, dominated by the Pashtuns who seem dangerously infatuated with their pre-modern views of Islam. While we cannot impose the former easily, we cannot allow the latter to continue.



## Endnotes

1. Bob Woodward, *Bush at War* (New York: Simon & Schuster, 2002).
2. John Horgan, "Disengaging from Terrorism," *Janes Intelligence Review*, December 2006. Sent to author by email from Dr. Horgan on 5 November, 2007.
3. David Galula, *Pacification in Algeria, 1956-1958* (Santa Monica: RAND Corporation, 2006 originally published 1963).
4. Horgan.
5. Bard E. O'Neill, *From Revolution to Apocalypse: Insurgency and Terrorism*, 2nd edition (Washington DC: Potomac Books, 2005).
6. Ali A. Jalali and Lester W. Grau, *Whither the Taliban?* (Fort Leavenworth: U.S. Army, Foreign Military Studies Office, 1999) Downloaded from the internet on 19 February, 2008 at <http://call.army.mil/call/fmso/fmso.htm>.
7. O'Neill.
8. O'Neill.
9. Bruce Hoffman, *Inside Terrorism* (revised and expanded edition) (New York: Columbia University Press, 2006).
10. Jalali and Grau.
11. David Ronfeldt, "Al Qaeda and its Affiliates: A Global Tribe Waging Segmental Warfare," *First Monday*, Volume 10, Number 3 (March 2005), accessed 13 February 2008 at [http://firstmonday.org/issues/issue10\\_3/ronfeldt/index.html](http://firstmonday.org/issues/issue10_3/ronfeldt/index.html).
12. CIA World Factbook.
13. V. Minorsky "The Turkish Dialect of the Khalaj", *Bulletin of the School of Oriental Studies*, University of London, Volume 10, Number 2, 1940 accessed from JSTOR, 19 February 2008 at <http://www.jstor.org.library.norwich.edu/view/13561898/ap020036/02a00120/0/0?currentResult=13561898%2bap020036%2b02a00120%2b0%2cEFFF3F&searchUrl=http%3A%2F%2Fwww.jstor.org%2Fsearch%2FBasicResults%3Fhp%3D25%26si%3D1%26gw%3Djtx%26jtxsi%3D1%26jcsi%3D1%26artsi%3D1%26Query%3DKhalaj%26wc%3Don>.
14. Battle of Plassey, 1757.
15. Peter Hopkirk, *The Great Game: The Struggle for Empire in Central Asia*, (London: Kodansha Globe, 1994).
16. Jalali and Grau.
17. Ronfeldt.
18. Jalali and Grau.
19. Ibid.
20. Ibid.
21. Thomas M. Huber, "Napoleon in Spain and Naples: Fortified Compound Warfare," U.S. Army Advanced Operations and Warfighting Course paper #H205, 2002. "Backlash to Revolution: The Decline of Napoleon" (Leavenworth: U.S. Army Command and General Staff College) accessed 15 October, 2007 at [https://courses.leavenworth.army.mil/webapps/portal/frameset.jsp?tab=courses&url=/bin/common/course.pl?course\\_id=\\_1455\\_1](https://courses.leavenworth.army.mil/webapps/portal/frameset.jsp?tab=courses&url=/bin/common/course.pl?course_id=_1455_1).

*Mike Holmes is an employee of Oberon Associates, currently assigned as an Operations Officer at the TRADOC Program Office for Biometrics and Forensics at the U.S. Army Intelligence Center, Fort Huachuca, Arizona. He is a lieutenant colonel in the Army National Guard serving as the S2 for the 49<sup>th</sup> Theater Information Operations Group, TXARNG. He has served in a variety of assignments, to include brigade and battalion S2, and was an Intelligence liaison and U.S. Arresting Officer for the British led MND-SE in Basrah in 2005. He holds an MA in Diplomacy with a concentration in International Terrorism from Norwich University, and is a graduate of U.S. Army Command and General Staff College. He may be reached at mike.holmes1@us.army.mil.*



# Transforming CI to Counter Low-Intensity Collection of High Technology:

## Forcing the Enemy Back to the Outside Game

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

***"Borders frequented by trade seldom need soldiers."***

— General Kyle Barton Yount

### Introduction

When General Yount, the founder of the Thunderbird School of Global Management, penned that quote, the Counterintelligence (CI) community undoubtedly cringed. Today, the issues are the same; only the technologies are different. As does the U.S. military, so too must U.S. CI incorporate these technologies into its weapons inventory, revise its doctrine, and implement a strategy for the new age. That strategy must focus scarce resources, empowering agents, and be flexible enough to respond to a dynamic environment.

In the wake of World War II, the general and many of his contemporaries considered the cause of war to be the fact that many countries, not only the Axis powers, had actively restricted trade with one another. Strategic thinkers of the time strongly believed the promulgation of open markets and unrestricted trade would remove the single most pre-

---

**by Mark A. Thomas, PhD**

---

dominant cause of war. Trade was the means to building a peaceful post-war era.

Many contend it was these ideals and the associated international organizations which brought the U.S. prosperity, led to the European *wirtschaftswunder*, contributed to post-war economic reconstruction, and arguably even ushered in the end of the Cold War. After all, it was not the fear of NATO military forces but awareness among citizens in the Soviet sphere of influence of the higher quality of consumer goods in the West which discredited the Communist regime's hold on power.

These are also the ideals which chill the blood of the CI agents, both then and now, who look judiciously upon benefits accruing to U.S. national security from scientists exchanging ideas and businessmen trading goods with their foreign counterparts. It is around these ideals where the U.S. CI and law enforcement agencies square off with their colleagues in the Departments of State, Commerce, and Treasury in

fervent battles over the merits of foreign acquisitions of U.S. firms, international scholarly exchange, and the proliferation of multinational firms as net gains for U.S. national security.

## A Historical Perspective

World War II was a very complex period for those protecting the Manhattan Project. Our CI forefathers had to wrestle with such daunting issues as at what stage of research it should become directly involved, how to manage the risk of U.S. and foreign scientists exchanging technical information, and a fungible world of foreign relations where countries' reliability as allies was unclear.

If history holds any lessons for today, it was foreign nationals who held the key to weaponizing Albert Einstein's basic research. Not surprisingly, CI strongly opposed their involvement in the Manhattan Project. Only Einstein's tireless and direct intervention to President Roosevelt enabled scientists, who had defected from Nazi-occupied Europe, to assist in the development of the first atomic bomb. Yet, it was American and British born citizens, who betrayed that technology to the Soviet Union.

For CI practitioners, the world has become even more complex since World War II and the immediate post-war years General Yount turned the sword of an Army airfield into the plowshare of a highly respected international business school. First, the means of communication are very different. Telephones and telegrams were the most rapid means of communication. Industry and government primarily used paper and postal service as the primary means of communicating large amounts of complex and sensitive data. And as the angst of World War II subsided, technology raced ahead to a time when the single greatest impediment to securing classified information was a photocopier. With photocopiers, a spy could duplicate comparatively large amounts of classified documents, put it back in the safe and nobody would even know it was compromised. Today, a perpetrator with single thumb-drive can remove most, if not all, of the contents of the Library of Congress, and transmit it to an adversary within seconds. Worse still, an operative can do it with comparatively low risk of a coworker witnessing the event.

## Three Challenges

As described in Thomas Friedman's *The World is Flat*, the proliferation of Internet, the success of Yount's vision, cheaper means for worldwide travel,

and the end of the Cold War have transformed not only how, but who can become involved in international trade. During the Industrial Age, individuals needed significant resources to exchange goods and services beyond the borders of their hometown, let alone beyond the borders of the country. Comparatively few people could truly call themselves "citizens of the world." Today, the Internet and modern aviation enable all people, except where technology lags or governments otherwise restrict it, to exchange ideas, trade and collaborate with incredible ease. Sadly, CI has been slow to understand the imperatives of the Information Age and slower still to adapt its methodologies. With the exception of isolated pockets, CI stands firm like a New Orleans levee, hoping to stem the outflow of U.S. critical technologies.

CI wrestles with three mutually compounding challenges in crafting a strategy to protect critical U.S. technologies. These challenges are largely the same as those facing the CI community as well as the rest of U.S. government as a whole. First and foremost CI agents, especially those involved with technology protection, must understand the world is even less insular today than it was in 1945 or when Thomas Jefferson wrote in the early nineteenth century, "Merchants know no country." Business and academia know no boundaries. And, that globalization of trade and exchange of knowledge holds both intrinsic benefits as well as inherent risks.

CI must first understand, and if not accept, the benefits of globalization to be credible to those in the industrial base and acquisition world, which increasingly rely on foreign sources. A xenophobic approach to globalization on the part of CI is both counterproductive and unrealistic. Only by understanding the benefits of global trade can a CI agent earn enough credibility with his customers to recommend countermeasures mitigating the risk, which only CI has the mission and expertise to communicate.

Second, the U.S. CI community, and most likely the majority of our NATO allies, must adapt doctrine and methods developed during the Industrial Age to the Information Age. The acquisition community and its partners in academia and industry are already riding the technology wave. The "network of networks," the heart of military modernization, hinges on integrating the Information Age technologies to give U.S. forces the combat advantage. Yet, CI strains to adopt cyber into its doctrine, either

in how cyber supports CI or how CI manages the threats associated with cyber technologies.

To put it in perspective, a gigabyte of data approximately equals the contents of five standard five-drawer safes. The average standard stand alone computer has a 40 gigabyte hard-drive, which means a single user has the equivalent of 200 five-drawer safes at his desk. A network of computers increases a single user's access in proportion to the size of the network. Calculate the exponential impact of a hacker or an insider who accesses a network which is linked to other trusted users' networks. What price would a member of the U.S. intelligence community have paid for the equivalent of 200 Soviet government safes during the Cold War? Even if they contained only unclassified documents an analyst, a true puzzle-master, could easily compile a high-value product to disclose some aspect of the Soviet government's strategic intent, strengths, and weaknesses.

The question before CI is not whether the Information Age brings new challenges. Of that there is little doubt. The question is whether CI wants to confront the challenges or to relegate the matter to an "operational security concern," essentially confining CI to the narrow lane of countering traditional Human Intelligence collectors, who themselves increasingly rely on cyber tradecraft to limit their sources' and their own risk of compromise. While computer network defenders and security professionals bear a large measure of responsibility, CI too must transition its approach, doctrine, and methods to the new era. And, like all in CI, technology protection agents must both embrace the technology as an ally as well as grapple with it as an adversary. Unless, we accept the challenge, to paraphrase Sean Connery in *The Untouchables*, we will bring a knife to a gunfight. Gratefully, this topic is beyond the scope of this paper and hopefully others, who have more expertise in cyber technologies, will address this in more detail.

Finally, as our military has had to do in Vietnam, Somalia, and other trouble-spots around the globe, CI agents confront an unconventional force. While conventional intelligence services like conventional militaries will continue to be a perpetual threat, CI agents must adapt to wage their battle against both enemies, conventional hostile intelligence services and sub-state actors who are prepared to use asymmetric intelligence collection methods to target sensitive U.S. technologies.

## **The Inside Game—Asymmetric Collection**

Asymmetric collection are those methods of intelligence gathering which intentionally avoid direct assaults on the conventional forces and use the jungle created by liberal democracies' embrace of free markets, open societies and Information Age technology as camouflage to stage their attacks. As U.S. and allied forces can deter and, when necessary, repel an adversary's conventional forces, CI services have proven to be adept at taking on traditional intelligence collectors. However, as U.S. CI services identify and neutralize traditional foreign agents, foreign intelligence services and their governments undoubtedly take the lessons learned to adjust and refine increasingly ineffective collection methods.

Not surprisingly, many of these governments have adapted their collection methods to exploit the seams and gaps and capitalize on interagency turf battles to the detriment of the U.S. military modernization efforts. And, as an offense adopts new plays to exploit weaknesses in the adversary's defense, the defense must respond in kind. Asymmetric collectors, who are not directly associated with foreign intelligence services and gather technical data only under broad government mandate, exploit the seam between customs enforcement agencies and CI. The collection is low risk, hidden in the noise of free trade and academic freedom, which are the keystones of economic prosperity and scientific progress.

In the end, the U.S. technology protection community must develop a strategy which is flexible enough to allow agents to react without bureaucratic or organizational restraints, risk-tolerant to respond to adversaries' new methods, and sufficiently dynamic to adopt new technologies. More importantly, the strategy must be realistic enough so as to empower our agents and credible in order to deter our enemies and to maintain the trust of those whom CI supports.

Since the late 1940s the U.S. and then after the mid-1960s, the other nuclear powers have struggled to slow and regulate the proliferation of nuclear technology (currently the single most devastating technology known to Man). Yet, despite broad international consensus and an international treaty to that effect, the threat of the spread of nuclear technologies countries, who seek to weaponize it and who are not yet signatories to or do not abide by the terms of the Nuclear Non-proliferation Treaty, continues to pose significant challenges. If the U.S. and its partners struggle to limit

such a technology where there is universal agreement on its destructiveness, it is unlikely CI and the rest of its partners in the technology protection arena can stop the migration of advanced technologies, often dual use technologies, such as communications and military surveillance technologies, to countries with interests inimical to the U.S. The best the U.S. government can expect and the CI community can expect from itself is to slow the loss long enough for U.S. scientists to maintain the technological advantage in areas deemed critical to national security. Although the ultimate goal of any CI strategy is to halt the loss of sensitive information, U.S. adversaries' tenacity and ingenuity will only allow CI agents, at best, to reduce the risk of loss while minimizing the damage resulting from hostile intelligence collection. In the area of protecting critical technologies, CI forces only act to slow the adversary's pursuit of technology and to prevent his unpredicted sudden leap ahead in technological advantage.

Drawing an analogy from basketball, the heart of any U.S. technology protection strategy is to take away the enemy's inside game, his high percentage 2-point shots, and force him to the outside where he must gamble on the more difficult and riskier task of recruiting an insider, namely those low-percentage shots, where the defense has greater time to react and the offense is at greater risk. Currently, the inside game is asymmetric collection.

Forcing the adversary to rely on his outside game, specifically conventional espionage, requires him to expend far greater resources and manpower than he does in asymmetric collection. In defending U.S. critical technologies, CI's role, in concert with security, anti-tamper, and foreign disclosure experts, is to force the adversary to increase his overall research, development and procurement costs. Whether the coverage is a man-on-man or a zone defense depends on the adversary's offense. In the end, CI must assist in preventing breakaway shots, lay-ups, and slam dunks, which current government policies and practices make available, and our adversaries exploit.

## **CI Technology Protection Strategy**

To force the adversary to the outside, a CI technology protection strategy must contain three elements. First, the strategy and its accompanying doctrine must provide a coherent focus. The natural starting point is to determine which technologies are critical to the U.S.<sup>1</sup> CI has spent much time and energy

identifying and attempting to protect critical program information, critical technologies or critical national assets (whichever nomenclature the community wishes to attach to those technologies). If these critical elements are compromised our military and/or economic advantage will be reduced, or similarly benefit hostile powers. Identifying critical technologies is only the first step, and possibly an errant step if the technology is so narrowly defined as to restrict protections and CI countermeasures toward a single formula or a component which a highly advanced country can develop indigenously if it understands or acquires the peripheral or enabling technologies.

The second element is determining the adversaries' collection objectives. Typically, CI relies on reports of illicit attempts to acquire the critical technology to ascertain foreign collection requirements. Such an approach captures only one part of the picture and limits it to reactive countermeasures. The traditional approach also may not capture the entire range of collection requirements approach and limits CI analysts' visibility to collection efforts occurring in the U.S. or against U.S. targets overseas. It does not capture collection efforts used by adversaries to acquire technologies from non-U.S. suppliers and trading partners overseas. Consequently, CI technology protection efforts unnecessarily hamstring U.S. firms by limiting their foreign sales of technologies which other foreign firms are already selling to countries with interests inimical to the U.S. Worse yet, CI squanders resources against a technology not in need of protection.

An alternative but complementary approach is to determine the adversary's technology gaps for those capabilities where the U.S. hopes to maintain a technological advantage. With regards to military acquisition, using a hostile country's military doctrine as that country's desired end-state and knowing the respective country's current state of the art, analysts can determine that technological gap. The adversary must fill that gap either through external procurement or intelligence collection. The technological gap is the country's military modernization priority intelligence requirement (PIR).

Scholars have long debated the veracity of an adversary's doctrine. During the Cold War, many viewed Soviet doctrine as largely propaganda. While they all contain elements of propaganda, doctrinal statements largely reflect the true intent of the for-

sign military. While intelligence analysts can always find evidence of internal debate, doctrine is a reliable means, even under authoritarian regimes, for governments to communicate strategic priorities to both the general public as well as to the specific community of interest. Doctrine enables leaders to justify resource expenditures, rally public support for policies and quash potential seeds of dissent. And, while omitting specifics, doctrine provides a clear baseline for analysts to determine general direction in a given period as well as to judge the government's effectiveness or change of priorities over time.

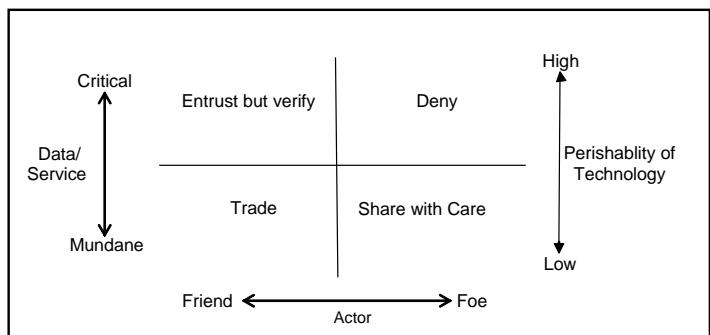
## Focusing CI Support

In addition to identifying the adversary's PIRs, analysts can also identify U.S. as well as foreign sources of the technologies necessary for the adversary to fill the gap. The next logical step in the analysis then would be to determine which foreign suppliers develop comparable or better technologies which the U.S. considers critical. Those technologies in which the U.S. does not have the advantage but considered critical by definition are no longer critical unless U.S. policy-makers can restrict the foreign sales of those technologies from reaching the factories and labs of U.S. adversaries. Where policy can restrict legal exports or deter third-country transfer, U.S. CI can then focus its support on those critical technologies which the adversary aims to acquire.

Many have said that by protecting all technologies CI protects no technology. The same holds true for attempting to focus scarce resources by implying all countries are an equal threat to the U.S. technological advantage. Such an assumption ignores the reality and the inherent benefit of international trade to U.S. military modernization. And, it also precludes opportunities for cooperation with allied CI services which share similar concerns.

The second requirement is then to determine the countries against which CI technology protection agents need to focus their energies. The end of the Cold War only complicated efforts and strained resources. While CI forces will always retain a staunch "zero-tolerance" stance against all countries and foreign entities attempting to illegally collect classified or sensitive U.S. information, focusing CI resources requires a prioritization of targets.

Figure 1 provides a conceptual framework both for CI to focus its pro-active technology protection



**Figure 1. Who is the Adversary?**

programs as well as potential basis for others to develop trade policies. Given a critical technology where the U.S. truly has the lead, CI should focus its programs on those upper-right quadrant countries, which have intelligence collection requirements for a given technology or its associated enabling technologies. The countries in the upper-left and lower-right quadrant become matters for policy makers in the U.S. Departments of State and Commerce to ensure compliance to bilateral agreements and multilateral counter-proliferation agreements, such as the Wassenaar Arrangement.

It is also possible to add yet another dimension to the framework, namely the technological sophistication of a country's industrial base. A country with a less developed industrial base has less capability to leverage highly technical data to upgrade its military or economic capabilities. However, a highly developed country with access to the same data has a greater likelihood of integrating advanced technologies into their industrial base and ultimately into their weapons modernization programs. Even among countries of generally similar levels, the impact of access to technical data will also vary according to the type of technology.

Not only is it important to categorize countries into threat countries, incorporating the industrial base axis into the analytical process is critical to refining the concept of compromise and ultimately to understanding the impact of an adversary's access to sensitive technical data. Unlike data related to intentions, plans, and operations, countries face distinct challenges in varying degrees in actualizing the potential benefit accruing from access to technical data. In the area of technology protection, access to technical data may not equate to compromise if the collector can not use it. Where attribution of an event to a collector and the data accessed are largely clear, factoring in the level of industrial

development also significantly improves the quality of damage assessments and prevents the tendency to dismiss a technology as compromised because a foreign entity merely had access to it.

A follow-on action to centering CI focus is to group countries according to the threat they pose to national security based on their ability and intent to illicitly acquire technologies; and their ability/willingness to limit third-country transfer. CI and their kindred law enforcement agencies would focus their efforts against those countries which steal critical military technologies and whom the U.S. or its allies will face on a battlefield directly or via a surrogate. The next set of target countries consists of those which target critical technologies and then transfer them to other countries or international terrorist groups. The remaining countries are all those targeting critical technologies.

## Leveraging CI Partners

Prioritizing the technologies and the countries of CI focus only identifies the opponent and defines the rules of the particular basketball game. If the strategy is to force the opponent to rely on this outside game, CI needs some more players with other skills on its team. The role of CI is only to fill and/or exploit the seams in the defense which its partners cannot otherwise cover. The second part of any technology protection strategy then is for it to leverage all partners and their strengths. Recruiting players from the traditional ranks of security and law enforcement communities no longer suffices. It must adjust its approach to protection to incorporate the scientist and the businessman as part of the solution, not simply part of the problem. In most instances, scientists and businessmen do not understand the CI mission and only view it as the individuals who investigate them or their friends with the intent of revoking their clearances or putting them in prison. CI must educate those it supports and more importantly ensure they understand the value CI brings to their work. Once aware, the scientists and business persons become tripwires widening the reach of CI to hostile intrusions. Closer cooperation with its customers is the technology protection version of “every soldier a sensor.”

To gain value-added through its new associates and more importantly to improve its credibility, CI must provide specific and actionable threat information upon which scientists and researchers can assist in developing countermeasures to protect themselves

and their work. More importantly, threat analysis (highlighting countries, their specific type of collection, and in certain cases, the specific profile of collectors against a specific technology) focuses researchers and business professionals reports of suspicious activity. The end result is more actionable reports upon which to base investigations and operations.

Likewise, CI must not stop its interaction with the report of a suspicious incident. It must complete the intelligence cycle with the customer by providing those appropriate and at the appropriate level periodic updates on investigation and operations impacting them or their technologies. CI must also work with program experts and intelligence analysts to conduct damage assessments when there is a compromise of technical data. Doing so allows its customers to adjust internal security policies, to change program direction as necessary, or regrettably, to invest in new technologies as foreign targeting compromises technologies which had been critical to that firm or government agency.

Additionally, CI must define its place in the Information Age, where the ability of the adversary to datamine the networks and the quantity of data processed have both increased exponentially and all but unabated. In such an era an adversary can datamine the Internet to compile sufficient quantities of unclassified information to produce documents which many experts would consider as classified. To remain relevant, CI needs to enlist the assistance of those who understand computer network defenses and information security to develop and provide advice on policy and procedures designed to minimize the risk of compromise of controlled unclassified information. Information assurance countermeasures and other technical fixes, such as restricting access to websites, etc., are only partial fixes. While Security must work to limit the content and type of data processed on computer networks, CI must define its role to counter those who are exploiting the computer networks. A first step would be analyze the type of data being targeted, correlate with the adversary's collection requirements, and then to develop operations to mitigate the threat.

Finally, CI must do more than simply remove stovepipes to information-sharing within the U.S. government and among other relevant members of the intelligence/CI and law enforcement communities. It must identify opportunities for cooperation

with foreign counterparts to target third-country exploitation of U.S. and U.S./host nation joint critical technologies. U.S. military service CI organizations have developed strong and enduring relationships with many countries' CI and security elements. Such cooperation has proven remarkably mutually beneficial to all those involved in countering those whose interests are detrimental to U.S., allies and coalition partners' strategic interests.

The third element in a viable CI strategy is to empower agents to work smarter not harder. Technology protection is not rocket science, but CI agents in the arena must deal with rocket scientists. Leaders must encourage their agents to learn and understand the basics of the key technologies they support. Several universities offer courses designed to assist business professionals in understanding complex scientific concepts. Likewise, many firms provide their non-technical departments training on the fundamentals of key technologies so sales associates better understand the goods they must sell. CI agents need to avail themselves of these courses.

Additionally, CI agents must develop and leverage "smart-pages," where they can both share lessons learned as well as develop a better understanding of the technologies they support. Aside from threat reporting, smart pages can include export-control guidance, program protection plans, technology control plans, and any other document which the agent uses to clarify whether an incident meets the threshold of a suspicious incident, assists him understanding other agencies' requirements or, improving his/her overall appreciation of the field. Such smart pages should also immerse the agent in the language of the technology so he/she can speak with some degree of familiarity with professionals in the field he/she is supporting. A "Wikipedia" type function, which other intelligence disciplines have adopted, would prove invaluable.

Working smarter, not harder entails agencies leveraging each others' strengths, be they matters of technical expertise or purely matters of original jurisdiction. Aside from adjusting the Cold War era guideline of information-sharing away from only those who can prove a definite "need to know" to all those who share a common mission, CI has thrown itself headlong into working in task forces. So much so, task force fever threatens to strain the very manpower they were aimed to save. Not to minimize the effects of the successful task forces in place, how-

ever, not all of them need to locate all their members in one physical location. Another model of a task force is a virtual one, where the supporting headquarters agree that a single office will be the central reporting point to correlate intelligence and to coordinate investigative and operational activities across the country and/or across the world. Aside from the traditional brick and mortar task force and the virtual one, headquarters must empower their agents to create other models of information-sharing.

## Conclusion

The Information Age offers CI a brave new world. The opportunities are as numerous as, and for creative agents outnumber, the vulnerabilities. The single greatest challenge is not the adversary; it is leveraging the creativity of the individual agents and preventing bureaucracy from stifling their inventiveness in responding to an agile offensive. A strategy of taking away the inside game relies on leveraging individual initiative and making our CI world as flat as the world in which it operates. To channel those scarce resources, though, the strategy must focus on the most strategic threats to specific technologies, enlist the assistance of new partners, and provide agents the means to use their time more efficiently.

Finally, CI must remain customer-focused. It is the mission of CI to provide the intelligence and appropriate countermeasures necessary for program managers to manage risk. By uniting with security specialists, law enforcement agents, and network defenders, CI can reduce the opponent's persistent ability to hit high-percentage shots. Likewise, as CI successes and failures feed the intelligence process, senior leaders have the bases to adjust and to develop new policies to improve the defenses more, further forcing the adversary to attempt more low-percentage shots.

## Endnote

1. CI does not have the mission to determine what a critical technology is. Only the scientists and developers understand the technology well enough to determine if it is critical. CI is merely a protector of what others identify as critical. Identifying what is critical needs an integrated product team (IPT) of specialists from the intelligence, CI and scientific communities. In certain instances, CI may find itself as a facilitator of these IPT.

*Mark Thomas is currently assigned to Office of the Assistant Secretary of the Army, Acquisition, Logistics, and Technology and is a senior advisor on the Army Defense Industrial Base Cyber Security Task Force. He earned an MBA from the American Graduate School for International Management and a PhD/MA in Political Science from the University of Notre Dame. He served with 501<sup>st</sup> MI Brigade, 902d MI Group, Allied Command-Counterintelligence and the Office of the Army DCS, G2.*

# Amateurs Talk Tactics, Professionals Talk LOGISTICS

*This article first appeared in the May June 2008 of Communiqué and is reprinted with permission.*

by DIA Staff Writer



Photos by Paul S. Cianciolo, CIV

Luis Ayala, DAL-1 chief; Nick Vamvakias, DAL staff officer and Logistics Engineering Command Center project manager; and Frank Vito, DAL-1C facility manager, examine the DIAC's emergency backup generators.

Hundreds of people work every day behind the scenes to keep the Defense Intelligence Agency (DIA) operational. Official and diplomatic passports are issued. Cargo is moved throughout the world. Weapons training is conducted. New office space is planned. Renovation projects are managed. And power and utilities are constantly monitored to ensure employees can work without worry.

Headed by John Davis, the DIA's Office for Engineering and Logistics Services (DAL), in the Directorate for Mission Services (DA), provides timely, professional and quality engineering and logistics services throughout the world. The office manages two divisions and a support cell of more than 100 agency employees and 350 contractors.

"The breadth and depth of the people that work in DAL is incredible," explained Colonel Robert Varela, DAL deputy chief. "We have architects, engineers, nurses and travel agents—just to name a few." To accomplish such diverse missions, DAL is split into three main functions: infrastructure, logistics and support to the Office of the Director of National Intelligence (ODNI).

## Maintaining the Infrastructure

The Facilities Engineering Division (DAL-1) takes a proactive, preventative maintenance approach to ensure that all DIA employees have a safe place to work wherever they are in the world.

The 25 year old DIAC building was originally designed for 2,000 employees, but now it's host to more than 5,000. With very significant space shortfalls throughout the agency, DAL-1 diligently provides expert space planning and management. The division is also responsible for the design and construction of the new \$58.5 million DIA facility being built in Charlottesville, Virginia. It is scheduled to open during the summer of 2010.

DAL-1 manages an average of 125 projects at any given time. They can range from construction projects, repair work, safety compliance, interior design, utility outages, or roads and grounds maintenance. An important task currently underway is the design of a new light-rail station in partnership with Bolling Air Force Base. The station will allow employees mass transportation access to the DIAC from the Anacostia Metro Station. It is planned for the corner of Brookley Avenue and DIA Access Road and should be completed in 2010.

Being proactive also means planning for emergencies. DAL-1 maintains the fire and emergency management control systems, ensures for uninterruptible power supplies, provides a medical clinic at the DIAC and protects the work force from a chemical or biological attack. "If the city lost power for two weeks, we would be fine," said Luis Ayala, DAL-1 chief. "We have also installed filters in the HVAC systems to protect against chemical and biological agents. The work force will be safe if they stay inside the building."

## Supplying the Tools

Issuing passports, providing official vehicles, accounting for property, preparing personnel for deployment and moving cargo around the world is not

a simple task — especially in the middle of two conflicts. This is what the Logistics Division (DAL-2) does every day.

DAL-2 maintains a fleet of more than 30 passenger vehicles, including some deployed to overseas locations. It also manages the shuttle bus services to the DIAC parking lots, DIA offices and Anacostia Metro. And its travel office provides the work force with temporary duty arrangements, travel ticketing, and official and diplomatic passport services.

"Our missions grew considerably after the start of the war," said Patrick Protacio, acting DAL-2 chief. "We used to be mainly focused on the National Capital Region, but now we are worldwide." The DIA Logistics Operations Center (DLOC), located in Landover, Md., is the central hub for all equipment and supplies used and stored by the agency. Classified and unclassified cargo moves somewhere in the world every week. Over recent months, DAL-2 successfully streamlined processes at the DLOC to track and deliver materials moving through the warehouse to customers. "Our sister agencies come to us because of our expertise in booking flights of cargo," stated Varela. "We're the envy of the [intelligence community]."

The DLOC is also home to the agency's deployment center. All personnel are processed through the center prior to and after returning from overseas. With \$7.5 million in assets, the central issuing facility can outfit anyone with the uniforms and equipment they need to deploy—from military, to civilian, to contractor personnel. They have everything a military deployment center has plus much more. The deployment



Photos by Paul S. Cianciolo, CP

Head nurse Michelle Humphrey prepares to draw blood from Virginia Cochran, DAL staff officer, during a medical exam at the deployment center.



Photos by Paul S. Cianciolo, CP

Cargo movements are tracked at the deployment center.



Photos by Paul S. Cianciolo, CP

Virginia Cochran, DAL staff officer, is tested for the proper fit of her gas mask at the deployment center.



Photos by Paul S. Cianciolo, CP

Daria Nelson, DAL-2B travel office chief, inspects passports awaiting issue to employees.

center also conducts complete medical exams, and the armory maintains weapons and qualifies personnel through simulated and live-fire training.

Two lesser-known functions of DAL-2 include property accountability and contingency planning coordination. During the last year, DAL-2 improved procedures and records in preparation for the agency's audit. Logistics planners also coordinate on support agreements with other organizations around the world—such as the one DIA has with Bolling AFB, which provides services ranging from security and fire protection, utilities, and morale, welfare and recreation services.

### **Supporting the DNI**

In 2005, DIA offered space in the newly constructed DIAC Expansion to the new cabinet-level ODNI. Since then DAL's ODNI Support Cell, headed by Edward Cartwright, coordinates DIA services to the more than 700 ODNI personnel occupying the top two floors of the DIAC Expansion building. DAL often coordinates with security escorts, caterers and a host of other services when presidential advisers and foreign diplomats visit the DNI at the DIAC. The DNI Support Cell is also lending a helping hand for the ODNI's relocation effort to a new facility in the Tysons Corner area, which is planned for June 2008.

Whether it's paying the DIAC's monthly utility bill or preparing an employee to deploy to Iraq, DAL is providing the work force with a first-class environment for intelligence support to the warfighter.



---

**"The breadth and depth of the people that work in DAL is incredible."**

---



Photos by Paul S. Ciandito

Luis Ayala, DAL-1 chief; John Davis, DAL chief; COL Robert Varela, DAL deputy chief; Patrick Protacio, acting DAL-2 chief; and Edward Cartwright, DAL DNI Support Cell chief, review plans for Rivanna Station in Charlottesville, Va.

### **MI LEGACY**

---



AN/PRD-1 direction finding set determined what direction enemy radio signals were coming from.

# *Intelligence Philatelic Vignettes*

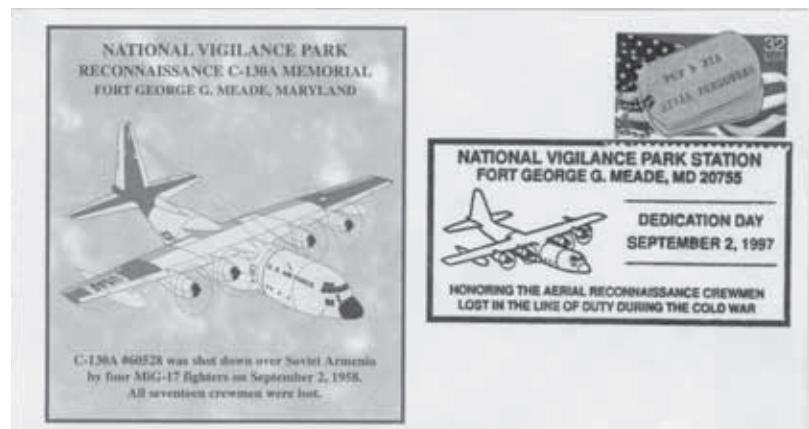
## National Vigilance Park, Fort Meade, Maryland

Material provided by Mark Sommer

Dedicated in September 1997, the National Vigilance Park was created by the U.S. Air Force 694<sup>th</sup> Intelligence Group and the National Security Agency, with the support of many other organizations, to honor the sacrifices made by aerial reconnaissance crewmen during the Cold War. Two of the aircraft, the C-130 and the RU-8D "Winebottle" figured prominently in Imagery and Signals Intelligence missions performed by these "silent warriors."



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





# CONTACT AND ARTICLE



## Submission Information

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

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

Articles about current operations and exercises; tactics, techniques, and procedures; and equipment and training are always welcome as are lessons learned; historical perspectives; problems and solutions; and short “quick tips” on better employment of equipment and personnel. Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the IC at large. Propose changes, describe a new theory, or dispute an existing one. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

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

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

### **What we need from you:**

- ◆ **A release signed by your local security officer or SSO stating that your article and any accompanying graphics and pictures are unclassified, nonsensitive, and releasable in the public domain OR that the accompanying graphics and pictures are unclassified/FOUO. Once we receive your article, we will send you a sample form to be completed by your security personnel.**
- ◆ A cover letter (either hard copy or electronic) with your work or home email addresses, telephone

number, and a comment stating your desire to have your article published.

- ◆ Your article in MS Word. Do not use special document templates.
- ◆ A Public Affairs release if your installation or unit/agency requires it. Please include that release with your submission.
- ◆ Any pictures, graphics, crests, or logos which are relevant to your topic. We need complete captions (the who, what, where, when, why, and how), photographer credits, and the author's name on photos. **Do not embed** graphics or photos within the article's text, attach them as separate files such as .tif or .jpg. Please note where they should appear in the article.
- ◆ The full name of each author in the byline and a short biography for each. The biography should include the author's current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications. Please indicate whether we can print your contact information, email address, and phone numbers with the biography.

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

Send articles and graphics to [sterilla.smith@conus.army.mil](mailto:sterilla.smith@conus.army.mil) or by mail on disk to:

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

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

# USAIC Commanding General's Top 15 Reading List

"If you only have time to read 15 books this year, read these."



**Ghost Wars: The Secret History of the CIA, Afghanistan and Bin Laden, from the Soviet Invasion to September 10, 2001** by Steve Coll, 2004.



**The Multiple Identities of the Middle East** by Bernard Lewis, 2001.



**What Went Wrong: Western Impact and Middle East Response** by Bernard Lewis, 2002.



**A Peace to End All Peace: The Fall of the Ottoman Empire and Creation of the Modern Middle East** by David Fromkin, 2001.



**From Beirut to Jerusalem** by Thomas Friedman, 1990.



**Longitudes and Attitudes: Exploring the World after September 11** by Thomas L. Friedman, 2002.



**The Crisis of Islam: Holy War and Unholy Terror** by Bernard Lewis, 2004.



**Seven Pillars of Wisdom** by T. E. Lawrence, 1991.



**Understanding Terror Networks** by Marc Sageman, 2005.



**Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam** by John A. Nagl, 2002.



**Insurgency and Terrorism: Inside Modern Revolutionary Warfare** by Bard O'Neill, 1990.



**The Age of Spiritual Machines: When Computers Exceed Human Intelligence** by Ray Kurzweil, 2000.



**In Athena's Camp: Preparing for Conflict in the Information Age** by John Arquilla, 1997.



**Lexus and the Olive Tree: Understanding Globalization** by Thomas Friedman, 2000.



**The Sling and the Stone: On War in the 21st Century** by Thomas X. Hammes, 2006.

# **USAIC Commanding General's Iraq / Afghanistan / Iran Reading List**

**The Assassins Gate: America in Iraq**  
by George Packer, 2005.

**Bear Went Over the Mountain: Soviet  
Combat Tactics in Afghanistan**  
by Lester W. Grau, 1996.

**The Fragmentation of Afghanistan:  
State Formation and Collapse in the  
International system, second edition,**  
by Barnett R. Rubin, 2002.

**Ghost Wars: The Secret History of  
the CIA, Afghanistan and Bin Laden,  
from the Soviet Invasion to September  
10, 2001** by Steve Coll, 2004.

**A History of Iraq** by Charles Tripp, 2002.

**The Iranians: Persia, Islam and the Soul  
of a Nation** by Sandra Mackey, 1998.

**Know Thine Enemy** by Edward Shirley, 1997.

**The Kurds in Iraq: The Past, Present  
and Future** by Tom Blass and  
Kerim Yildiz, 2004.

**The Other Side of the Mountain:  
Majahideen Tactics in the Soviet-  
Afghan War** by Ali Ahmad Jalali, 2003.

**The Reckoning: Iraq and the Legacy  
of Saddam Hussein** by Sandra Mackey,  
2002.

**Soldiers of God: With Islamic Warriors  
in Afghanistan and Pakistan**  
by Robert D. Kaplan, 2001.

**The Shi'is of Iraq** by Yitzhak Nakash,  
2003.

**Tehran Rising: Iran's Challenge to the  
United States** by Ilan Berman, 2007.

The Director of Doctrine, U.S. Army Intelligence School and Fort Huachuca, would like to announce the worldwide staffing of the Initial Draft of the new FM 2-0, Intelligence. When published, the new FM 2-0 will replace the current FM 2-0, 17 May 2004, with Change 1 dated 11 September 2008.

FM 2-0 is the Army's keystone manual for Military Intelligence (MI) doctrine. It describes —

- ◆ The fundamentals of intelligence operations.
- ◆ The operational environment.
- ◆ The intelligence warfighting function.
- ◆ The intelligence process.
- ◆ MI roles and functions within the context of Army operations.
- ◆ Intelligence in unified action.
- ◆ Intelligence considerations in strategic readiness.
- ◆ The intelligence disciplines.

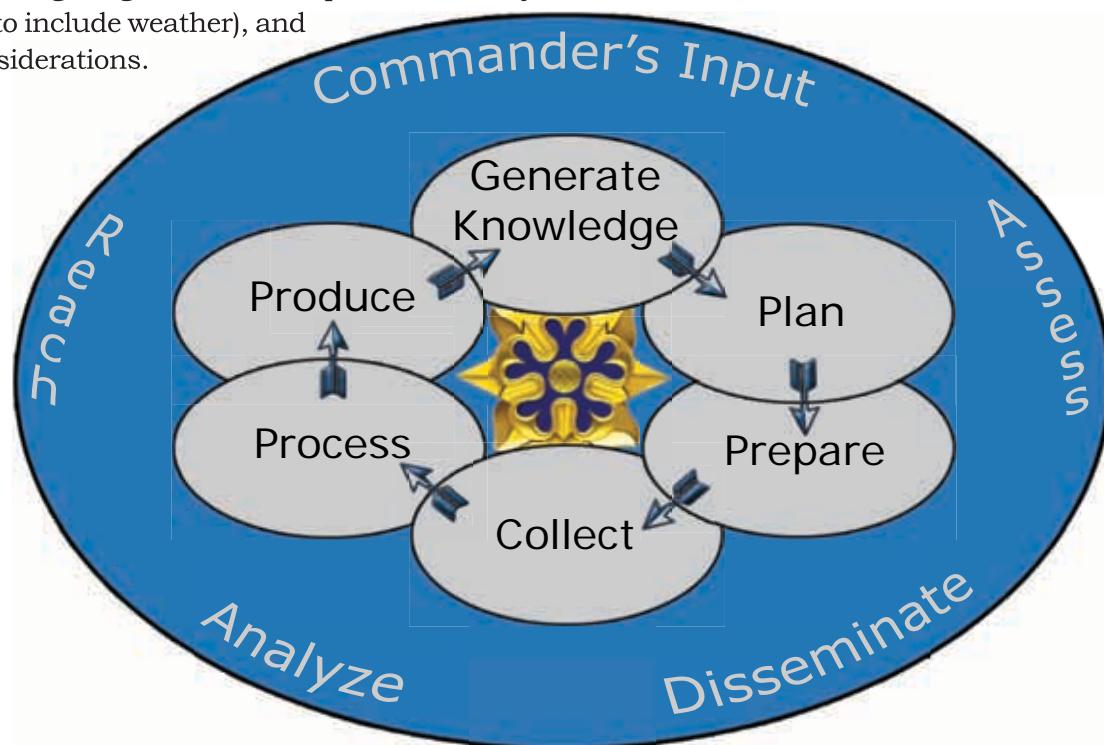
This FM provides doctrinal guidance for the intelligence warfighting function in support of commanders and staffs. It also serves as a reference for personnel who are developing doctrine; tactics, techniques, and procedures; materiel and force structure; and institutional and unit training for intelligence operations. It forms the foundation for MI and intelligence warfighting function doctrine development.

The Initial Draft updates outdated concepts and adds several new concepts and definitions. These include:

- ◆ Replaces the intelligence battlefield operating system with the intelligence warfighting function and discusses the mission variables for which the intelligence warfighting function is responsible: enemy, terrain (to include weather), and civil considerations.

- ◆ Updates the intelligence tasks (METL).
- ◆ Addresses the concept of actionable intelligence.
- ◆ Reintroduces the four characteristics of effective intelligence (timely, relevant, accurate, predictive, and tailored).
- ◆ Updates the definition of priority intelligence requirements and defines intelligence requirements.
- ◆ Updates the intelligence process, adding a sixth step (Generate Knowledge) and two additional functions (Commander's Input and Intelligence Reach).
- ◆ Introduces the concept of the intelligence survey as a means to provide the unit intelligence officer with an initial assessment for recommending intelligence asset apportionment within the area of operation (AO) and how best to use the unit's intelligence assets within the AO.
- ◆ Increases the number of intelligence disciplines from 7 to 9 by adding Geospatial Intelligence (GEOINT) and Open-source Intelligence (OSINT).
- ◆ Discusses the concept and includes the Army definition of reconnaissance, surveillance, and target acquisition/intelligence, surveillance, and reconnaissance (RSTA/ISR).
- ◆ Addresses the concept of Red Teaming.
- ◆ Addresses the concept of critical thinking.
- ◆ Updates each of the intelligence discipline chapters.
- ◆ Updates the linguist support appendix.
- ◆ Adds a short discussion of language technology.

*The point of contact for comments on FM 2-0 is Michael Brake at [Michael.brake@us.army.mil](mailto:Michael.brake@us.army.mil), COMM: (520) 538-1021 or DSN 879-1021.*



**ATTN: MIPB (ATZS-CDI-DM) 12  
BOX 2001  
BLDG 51005  
FORT HUACHUCA AZ 85613-7002**

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

**PIN:085011-000**