MIPB

Military Intelligence Professional Bulletin

July-September
2009
PB 34-09-3

GEOINT

FROM THE EDITOR

The employment of GEOINT in current tactical operations is highlighted by contributions from the field. MSG Cromer and LTCs McDonough and Conway from the 10th Mountain Division describe how that division developed a multi-disciplined GEOINT section providing fused analysis for lethal and nonlethal operations. The 3rd MI Center, NGIC, provides information on the employment of the Global Broadcast Service. Of interest to readers are two other articles from the Center outlining its training opportunities for the deploying GEOINT Soldier and an article by CPT Nohle discussing improvements to the Shadow TUAS.

CPT Christiana offers tips on successful targeting within the current operating environment (COE); CPT Olson discusses threats to U.S. forces through cyberspace in the COE; LTC Tatarka discusses the overlooked importance of adequate sleep for the intelligence analyst; and LTC Johnson gives some cautionary advice regarding the impending withdrawal of U.S. forces from Iraq. From CAC, we have an introductory article regarding the Doctrine reengineering project and the WIKI pilot program.

Themes have been set for the following issues:

		Suspense for submissions:
Oct Dec 2009	ISR	30 Dec 2009
Jan Mar 2010	Cultural Awareness	Special Issue
Apr Jun 2010	MI at Battalion and Below	30 Apr 2010
Jul Sep 2010	MI Organizations and Training Strategies	30 Jul 2010

Future topics for 2010 and 2011 are: Advanced Analysis; HUMINT; AFRICOM; Joint MI; MI Support to Non-MI Units; Law Enforcement; Homeland Security; Intelligence TRADOC Capability Managers (TCMs). If you are interested in writing an article for any of these topics, please see our contact and submission information within this issue.

Sterilla A. Smith
Editor

MILITARY INTELLIGENCE

PB 34-09-3 **Volume 35 Number 3** **July - September 2009**

FEATURES

DEPARTMENTS

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

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

By order of the Secretary of the Army:
Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0929306

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

ALWAYS OUT FRONT

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

My column for this issue of MIPB focuses on an enduring intelligence capability that is critical to the current fight and to all future operations–Weapons Technical Intelligence (WTI). It is important for all Military Intelligence Soldiers and professionals to understand how this capability is shaping current operations and its future within all full-spectrum operations. The advancement in biometrics, forensics, and other technical capabilities has provided the Department of Defense (DOD) with incredible tools that significantly improve our ability to rapidly exploit sites, equipment, and information. This exploitation and intelligence analysis in turn improves our ability to rapidly identify, and eliminate enemy threats. In Operation Iraqi Freedom (OIF), these capabilities led to the development of Weapons Intelligence Teams (WIT), the tactical collection capability that feeds WTI. WTI represents a significant evolution of Technical Intelligence (TECHINT) capabilities through the incorporation of the latest biometrics and forensics technologies into the primary functions of collection, exploitation, and intelligence analysis. Coalition Forces have made great improvements in identifying and defeating insurgent improvised explosive devices (IEDs) networks through the use of these critical capabilities.

Based on current operations, WTI has evolved as a significant subset of TECHINT that focuses on weapons including IEDs, associated components, improvised weapons, and other weapon systems. TECHINT as an intelligence discipline has been a part of U.S. Army operations since World War II. While the U.S. has had a long history of employing TECHINT in warfare, this is the first time that biometric and forensic technologies have become a major part of intelligence efforts and an inextricable part of TECHINT operations. Our focus on countering a conventional threat during the Cold War and post-Cold War periods naturally led TECHINT to focus on responding to national and strategic Scientific and Technical Intelligence (S&TI) requirements. Today, when faced with an adaptive insurgent threat that deftly employs asymmetric threats against our forces, WTI places the right emphasis on responding to the tactical commander's intelligence requirements. This WTI focus results in the ability to more rapidly defeat insurgent networks that are difficult to detect and exploit and vary from one area of operation to the next.

As OIF progressed beyond 2004, IEDs emerged as the most lethal weapon U.S. forces faced. In order to counter the IED threat, DOD instituted a WTI capability largely based on a British model used in operations in Northern Ireland. The purpose was to identify insurgent IED manufacturers in order to target the production and supply networks that allowed IEDs to proliferate throughout Iraq. The National Ground Intelligence Center (NGIC) developed the Counter-IED (C-IED) Targeting Program (CITP) to provide strategic and operational analytical support to the Warfighter. WITs were created to collect materiel and information to support WTI analysis and exploitation. The Combined Explosives Exploitation Center (CEXC) also contributed to WTI by providing detailed technical and forensic exploitation of IEDs to maximize the information collected from a particular IED. Thus, the three major components of WTI: collection (employing a WIT); exploitation (performed by the CEXC), and analysis (at the CITP), came together to provide a critical capability. Together, this WTI capability resulted in more timely and accurate support to targeting of networks, sourcing of materiel, support to prosecution, and support to force protection.

(Continued on page 2)

CSM FORUM

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

Our United States Army has developed considerably over the several hundred years of its existence. It has progressed from fighting wars using early forms of intelligence collection such as scouts on horseback during the American Revolution to the unmanned aerial aircraft in today's War on Terror. The battlefield is constantly changing and our forces continue to improvise, adapt, and evolve to the level that is required of our fighting forces to find, know, and never lose the enemy. The Defense Intelligence Community (IC) has expanded so vastly that it has divided into several intelligence disciplines required to extract every bit of truth and knowledge from our enemies and suppress any threat necessary to protect our nation's freedoms. A major development within the IC is the evolution of Geospatial Intelligence (GEOINT).

GEOINT is a form of intelligence collection that has become technologically advanced. It is the form of intelligence that could be best described as our modern-day reconnaissance capability. GEOINT comes in several forms, to include Motion Imagery Exploitation, Advanced Geospatial Intelligence, Geospatial Analysis, Moving Target Indicator (MTI), Commercial Imagery, Precision Targeting, and Multi-Intelligence Fusion. All of these sub-disciplines are what make up our "eyes in the sky" or GEOINT.

Consider past wars and conflicts where reconnaissance was needed to help ground commanders make timely decisions. Some forms of intelligence and reconnaissance information gathering included Long Range Reconnaissance Patrol units moving tactically, in small elements of five to eight Rangers over vast distances, only to report back to their headquarters and provide distance, direction, and identification of enemy forces. High flying aircraft manned by one, two, or several service members obtaining photographic intelligence of an enemy patrol base is another example. Although, those methods were effective during those time periods, the main flaw of these intelligence gathering capabilities was the inability to take the raw data from the Soldiers and Airmen in a timely manner and create a product that ground commanders could use to shape the battlefield in which their units must operate.

In today's current War on Terror, GEOINT has proven to be extremely successful on the battlefield. Everyday, GEOINT gives our ground forces the "eagle's eye" view of insurgents emplacing improvised explosive devices on coalition supply routes. Everyday, GEOINT provides the collaborating information that further solidifies intelligence gathered by other disciplines to include Human (HUMINT) and Signals (SIGINT) Intelligence. Everyday, GEOINT gives ground commanders live video feed and imagery of weapons caches, insurgent training camps, insurgent strongholds, enemy movement and more. GEOINT's capabilities have reached far beyond the imagination of our enemies abroad.

Our GEOINT Soldiers (MOS 35H Common Ground Station (CGS) Operator and MOS 35G Imagery Analyst) in training are performing missions for Soldiers down range every day. They are currently training with real time feed from abroad in Operations Iraqi Freedom and Enduring Freedom (OIF/OEF). They're augmented during training by analytical sensors via video to them from theater. This becomes value added in what a GEOINT Soldier can provide once deployed because the newly graduated Soldiers already have the most up-to-date knowledge of enemy tactics, techniques, and procedures (TTPs) and the latest equipment used to discover these enemy TTPs on the ground. This wealth

(Continued on page 5)

(Continued from page 2)

The future of WTI is vital to our success in an era of persistent conflict. We are building this critical intelligence capability into our future force, ensuring that it incorporates law enforcement, Explosive Ordnance Disposal, and intelligence expertise based on the Operational Environment. As threat capabilities develop beyond IEDs, it is crucial that we are able to employ an effective WTI capability to meet the entire spectrum of threat systems. Various DOD organizations, the Department of the Army, NGIC, and TRADOC are working diligently to develop an enduring WTI capability. For example, in 2008, DOD announced that WTI would become an enduring capability with the Army as the service proponent. The Intelligence Center of Excellence has been a key member of this Army team from the very beginning and has developed Training Circular (TC) 2-22.4, Technical Intelligence (TECHINT), the TECHINT doctrine that will help guide the WTI capability. Additionally, we are currently staffing TC 2-22.401, Weapons Technical Intelligence (WTI). This TC will provide the most comprehensive doctrine to date on tactical battlefield employment of WTI capabilities and operational and strategic WTI capabilities that will help the Warfighter accomplish his mission.

The Weapons Intelligence Course (WIC) is currently held at Fort Huachuca to train soldiers deploying to OIF and Operation Enduring Freedom (OEF) to conduct the WTI mission in OIF and the C-IED Team mission in OEF. This course has already trained 361 soldiers, sailors, airmen, and marines in battlefield WTI techniques. An ongoing effort to determine force structure changes to support WTI will be completed in March 2010. This effort will impact the Army for years to come and it is imperative that we provide the Army an effective and efficient enduring capability to meet future threats. Using WTI lessons learned, TECHINT capabilities will also be updated to ensure that future developing enemy communications, mobility, and intelligence, surveillance, and reconnaissance technologies are collected, exploited, and analyzed as well. The Intelligence Center will soon be setting up a WTI website for your input and comments as we further develop this capability. Look for it and participate.

As we move forward with experimental, conceptual, force structure, doctrinal, and training developments, we will need your help in getting the issues right, finding viable solutions, and carefully articulating a path forward for WTI. These are changing and challenging times but our constant is the quality of intelligence we provide as the critical warfighting function of the preeminent land force in world history.

Always Out Front!

(Continued from page 3)

of knowledge is constantly being refreshed and updated in a GEOINT Soldier's mind. The OPTEMPO of GEOINT has risen so much that leadership is now implemented in the school house training. CGS Operators and Imagery Analysts will soon be combined into one MOS. This will give a ground commander greater use of their Soldiers who will have the training and ability to use of MTI and Imagery interchangeably.

GEOINT is not a name but a technology and TTP change. We are teaching our Soldiers basic skills of GEOINT and analysis to provide sub-terrain information in a model form for a commander on the ground to include detailed knowledge of possible ingress and egress routes for enemy insurgents, entry points to building roofs, depth of walls and terrain features such as hills, mountains and caves and more while they learn how to manipulate light directional arrangement. This type of information, provided by GEOINT reporting and analysis, has validated HUMINT and SIGINT reporting at multiple levels and helps a ground commander make more solid and informed decisions to not only suppress an enemy threat but map out an area of operation for a successful foot patrol.

A recent graduate of GEOINT here in Fort Huachuca, Arizona wrote, "Many of the things that I have learned in the school house definitely apply here. Due to mountainous terrain, it is somewhat difficult to pinpoint caches but my team has been able to find 3 major ones that were in caves that no other form of intelligence was able to confirm or deny." It is Soldiers like these that show the IC that we are on the right track to victory over terrorism. However, we must continue to develop technology faster than our enemies can react.

The possibilities of GEOINT are endless and constantly evolving. We are changing our training and developing GEOINT capabilities as fast as our enemies are changing their TTPs. We have come a long way since our forefathers in the American Revolution, our patriots of the World Wars, and the Soldiers who fought in the jungles of Vietnam. Regardless of the change in the way our Soldiers fight a war, our mission remains the same–*find, know, and never lose the enemy.*

NCOs Lead from the Front!

The intent of this project is to:

- Make doctrine more responsive to the user.
- More effectively maintain Army doctrine by redefining what doctrine contains.
- Make doctrine more accessible to the user.

To do this, the Army must change how to categorize doctrine and how to develop and maintain it. There are several tasks to the project. First, the Army will reduce the amount of doctrine to a manageable level, that which can be kept current with the current doctrine resources. Two key elements apply to this task-reduce the number of manuals and reduce the size of manuals. Both elements will make it easier to write and maintain doctrine that is current. Second, the Army will move much of doctrine from the current category of field manuals (FM) to a new category of manual–the Army tactics, techniques, and procedures (ATTP). The majority of ATTP will be updated through a wiki-like process that allows users in the field to make changes to the ATTP.

The U.S. Army Training and Doctrine Command (TRADOC) commander's intent for this is encapsulated in the following guidance provided to the Combined Arms Center (CAC):

- *FMs: The principles. Enduring.* The vocabulary of our profession. Posted on-line in read-only format. Non-negotiable with our audience. Foundation of Programs of Instruction. Revised very carefully and deliberately.
- ATTP: *Informed by current events. Adaptable.* Posted on-line in open collaboration (Wiki). Revised whenever someone takes the time to log on and share their professional experiences. Self-governing. Periodic review by proponents.

To accomplish this goal, the Combined Arms Doctrine Directorate (CADD) has thoroughly scrubbed existing doctrine to determine what to retain as doctrine and what to move into some other category. The first step was to redefine these categories. Without going into detail, the following discussions were used as working definitions until Army and TRADOC regulations that deal with doctrine can be formally changed.

An FM is a Department of the Army publication that contains doctrine principles, with common and enduring TTPs that apply across the force, and that describes how the Army and its organizations operate while conducting operations and training for those operations. FMs pertain to the operating force, and those parts of the generating forces that deploy with, or directly support, that force in the conduct of operations.

An FM will contain information that:

- Is intended to apply to forces worldwide and is not limited to specific areas of responsibilities, joint operations areas, or countries.
- Relates to the conduct of combined arms operations or applies to two or more proponencies or branches.
- Has enduring qualities such that the information is intended to be applicable for an indefinite period.
- Explains how various echelons function during operations.
- Describes how the forces operate using internal techniques and procedures that apply across multiple echelons, branches, and proponencies.
- Or, is the keystone publication for a proponent.

An FM does not contain the following types of information or instructions:

- How the Army operates in garrison or is administered.
- Techniques or procedures for the conduct of training (except FM 7-0, Training for Full Spectrum Operations).
- Details on maintaining, using, operating or training on equipment, to include weapons or weapons systems.
- TTP that have a limited shelf life (pertain to specific enemies, locations, or ongoing operations). These TTP are covered by ATTP manuals (see below), lessons learned, best practices, and local area networks.
- Prescriptive information that directs detailed procedures that must be followed precisely. information that is prescriptive is not normally included in FMs but in other publications. The exceptions to this are terms and symbols.

An ATTP manual relates primarily to the conduct of a single branch, functional area, or company, troop, battery, or lower echelons and staff sections. Updating ATTP manuals will be a wiki-like process patterned after Wikipedia. On 2 July, TRADOC launched a pilot program placing seven draft and current FMs and ATTPs on an Army Knowledge Online (AKO) doctrine wiki site. Department of Defense (DOD) personnel can quickly access the site, review the text, and add changes to the documents on-line. This wiki venue will enable DOD personnel, especially Soldiers, to input valuable TTPs quickly from their current deployments and recent experiences. Such immediate input will make TTP more relevant to today's warfighter. Wiki doctrine aims to ensure input is contributed to ATTPs at the widest and lowest levels of the Army versus a small section of subject matter experts. Personnel can access the web site with a common access card or AKO username and password at https://wiki.kc.us.army.mil/wiki/Portal:Army_Doctrine. Civilian and military personnel are encouraged to visit this site and make changes to these manuals which can be accessed through AKO using the following procedure:

- First log on to AKO.
- On the tool bar, select *Self Service,* then *My Doctrine.* This will take one to the Army Publishing Directorate's (APD) doctrine repository.
- Look in the left-hand column for the *ATTP Pilot* button.
- Click this button to enter the Army Doctrine Portal.
- From here, access and make changes to the test publications. A good place to start is the *Getting Started* and *Army Doctrine Portal Rules of Conduct.*

In addition to creating this distinction between FMs and ATTP manuals, the Army has also pared down the number of publications considered to be doctrine. All gunnery manuals and all handbooks are moving into the training circular (TC) category. Many highly technical publications are moving into the general subject technical manual (TM) category. This will allow doctrine writers to focus on the conduct of operations in the field. Finally, many FMs that no longer apply to the current and projected force are being rescinded.

When all these changes are accomplished, the figures will tally close to these lines:

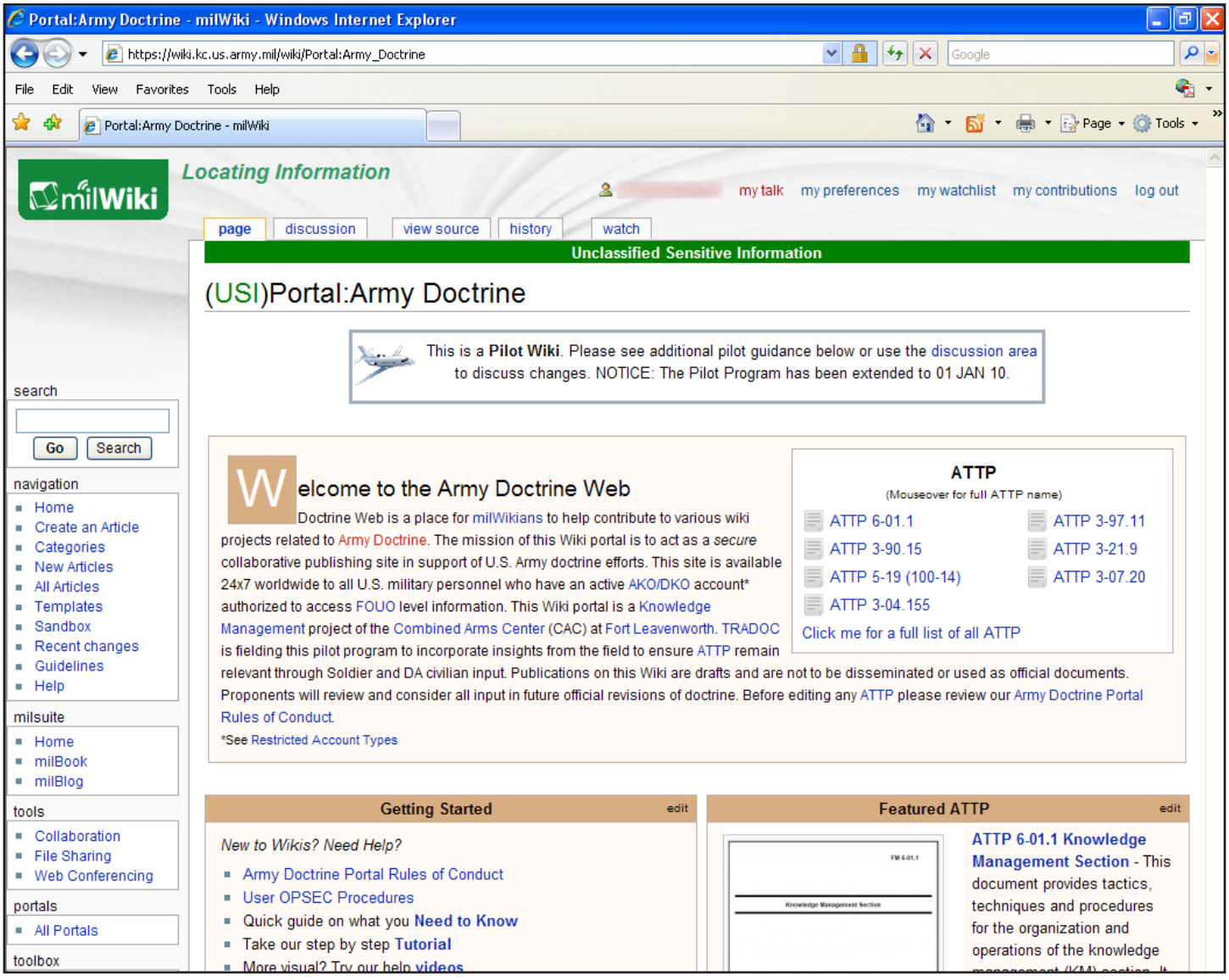
- To remain as FMs-94.
- To become ATTP-257.
- Rescind outdated FMs-74.
- Move to TMs all FMs that deal with technical procedures-62.
- Move to TCs all FMs that deal primarily with training-40.

Criteria for reducing the size of manuals. In addition to reducing the number of FMs, the Army will reduce the size of those manuals that remain. The target size is 200 or less pages. A few of the top-level manuals may exceed this limit to provide the overarching constructs that will eliminate the need for repetition in subordinate FMs. The guiding principle is to not duplicate information contained in other publications. This ensures that doctrine is consistent, avoids unnecessary duplication and modification, and

ensures that FMs do not automatically become obsolete when other FMs are revised. Specifics will be included in a rewrite of TRADOC doctrine regulation.

Doctrine Education and Training Board. In addition to reengineering the doctrine process and structure, CAC has stood up a Doctrine Education and Training Board to evaluate how best to inculcate doctrine into the force, both the generating and the operating force. Part of the TRADOC CG's guidance was that FMs are to be the "Foundation of Programs of Instruction." In addition, the Army needs to do a better job of advising and informing the field of changes in doctrine and the implications for the DOTMLPF domains. The Doctrine Education and Training Board will look for programs that can improve the Army's knowledge and use of doctrine.

Doctrine DVD. The APD Website (accessible through AKO at https://akocomm.us.army.mil/usapa/index.html) contains all unclassified doctrine publications. APD has also published a set of DVDs (EM 0205 IDN 990003, dated 1 December 2008) with all Army FMs on it. One disc contains all FMs that are Distribution Unrestricted. The second contains those FMs that are Distribution Restricted. Using the DVDs enables one to download the entire doctrine library onto a hard drive even without internet access or bandwidths limiting download capabilities from the Website. This is a significant upgrade from the previous CD ROM set but still needs to be better. CADD would like any ideas for making this more user friendly or more useful. Please send any suggestions to clinton.ancker@us.army.mil.



by Master Sergeant Michael S. Cromer, Lieutenant Colonel William G. McDonough, and Lieutenant Colonel John A. Conway

Introduction

Geospatial Intelligence (GEOINT) analysis truly drives the majority of our combat operations in Multi National Division-Center. The 10th Mountain Division (LI) established a GEOINT section and analytical approach resulting in more holistic and multi-disciplined intelligence products that most comprehensively displays fused analysis for commanders. At the base of this analysis is ground moving target indicators (GMTIs) upon which all other available intelligence is "layered." The section is designed to support lethal and nonlethal operations; exploit all available intelligence information in order to understand and characterize patterns of life activity for areas of interest (AIs) or on specific individuals; target tracking and/or development, and tipping and cueing for intelligence, surveillance, and reconnaissance (ISR) operations.

The section uses established analytical "Battle Drills" where all significant activities (SIGACTs) and cache finds are automatically analyzed based off historical GMTI data and ISR forensics to assist in situational understanding of why and how events occurred. This effort started at Fort Drum, New York with the GEOINT section able to conduct live environment training prior to deployment to Iraq. Once in Iraq, the section further developed their processes and products which are largely designed to be immediately actionable by both U.S. and Iraqi ground maneuver forces.

Background

In February 2006, the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) designated GEOINT as an intelligence discipline. It envisioned the GEOINT concept as a collaborative effort between the Intelligence and Engineer Communities. In June 2006, the USAIC&FH-U.S. Army Engineer GEOINT Memorandum of Agreement (MOA) defined GEOINT as intelligence "derived from the exploitation, analysis, and fusion of imagery with geospatial information to describe, assess, and visually depict physical features and geographically referenced activities in the battlespace. GEOINT consists of imagery, imagery intelligence (IMINT) and geospatial information." In sum, GEOINT was the combination of IMINT and Geospatial Information and Services (GI&S) data.[1]

Additionally, in September 2006, the National Geospatial-Intelligence Agency (NGA) defined GEOINT as "the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. GEOINT consists of imagery, Imagery Intelligence, and geospatial information"–reinforcing the June 2006 joint USAIC&FH-U.S. Army Engineer GEOINT MOA definition.[2] The IMINT portion of GEOINT includes electro-optical (EO), advanced geospatial intelligence or imagery-derived Measurement and Signatures Intelligence (MASINT), overhead non-imaging infrared, synthetic aperture radar, GMTI, infrared (IR), and full motion video (FMV).[3]

Geospatial data is considered the main source of data for the components of GEOINT–IMINT and GI&S. However, NGA expanded its definition by stating that GEOINT "incorporates data from other intelligence disciplines, such as Human Intelligence (HUMINT), Signals Intelligence (SIGINT), MASINT, and Open Source Intelligence (OSINT)….to corroborate and provide context to geospatial data and information; they are integral to the GEOINT discipline. The consideration or use of all types of intelligence, or multiple-source intelligence (multi-INT), adds additional perspective to ensure a more comprehensive GEOINT product. The full potential of GEOINT is realized when different types of geospatial and intelligence data are combined, an-

alyzed using intelligence information, and/or integrated into a single geospatial product."[4] The 10th Mountain Division's GEOINT section embodies this expansive and holistic GEOINT definition.

Genesis

Since the GEOINT concept is relatively new within the Army, other observed nascent efforts and products as well as professional writings, presentations, and unofficial email overwhelmingly emphasize the IMINT and GI&S aspects of GEOINT as opposed to the fuller and richer concept of GEOINT which results in comprehensive multi-intelligence products. This narrow IMINT and GI&S-only focus results in geospatial data overlaid on images with little to no use to other intelligence disciplines and arguably of little use to units on the ground.

The beginnings of the 10th Mountain Division (LI) GEOINT section started with the objective of providing multi-intelligence GEOINT products of value to the subordinate brigades (and later Iraqi partners) and the division headquarters. The placement of subordinate units in front of the division headquarters is not an error; the emphasis of the division and GEOINT products are the action arms on the ground. GEOINT products are designed as actionable by a unit on the ground or as a tipping/cueing product for ISR collection. Typical products include analysis of suspected training facilities; key terrain; illegal border crossing sites; cities/routes; tactical reporting; high value individuals; explosively formed projectile/improvised explosives device (IED)/indirect fire incidents; caches; smuggling routes; pre/during/post operations; GMTI density; GMTI pattern of life; specific areas, and missing/captured personnel reporting.

In June 2007, the 10th Mountain Division (LI) G2 approved the GEOINT Concept of Operations, which outlined the vision, hardware and software requirements, and task organization for the section. The Division GEOINT section was specifically designed to process and analyze multiple sourced data–Communications Intelligence (COMINT), HUMINT reporting, tactical reporting, GMTI analysis, Imagery Analysis, and geospatial data.

Organization and Functions

The GEOINT section was manned from portions of the division G2 Analysis and Control Element's (ACE) Modified Table of Organization & Equipment (MTOE). The section's design and optimal strength is 22 Soldiers based on the following portions of the MTOE:[5]

Division Tactical Exploitation System (DTES) Section

GEOINT Section Title	MTO&E Title	Rank/MOS	Quantity
OIC	Imagery Technician	CW2/350G0	1
Imagery Analyst	TES Data Analyst	E5/35G20	1
SIGINT Analyst	TES Data Analyst	E5/35N20	1
Imagery Analyst	TES Data Analyst	E4/35G10	1
SIGINT Analyst	TES Data Analyst	E4/35N10	1

Common Ground Station (CGS) Section

GEOINT Section Title	MTOE Title	Rank/MOS	Quantity
NCOIC	Senior CGS Sergeant	E7/35H40	1
Team Leader	CGS Sergeant	E6/35H30	2
Forensic GMTI Analysts / Real-Time GMTI Analysts	CGS Operator	E5/35H20	2
Forensic GMTI Analysts / Real-Time GMTI Analysts	CGS Operator	E4/35H10	4
Forensic GMTI Analysts / Real-Time GMTI Analysts	CGS Operator	E4/35H10	4

Tactical Command Post (TCP) 1 Fusion Cell

GEOINT Section Title	MTOE Title	Rank/MOS	Quantity
Imagery Analyst	Imagery Analyst	E5/35G20	1
Imagery Analyst	Imagery Analyst	E4/35G10	1

Tactical Command Post (TCP) 2 Fusion Cell

GEOINT Section Title	MTOE Title	Rank/MOS	Quantity
Imagery Analyst	Imagery Analyst	E5/35G20	1
Imagery Analyst	Imagery Analyst	E4/35G10	1

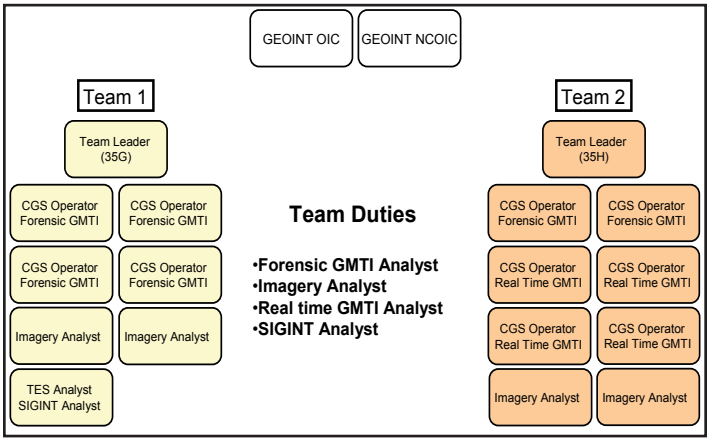


Figure 1. GEOINT Section - Proposed

The GEOINT section's task organization was fluid, based upon personnel shortages. The vision was to organize the section with an OIC and NCOIC overseeing two teams each led by a CGS Staff Sergeant (See Figure 1). Each team consisted of five additional Military Occupational Specialty (MOS) 35H

Common Ground Station (CGS) Operators, three MOS 35G Imagery Analysts, and one MOS 35N Tactical Exploitation System (TES) Data Analyst. We purposely placed all 35Gs into the GEOINT section for two reasons. First, while 35Hs can perform the functions of a 35G to a degree, 35Gs are overall simply better prepared and trained to perform imagery analysis and collection. Second, because we had all 35Gs on hand early in the pre-deployment train up for Iraq, they mitigated the shortage of 35Hs, many of which did not arrive until the mission readiness exercise or in theater. Later, because we did not receive a full complement of MTOE Soldiers and suffered some attrition, we adjusted the task organization to two teams; one led by a CGS Staff Sergeant and one led by an Imagery Analyst Staff Sergeant and a different mix of 35Hs, 35Gs, and one 35N (See Figure 2).

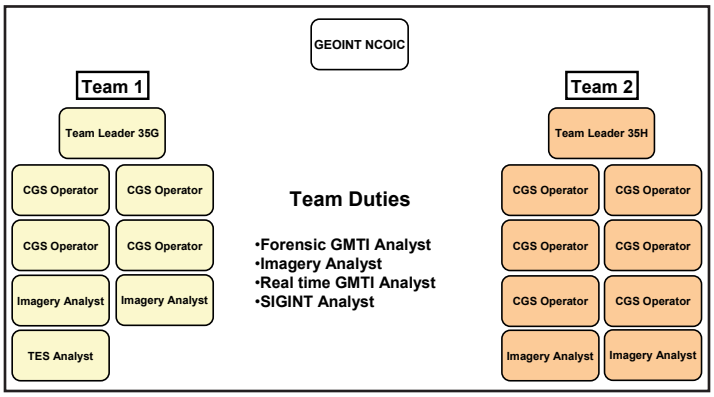


Figure 2. GEOINT Section - Actual

We trained our 35H personnel on the use of Softcopy Exploitation Tool–BAE Systems' SOCET GXP software, the Imagery Workstation (IWS), and Imagery Analysis techniques. We also maintained their CGS operator and GMTI analysis skill sets. Additionally, we cross-trained our 35Gs on GMTI analysis using ISR Forensics (ISRF) software. Finally, we trained our 35N to collect and analyze SIGINT related data via the DTES. Our 35N Soldier also worked in conjunction with the G2 ACE SIGINT Section for access to NSANet and other SIGINT resources not available in the DTES and conducted limited cross training on other GEOINT systems.

Each team was further broken down into technical and/or functional specialties. Most were aligned by MOS, some by individual capability. These areas of focus are: Forensic GMTI Analyst, Imagery Analyst, Real-Time GMTI Analyst, and SIGINT Analyst. The team leader received the project, broke out the analyst tasks, and monitored the progress for each analyst's task(s).

Forensic GMTI Analysts research historical GMTI data via Web-Based Access and Retrieval Portal, Air Force Research Laboratory, or the GMTI Data Warehouse (upon its availability). The data is displayed, analyzed, and cross-cued with the IMINT and SIGINT Analysts (and other intelligence disciplines as applicable). This assists Forensic GMTI Analysts in properly identifying what a GMTI track of interest is doing. Analysts cross reference the GMTI data with locally available Compressed ARC Digitized Raster Graphics (CADRG) and Controlled Image Base (CIB) one meter imagery as well as national imagery. They also use geospatial data such as routes, boundaries, key locations, bridges, and road conditions to make sense of the GMTI data. GMTI information without geospatial data can often lead to inaccurate or meaningless reporting. For example, when displaying an Iraqi border fort shapefile with overlaid GMTI track data indicating movement around the Iran/Iraq border, it becomes obvious that the tracks are simply traffic from one border post to another. Without the geospatial data, the GMTI tracks would be suspicious due to their proximity to Iran/Iraq border. The analyst also obtains, analyzes, and graphically displays HUMINT derived tactical reporting. By analyzing multi-intelligence reporting with GMTI patterns of movement, the analyst can draw conclusions as to whether or not the GMTI movement is suspicious.

Additionally, while all GEOINT analysts are trained in researching historic FMV, Forensic GMTI Analysts are the primary FMV data researchers. As such, they are responsible for checking the availability of historic FMV primarily through Raytheon's Persistent Surveillance and Dissemination System of Systems (PSDS2). If PSDS2 is unavailable, the analyst uses ISR Information Service to search for historic FMV. These analysts can capture applicable screen shots and submit the images to an Imagery Analyst for exploitation (using SOCET GXP image and geospatial analysis software and/or RemoteView imagery exploitation and analysis software).

Real-time GMTI Analysts are responsible for locating, tracking, and reporting near real-time (NRT) GMTI tracks which meet reporting criteria. They are also responsible for assisting in the creation of NRT GMTI derived products and target data. Real-time GMTI Analysts are also familiar with GMTI and

FMV real-time cross-cueing procedures. The analyst uses the CGS to provide NRT GMTI data and analysis. The CGS is linked via fiber optic wire with its Remote Workstation (RWS) located in the ACE. The RWS emplacement in the ACE allows for cross-cueing and ensures that real-time GMTI analysts are aware of current ACE operations. Real-time GMTI Analysts interact with other members of the GEOINT section in order to provide or receive amplifying intelligence data regarding potential NRT GMTI tracks.

Imagery Analysts are primarily responsible for providing imagery and imagery analysis using both classified and unclassified imagery using the DTES and Secret Internet Protocol Router Network (SIPRNet) commercial off the shelf (COTS) machines. They also provide imagery to our Forensic GMTI Analysts based upon forensic analysis. Our Imagery Analysts are cross-trained in GMTI analysis to facilitate the cross-cueing of imagery with the real-time GMTI Analyst. The Imagery Analyst also researches and analyzes HUMINT reporting as applicable. Finally, the Imagery Analyst produces normal IMINT products such as helicopter landing zone analysis, point target analysis, and area overview analysis.

The SIGINT Analyst researches SIGINT data for applicable reporting for a project and, if applicable, collaborates with the G2 ACE SIGINT Section for additional resources such as NSANet. The SIGINT Analyst also works in conjunction with both the Forensic GMTI and Imagery Analysts. The SIGINT Analyst is normally tipped by other GEOINT team members to a location where COMINT data is required. A fuller description of the SIGINT Analyst's duties is not available at the unclassified level.

The team leader ensures that, as appropriate, external entities are contacted to further enhance the multi-intelligence product. Common agencies, sections, and units include NGA; National Ground Intelligence Agency; National Air and Space Intelligence Center (NASIC); the division's IED–Defeat Cell, and subordinate brigade combat teams (BCTs). The GEOINT section fuses all of this data using organic COTS and Program of Record (POR) intelligence processors and new or upgraded intelligence analytical and product creation toolsets described later in this article.

An additional benefit in theater is NGA's embedded Geospatial Intelligence Support Team which provides five Imagery Analysts with a tremendous on site and reach back imagery analysis capability. This team is collocated with the division's GEOINT section and is, in fact, considered part of the GEOINT section while deployed.

Analysis

The incorporation and analysis of relevant intelligence data using a phased (from real-time to forensic), layered approach produces a multi-intelligence graphic analytical product designed to be actionable by a subordinate unit. Instead of several products and assessments covering the same requirement, the GEOINT section provides one encompassing stand-alone product capable of answering multiple essential elements of information (EEIs).

In addition to the mindset of conducting multi-intelligence analysis, the section's analytical approach is an interactive process throughout its phased analysis. The section provides both real-time and forensic analytical support, but they are not mutually exclusive. Forensic analysis drives real-time analysis and vice versa. For example, for a Cache Exploitation assessment, the GEOINT section analyzes historical data, whether it is GMTI, COMINT, and/or Imagery to detect changes in the environment. Forensic GMTI Analysts view historical GMTI based upon the location of the cache site. The historical GMTI analysis is used to link the cache to other sites to include associated caches and facilitator locations. This could lead to real-time GMTI collection and analysis to confirm or deny historic GMTI data or focus collection in other areas related to the historic cache data. The section also adds any HUMINT, SIGINT, and tactical reports. This analysis could serve as tipping/cueing for other collection such as FMV or subordinate units. Throughout this process is also the constant dialogue between internal ACE sections and the supported unit on the ground.

The GEOINT section is not only request for information (RFI) driven requiring specific taskings in order to focus its assets and resulting analysis but has the latitude to define its own projects based upon the operational environment (OE). GEOINT products avoid a plethora of data on a single slide. This ensures an avoidance of information overload and the end user's ability to quickly grasp and understand the final analysis. When completing large scale and more complex products, the end result is a product using a drilldown

method of graphic presentation. This type of product is interactive and enables the customer to drill down on specific points throughout the product as they see fit through the use of hyperlinks embedded into the final product. (See Figure 3).

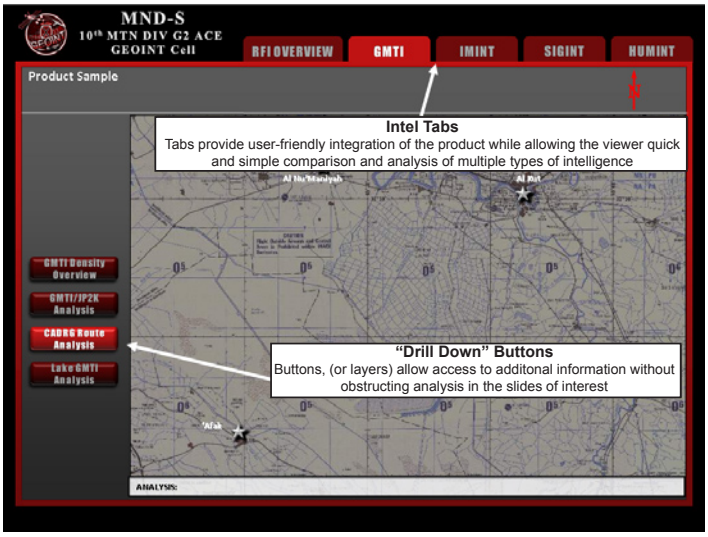


Figure 3. Example of a drilldown product

RFI Process

As mentioned, RFIs are one way that the GEOINT section focuses production effort. Figure 4, GEOINT RFI Production Flow, outlines our RFI process. The following vignette illustrates this process.

A unit asked for GEOINT analysis in order to determine current activity patterns within a certain marsh area and various locations. It wanted GMTI and Imagery Analysis along with GMTI Pattern of Life analysis in order to identify possible smuggling routes through the marsh and provide locations/points of interest for future ISR focus and Iraqi Department of Border Enforcement (DBE) operations.

Once the GEOINT section received the unit's RFI, the section leadership planned the actions required to complete the RFI and answer all EEI. An initial look at a map, a verification of U.S. and Iraqi maneuver unit locations, and a verbal briefing from the G2 ACE All Source section provided background information. Based on the scope and intent of the unit's request, the GEOINT section decided that a drilldown product was necessary since there would be multiple ways to exploit and display the marsh product. This process took approximately two hours.

The GEOINT Team NCOIC briefed the RFI to his analysts. Forensic GMTI Analysts were tasked to analyze GMTI using 30 days of historical data. Additionally, they were to research all HUMINT reporting within a three month period centered on the marsh. Finally, they were to fuse their historical GMTI analysis with other reporting and cross-cue relevant GMTI analytical findings with the Imagery Analysts.

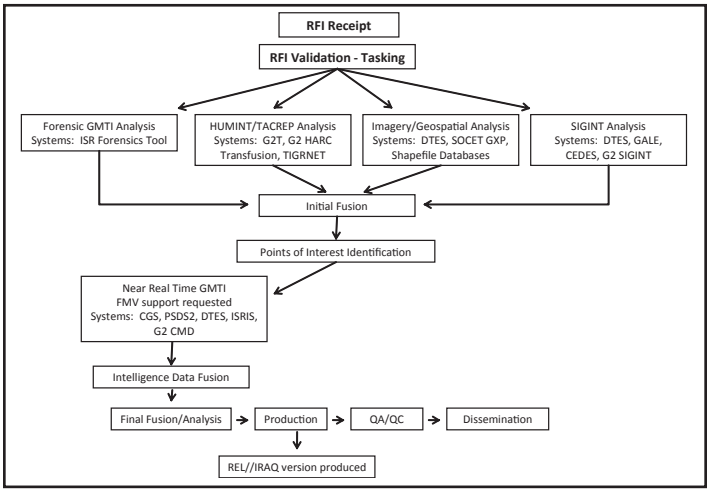


Figure 4. GEOINT RFI Production Flow

The Imagery Analysts were tasked to request up to date National Technical Means imagery of the entire marsh, create an imagery mosaic, research geospatial data for current DBE locations, research the NGA database for past products, and overlay the historical GMTI density plot on the new imagery mosaic to identify boat and land routes associated with the marsh. The analysts also used OSINT to identify the types of traditional boats used in the marsh and compared those pictures to the GMTI data and FMV. SIGINT analysts were tasked to pull all recent communications externals data in order to identify communication devices and patterns.

The Forensic GMTI, Imagery, and SIGINT analysts performed their tasks simultaneously with constant cross talk between analysts. When the Imagery Analyst completed the mosaic of the marsh, the Forensic GMTI Analyst provided the GMTI shapefile data to the Imagery Analyst who overlaid the data on the mosaic. This overlaid data highlighted movement activity and six key areas of interest (AIs.) These AIs were passed to the real-time GMTI Analysts who monitored the areas using NRT Joint Surveillance Target Attack Radar System (JSTARS) GMTI and verified that the forensic analysis was valid. The real-time GMTI Analysts cross-cued the live data with a FMV asset equipped with EO/IR sensors. The real-time GMTI Analysts applied the FMV data to the other analyst's production effort. The SIGINT Analyst provided AIs which contained communication external hits and cross-cued the data with existing GMTI and imagery.

At this point, the GEOINT section fused the forensic and real-time GMTI, national imagery, geospatial data, SIGINT, and HUMINT data. Once the initial fusion of data was completed, the individual analysts wrote their assessments based upon the visual or textual depictions of activity. This analysis is embedded onto each slide of the drilldown product in order to provide the requestor a multi-intelligence, analyzed GEOINT product.

The drilldown product used hyperlinks to jump to various parts of the graphic presentation. The product provided points of interest; the receiving unit further cross-cued the points of interest with the unit's FMV asset and passed those to the DBE for action. The DBE repositioned forces in this area resulting in the eventual decrease of illicit activity.

Hardware

The GEOINT section uses a variety of organic MTOE and COTS equipment to perform its mission. The POR CGS, DTES, IWS, and several COTS desktop/laptop computers are the key hardware systems the section uses for analytical production.

The CGS receives real-time GMTI primarily through the Surveillance and Control Data Link antenna with a secondary means via its resident Data Forwarding capability. The CGS is also linked to other CGS systems in theater via SIPRNet and can pull/push GMTI via those systems as well as maintain communications via Internet Relay Chat (mIRC). While it primarily receives GMTI, it is also able to receive, manipulate, display, store, and disseminate FMV, SIGINT, and broadcast intelligence and secondary imagery from tactical, theater, and national systems.

The DTES allows access to various types of imagery and includes backup imagery analysis software. The DTES collects and exploits SIGINT and IMINT data (to include FMV imagery) via the Global Broadcast Service (GBS). The system also contains software to receive, record, and analyze FMV pulled via the GBS. The DTES provides the singular ability to provide analysis on Electronic Intelligence. Also, the DTES allows both Secret and Top Secret data mining; providing additional Top Secret information for GEOINT products as applicable. The DTES GBS provides a robust imagery conduit and frees up SIPRNet bandwidth on the main SIPRNet backbone for the headquarters. Additionally, the DTES Imagery Product Library provides two terabytes of local storage available via File Transfer Protocol (FTP).

Next, the section's two POR MaxPac X Class 8230XRA2 IWS high-end workstations use RemoteView software that allows imagery analysis and provides product creation tools and virtual flythrough capabilities. The IWS platforms have a dual-processor/dual-core quad CPU which is ideal for intense graphics work and possess a large storage capability.

Finally, the four high-end COTS desktops–two Dell XPS 720 and two Hewlett Packard xw8400 systems–and three COTS laptops (Dell Latitude D830) are the workhorses for GEOINT production. These systems possess high speed processors (the desktops have dual processors), dual video cards, and large size random access memory capability (4GB each) to handle multiple large sized imagery, FMV, and GI&S products. The systems are loaded with various software applications such as SOCET GXP, mIRC, and ISRF. The four desktops are linked to other GEOINT computers via a SIPR Intranet which allows for the FTP of shape files to include Forensic and Real-Time GMTI.

Software

Forensic GMTI Analysts use MITRE Corporation's freeware ISRF tool for analysis visualization that supports forensics data exploitation. The ISRF tool is one of the most highly used tools in the section due to its robust capabilities. The software can view a variety of imagery and mapping formats, such as JPEG 2000 imagery from stitched one meter CIB and CADRG. The ISRF software can use Web Mapping Service feeds as its map background, can ingest ESRI shape files, and can play NATO-EX and 4607 mission files. The ISRF tool is also used as the host for Transfusion Query Tool and can import text reporting (IIR, SIGACT, WIT, TD, M3, etc.) in the form of shape files which in turn are used to augment forensic GMTI data and analysis.

Forensic GMTI Analysts also use MITRE Corporation's Transfusion Query Tool for HUMINT and tactical reporting retrieval. This SIPRNet web-based application is a prototype data warehouse with a query and retrieval capability; it is the section's primary data mining tool. Transfusion Query Tool is used in conjunction with the ISRF tool and other tools such as Google Earth. Data such as Intelligence Information Reports (IIR), Draft Intelligence Information Reports (DIIR), Tactical Debriefings (TD), and M3 reporting are ingested into

the ISRF Tool via shape files. The information is displayed as an individual icon which an analyst can select to read the textual report. While Transfusion Query Tool is the primary data mining tool, the Forensic GMTI Analysts also use Geo Browser, Query Tree, Intellipedia, and SIPRNet Intelink.

Imagery Analysts use BAE Systems' SOCET GXP Classified IA Advanced Bundle as the primary Imagery Analysis software. SOCET GXP can view multiple types of imagery (national, commercial, BuckEye, etc.) and manipulate, display, annotate, and export data in industry standard formats. SOCET GXP is capable of importing and exporting shape files compatible with the ISRF Tool. This allows the overlaying of forensic GMTI shape files over national imagery. SOCET GXP interacts with Google Earth and ArcGIS which greatly improves the section's production capabilities.

Training

The most important component of the GEOINT section are its Soldiers; the hardware and software are simply tools. A key component was the starting objective to produce multi-discipline GEOINT products which drove the focus for the GEOINT Soldiers' training. All GEOINT analysts are cross-trained in each other's MOSs. Additionally, the analysts understand and are able to apply HUMINT, MASINT, OSINT, tactical reporting, and operational terms to their analysis. In theater, they maintain situational awareness of the intelligence and OE and maintain a habitual relationship with the BCTs for greater situational awareness. The analysts are also trained on enemy techniques, terrain, and possess varying levels of knowledge regarding ISR asset capabilities. The analysts developed excellent working relationships with the G2 ACE All Source, Targeting, Collection Management, SIGINT, G2X, and G2 Operations sections. These sections are excellent resources for GEOINT analysts and the interaction promotes cross talk and sharing of intelligence data. This cross talk with other sections forced the 35G/H/N Soldiers to become familiar outside of their MOS, understand operations, and comprehend what these other sections do and produce. The end results are GEOINT Soldiers who are very familiar and comfortable with all intelligence disciplines as well as the battlespace.

Our unit pre-deployment training spanned a ten month period. The first four months consisted of getting buy-in and support for the GEOINT concept; hard wiring the CGSs to allow GMTI feed from the external CGSs via SIPR to the GEOINT office area located inside the Sensitive Compartmented Information Facility; coordinating for the IWS and COTS hardware; purchasing the SOCET GXP software; using the Transfusion Query Tool; sending select Soldiers to the TES Analyst (T6) Course; receiving three days of SOCET GXP training from BAE Systems, and working relationships and responsibilities with other G2 ACE sections, particularly the SIGINT section. Available Soldiers were trained on GEOINT concepts and analysis on both legacy and new systems as they became available.

The next three months consisted of a DTES upgrade (with little impact to training since we could access the same products off of the Fort Drum fiber optic network); sending four Soldiers to the DTES software upgrade site to receive training; receiving a week long ISR Forensics software training by MITRE Corporation at Fort Drum; conducting a week long MaxVision IWS New Equipment Training/ New Equipment Fielding; coordinating with several external agencies such as NASIC, and sending our one 35N to DEPL 2000 (Geospatial Analysis for Deployers) with other G2 ACE SIGINT Soldiers.

The last three months focused on team training (since all hardware and software items were present and running and roughly 80 percent of the section's personnel had arrived); DTES upgrade training (GBS, Multimedia Analysis and Archive System, and Moving Target Information Exploitation), and deployment preparation. All equipment and approximately 50 percent of the GEOINT section arrived in theater via Strategic Air as a GEOINT package.

Way Ahead

JSTARS/GMTI analysis is very valuable and truly drives future operations in the full spectrum combat environment. While not discussed previously, there is a need for more GMTI collection, whether through more E-8 JSTARS airplanes or other assets. This is one area where there is a shortage of collection in theater today. There is also a need for more research and development in GMTI for better technological advancements. One possible option may be to improve the AN/APY-7 radar to increase its 120 degree field of view in the GMTI mode and expand day-time collection capabilities. Directly related to this is a recommendation to improve the

AN/APY-7 radar to pick up stationary objects in the GMTI mode as well as improve its ability to detect helicopters, rotating antennas, and low (and slow) moving fixed wing aircraft.

As of this writing, there is no formal GEOINT training. The MOS 35G and 35H courses provide some systems training and the GEOINT Foundry course provides training on geospatial data. However, there is no formal course designed to teach all GEOINT facets including the fusion of multi-disciplined intelligence into a GEOINT product. A model could be the one employed by the 10th Mountain Division (LI) and tailored to a shortened time frame and/or conducted in phases where a unit accomplishes certain training objectives at home station or other temporary duty locations before attending the GEOINT Foundry course.

A GEOINT Foundry site, with geographic areas of responsibility, is the answer. Our recommendation is to create GEOINT Project Foundry sites in the existing SIGINT Foundry Sites to provide this GEOINT training. What is needed is a centralized location for Soldiers to train on GEOINT with the right equipment, software applications, and experienced instructors. NGA is already heading in this direction by embedding a Geospatial Technician at the division. However, this Geospatial Technician will work in the MTOE Imagery Section with a single source focus.

We recommend that the U.S. Army Intelligence and Security Command (INSCOM) fund and source a GEOINT element into its existing SIGINT Foundry sites. The aforementioned 10th Mountain Division (LI) GEOINT Cell hardware and software provide a good guide to source these GEOINT Cells. In addition to the NGA Geospatial Technician, an instructor with a strong GEOINT background or at least solid and recent GMTI experience should be hired to complement the NGA Geospatial Technician. This, of course, would necessitate an agreement between NGA and INSCOM on the use of the NGA Geospatial Technician as part of the GEOINT Foundry element. Any GMTI instructor would have to be familiar with the multi-disciplined approach to GEOINT as well as be knowledgeable on the hardware and software applications that INSCOM would source. Depending on the size of the GEOINT Foundry site, more personnel could be hired. The SIGINT portion of the instruction could be handled by the existing SIGINT Foundry cadre based on guidance from the GEOINT Foundry cadre.

Endnotes

1. CW4 Thomas R. Dostie, "USAIC&FH Geospatial Intelligence Enterprise Initiatives," *Military Intelligence Professional Bulletin*, January-March 2006 at https://icon.army.mil.

2. National Geospatial-Intelligence Agency, *Geospatial Intelligence (GEOINT) Basic Doctrine Publication 1*, September 2006, 5 at http://www.nga.mil/NGASiteContent/StaticFiles/OCR/geopub1.pdf.

3. Dostie, "USAIC&FH Geospatial Intelligence Enterprise Initiatives."

4. NGA, *Geospatial Intelligence (GEOINT) Basic Doctrine Publication 1*, 10.

5. The section never achieved full strength and lost Soldiers during deployment for various reasons.

Master Sergeant Michael S. Cromer is currently the GEOINT OIC for the G2 ACE, 10th Mountain Division (LI) supporting Operation Iraqi Freedom (OIF) VI and the creator of the division's GEOINT section. He is a graduate of the Advanced Noncommissioned Officer's Course, Advanced Field Artillery Targeting Data System Course, and the Battle Staff Course. He has an AAS from Cochise College and is currently finishing his BA in Intelligence Studies at American Military University. His assignments include providing counter drug support from Soto Cano AB, Honduras; Hunter AAF, Georgia as an Aerial Intelligence Specialist; Camp Long, Korea as part of the Combat Support Coordination Team; Fort Huachuca, Arizona as an MOS 96H Instructor; Fort Sill, Oklahoma as a Brigade CGS NCOIC; Fort Drum, New York as the 42nd ID Division CGS Section NCOIC; and Fort Huachuca as the MOS 96H Service School Committee Chief/Senior Instructor. MSG Cromer's deployments include Operations Joint Endeavor, Uphold Democracy, Caliphan Mike, and Iraqi Freedom I and III. MSG Mike Cromer can be reached at michael.cromer@us.army.mil.

Lieutenant Colonel William G. McDonough is currently the G2 ACE Chief for the 10th Mountain Division (LI) supporting OIF VI. He has served in a variety of assignments from the platoon to corps level as an Infantry and Military Intelligence (MI) Soldier including deployments in support of Operations Hurricane Andrew, Restore Hope, Uphold Democracy, Joint Endeavor, and Enduring Freedom IV and VII. He holds a BA and MA in History from the California State University, Sacramento; an MS in Military Operational Art and Science from the Air Command and Staff College; and an MS in Airpower Arts and Science from the School of Advanced Air and Space Studies.

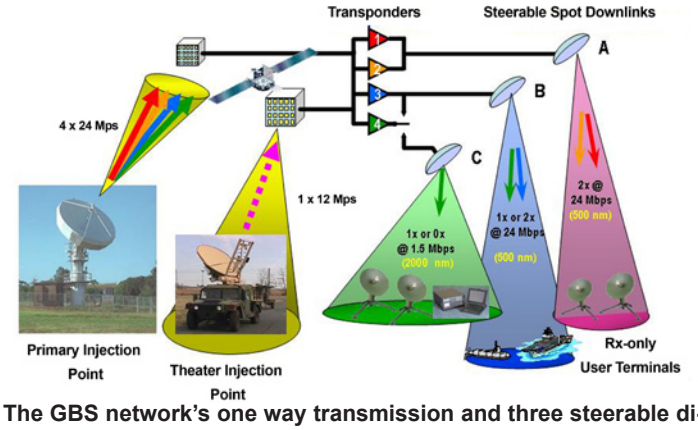
Lieutenant Colonel John A. (Jake) Conway is currently the G2 for the 10th Mountain Division (LI) supporting OIF VI. He has served for the past 20 years in a variety of artillery and MI positions to include Infantry Battalion S2 in support of Operation Uphold/Maintain Democracy and BCT S2 in support of OIF IV. He holds a BA in Pre Law from Penn State University, an MA in Management from Webster University, St. Louis, Missouri, and is a graduate of the Post-Graduate Intelligence Program, Washington D.C.

GBS: What it Is, What it Does, and Why You Should Care

by Chief Warrant Officer Three Martin Schwerzler

Introduction

Over the years the Army has faced the problem of getting large imagery files and unmanned aircraft system (UAS) full motion video (FMV) to ground commanders where it can be most relevant to time sensitive operations. The Global Broadcast Service (GBS) is the current design fielded to military units, specifically divisions, brigades, and most recently, battalions. The GBS is a very versatile open architecture system which can be located with the S6 or the S2 depending on decisions made.



The GBS network's one way transmission and three steerable directional beams.

Most units have received the GBS and only use about a quarter of its full potential; however, this is not the fault of the unit, the Soldiers, or the fielding team. Trained personnel may leave, and there is no military occupational specialty (MOS) on any unit's modified table of organization and equipment that provides for a GBS operator.

But how can you know what you are missing if you don't fully understand what a GBS is and can do?

When you look at the brochure for the GBS you find one of those cryptic all-in-one definitions:

"GBS is an extension of the Global Information Grid (GIG) that provides worldwide, high-capacity, one-way transmission of video and other IP streaming data along with imagery, web sites and other file based information."

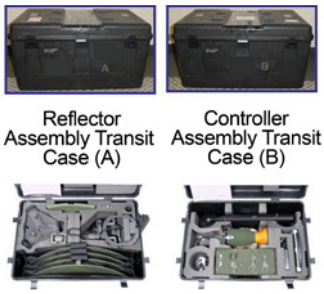
You are still left wondering, "But what does it do?"

If we rewrite this definition in a way that makes it more palatable to the average Soldier it would be something like this:

"A satellite TV receiver like system that provides news and military television stations, various UAS video channels, classified large data sets (imagery files) unclassified large data sets (maps and terrain products), and regular classified web page pulls (daily read files.)"

So, what comes in that big box?

The basic GBS that is fielded to Army units is the AN/TSR-8 which comes in three transit cases, weighs approximately 250 pounds, and costs roughly $150,000. It consists of a Next Generation Receive Terminal (NGRT) and a Receive Broadcast Manager (RBM).



Next Generation Receive Terminal.

Receive Broadcast Manager.

Dish Antenna.

The NGRT is readily recognizable to everyone as the dish antenna. The RBM is a very densely packed case with a satellite receiver, KG-250 Encryptor, two network switches, and a classified laptop, all rack mounted. In addition to the rack mounted equipment, there is one other unclassified laptop associated with the RBM which normally resides either on top or next to the transit case. All of the components have custom cut foam dividers and sections with laminated cards attached to each transit case showing a complete parts list with stowage location. For $150,000, you get a very well packed, deployable system.

Okay, if it's densely packed, how can it be such an open architecture?

While the GBS is a tightly packed system, it has a very robust and open architecture which allows it to

be configured for maximum integration into whatever organic architecture a unit has, provide the basis of a small network, or act as a stand-alone system with limited capabilities. This is accomplished in the design and by leaving the component items in a basic configuration with administrator privileges. This immediately sends most S6 shops into a state of panic as it can not be locked down, it can not be controlled, and it can not be forced into unusable submission.

In order for the GBS to work efficiently, it has to have services running that are usually denied on networks because they are considered vulnerabilities, but if it is incorporated with these considerations, it can be on the network. Another key element to this open architecture is the managed network switch which allows the unit to easily connect a variety of computers or systems together with the GBS such as a Geospatial Intelligence (GEOINT) Cell.

This raises a big question, "Where should the GBS be located within the staff organization?" As mentioned earlier, the S6 will hate integrating the GBS and most of the functionality of the GBS is a force multiplier for the S2. So for most units it should be an easy decision to place the GBS under the control of the S2 with some coordination with the S6 in order to provide video feeds to the various staff elements that require it. Ideally the GBS is the networking nexus for the GEOINT cell and has direct communication with the Imagery Workstation System (IWS), and Digital Topographic Support System (DTSS). The IWS provides the unit's MOS 35G Imagery Analyst with a powerful toolset for exploitation and production of overhead still imagery with Socet GXP; ground moving target indicator (GMTI) data with Moving Intelligence (MOVINT) client; FMV data with Insyte, and shape file production with Google Earth and FalconView–all on a compact portable workstation with dual monitors and 4 terrabytes of storage. The DTSS accepts topographic and multi-spectral imagery data from national and commercial sources to create intervisibility, mobility, environmental, and 3D terrain visualizations as well as the creation, augmentation, modification, and management of topographic data; while providing updated map background and terrain intelligence information to all Army Battle Command Systems. The reasoning for this central location is that both the IWS and the DTSS exploit very large data sets which can easily be in excess of 1 gigabyte and by isolating that traffic to a closed network, it alleviates congestion on the unit's networks (See also the article *CTC Support by the 3d MI: A Retrospective Evaluation* in this issue).

So, we've decided where it goes...now what makes it go?

It is essential that the GBS be viewed as a system in that if any component is left out you may lose a capability or potentially any capability with the GBS. Some examples are:

1. Forget the crypto and you only get unclassified video and data, *no* UAS and *no* imagery for the IWS.
2. Forget any component of the NGRT other than the coaxial cable (because it can be substituted by any coaxial cable) and you are completely nonoperational.
3. Forget the little Smartcard and you again lose all unclassified feeds.
4. Forget the classified laptop or its hard drive and you get only unclassified information.

The GBS is a very unique piece of equipment and finding substitute or interchangeable parts with other Army systems is rare. The few generic parts are: the coaxial cable; the Ethernet cable; power supplies for the laptops; the compass; stakes, and grounding equipment.

Besides the equipment it is necessary to plan for the employment of the GBS. The antenna must be located where it will be undisturbed and secure. It is a receive-only system so there isn't a radiation concern; however, its location should be coordinated with the unit's frequency manager, usually located in the S6, so that there is little or no interference from other transmitters. A clear line of site to the target satellite's location is necessary in order to ensure a solid signal. No trees, buildings, tents, generators, or other obstructions should be in the way. Running from the RBM suite to the NGRT antenna, is a 150 foot cable which allows for options when looking for a good location.

Another consideration is power, the RBM has only one electrical plug and the NGRT has one plug, but these are large amperage requirements and should not be considered the same as a normal laptop plugged into a circuit. It is not uncommon to find that the circuit that the GBS is plugged into will

overload and flip a breaker; therefore, plan your power layout accordingly or expect problems.

Finally for a good emplacement you must have a good ground. This is sensitive equipment with components that are exposed to the elements and a poor ground can either injure a Soldier or possibly cause damage to the equipment.

The best way to keep a GBS working is to use it, use it, use it.

It may sound trivial or trite, but the more Soldiers use a GBS in conjunction with the other systems, the more proficient they become. They begin to notice when things start running slow and they need to perform basic maintenance on the file systems by deleting old files and keeping the database clean. They identify how to connect different systems and handle different data types which are provided by the GBS. They have an opportunity to download relevant imagery in a timely fashion for real-world production requirements in garrison. They can build data sets in preparation for deployment. They can begin to explore the extra capabilities of the GBS which most units never get to such as the regular updates of active web pages hosted throughout the Intelligence Community and providing that information to the rest of the staff.

Ultimately, if the GBS is up, operational and in use, then you know it works and your Soldiers know how to set it up. Practice teardown and setup on a monthly or at least a quarterly basis to ensure those skills stay strong. Soldiers will surprise themselves at how fast they can get from in-the-box to operational with practice.

I know what I am doing...why is it still not working?!?

The GBS is a very reliable system and the software has been improved over the years to a point that it also is very reliable, so when it does not work, 95 percent of the time it is because the operator has overlooked or failed to check something simple. The first step to correcting a problem during setup is to stop, return to the beginning, and start over. Sometimes it requires having another operator come in and double check or do the setup independently. Examples of simple mistakes that I have seen when Soldiers are having problems are:

- The antennae is pointed 180° off.
- The frequency in the IRD is incorrectly set because it was not saved before power-down.
- The cables are connected backwards between the NGRT and the RBM.
- Wrong (or worse) no crypto.
- The feedhorn offset is incorrectly set on the antenna.
- The Smartcard is not inserted or is not being read by the Integrated Receiver Decoder (IRD).
- The SECRET laptop is not plugged into the switch.
- One of the several connections is not correct.

When you have stopped, regrouped, and retried each step multiple times then, and only then, do you stand a chance of calling the Helpdesk and not having them make you feel stupid for not noticing that a decimal was out of place or you swapped the W1 with the W2 cable. Seriously though, when all else fails the GBS Helpdesk is always there, helpful, and extremely knowledgeable on the intricacies of the GBS Suite, and they are more than happy to assist. You can not help but notice as you unpack a GBS for the first time that they plaster the GBS Helpdesk phone number all over the system and the cases, so when all else fails... call the Helpdesk.

Additional Resources

https://www.tec.army.smil.mil

http://gbs-norfolk.navy.smil.mil

Norfolk Helpdesk (Comm) (757) 444-9190, (DSN) (312) 564-8993

Hawaii Helpdesk (Comm) (808) 653-5050, (DSN) (315) 453-5050

Chief Warrant Officer 3 Martin Schwerzler is currently assigned to 3d MI Center, NGIC in the GEOINT Sustainment Branch as JRTC MTT Chief. His previous assignments include 3d Infantry Division, 101st ABN DIV (AASLT), and V Corps G2 working in various intelligence sections culminating as the Collection and Requirements Manager during OIF 3 and 5 for the 3ID. He instructed at Fort Huachuca, Arizona for the MOS 96H CGS Operators Course. CW3 Schwerzler has an Associates degree from Cochise College and will complete his Bachelor's degree this summer with Excelsior College. He has published numerous articles in this and other professional publications and was named the Writer of the Year for MIPB in 1999. He can be contacted at martin.schwerzler@us.army.mil.

CTC Support by the 3d MI Center: A Retrospective Evaluation

by Chief Warrant Officer Three Martin Schwerzler

Where We Were a Year Ago for Support

Approximately a year ago the 3d MI Center revamped the support they were providing to rotational units and the combat training centers (CTCs) under the Geospatial Intelligence (GEOINT) Foundry Program. As the proponent for the oversight of Foundry, the U.S. Army Intelligence and Security Command (INSCOM) established the 3d MI as the lead for all GEOINT support in accordance with the Army Force Generation (ARFORGEN) concept. (See Figure 1)

The Plan to Support a Unit from Pre-deployment to CTC Rotation

Our current model for support begins with the early engagement of the leadership of a brigade, through a Mobile Training Team for Leaders (MTT-L), that is identified on the patch chart as deploying to either Operations Enduring Freedom or Iraqi Freedom. We prefer to make this contact between six and nine months out to ensure the leadership fully understands the training available to their unit analysts either through an MTT or at our GEOINT Sustainment Training Facility (GSTF) at the Washington Navy Yard. Currently the MTT-L is conducted by the senior leadership of the 3d MI Sustainment Branch; however we are transitioning to a plan whereby all engagements with a brigade will be conducted by members of the same team that is scheduled to support them during their CTC rotation.

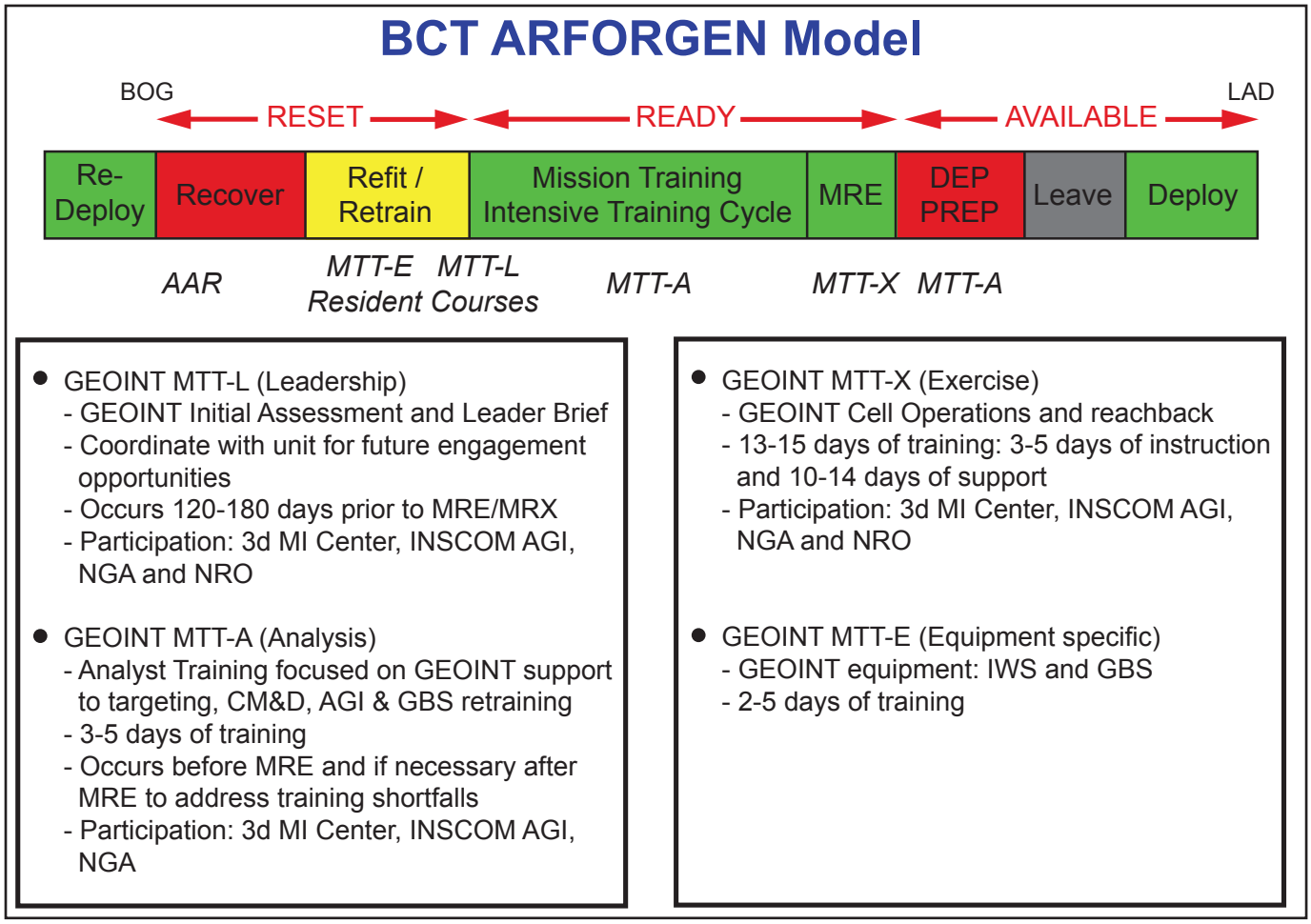


Figure 1. Alignment of GEOINT Foundry engagements as they correspond to the ARFORGEN Cycle.

By establishing this continuity, we hope to build a rapport with the brigade staff and analysts early in the train-up period so we can help identify training gaps, equipment issues, and relay relevant changes to procedures, equipment, or techniques. We recommend that senior section representatives attend the MTT-L that can address specific objectives and levels of proficiency for Imagery Analysts, Common Ground Station (CGS) Analysts, and Geospatial Analysts. Additionally, we can help track progress of training objectives identified at the MTT-L by the brigade leaders and monitor individual Soldiers by name up to deployment as they attend various Foundry training opportunities.

The second step of this process is the MTT for Analysts (MTT-A). This engagement is targeted to the analyst. We bring representatives from the various agencies who have expertise in their respective GEOINT sub-discipline per the training gaps identified by the brigade leaders at the MTT-L to the unit for hands on training. We can cover operations with the Global Broadcast Service (GBS), Imagery WorkStation (IWS), and Digital Topographic Support System (DTSS). Basic requirements for this training to be effective are: equipment in good operational condition, SIPRNET connectivity, and personnel identified and isolated for training. By the end of this training, the GEOINT Cell should be ready to perform optimally at its respective CTC rotation; however, as we all know the best laid plans . . .

So What Have We Seen Over a Year?

This brings us to the main point of this article. Just what have we seen over the last year of support to the rotational training units (RTUs) at their CTC mission readiness exercise (MRX)? As we discussed earlier, 3d MI developed this plan for more consistent engagement of the unit from senior to junior levels, designed a variety of training opportunities, and a larger support system of subject matter experts to be accessible at each training opportunity. But has it made a difference and what trends do we see emerging now?

One of the most obvious problems which units probably have the least ability to impact is that of personnel. We have seen several units receive new analysts just a few months prior to their CTC rotation; consequently they have not received the benefit from the earlier GEOINT Foundry engagements or multiple training opportunities. While this will likely continue to be a problem, there are options available to mitigate the severity of its impact. As soon as your unit knows there are inbound Soldiers, it can contact 3d MI to find out if they have already received training within the last year through any of our GEOINT Foundry classes. If they have not or if they are coming straight from Advanced Individual Training, then we can attempt to schedule them for immediate attendance to prioritized applicable courses once they arrive and complete the necessary inprocessing requirements of your unit. Additionally, this training needs to be coordinated through the Foundry representative on your post.

Surprisingly, we have had several units believe that their equipment was either fully operational, complete, or believed that it would be provided by the CTC. When we notice equipment problems at an MTT-L or MTT-A, we attempt to fix the problem or get the unit in contact with the appropriate maintenance channel for correcting the deficiency, but ultimately the unit is responsible for the maintenance and operation of their equipment. Critical components for a GEOINT Cell are the IWS, GBS, CGS, and DTSS. Personally, I advocate that units have this equipment up and operational year-round because this ensures all the analysts are familiar with the equipment, software, connectivity, and maintenance requirements. While the CTC has this equipment, it is already being utilized by support personnel who are simulating echelons above brigade and supporting the CTC Operations Group requirements. Finally, crypto keys must be brought by the RTU for the equipment.

Where is that GBS?

One piece of equipment which has found its home in various places is the GBS receive suite. Most of the units we visit have it assigned and maintained by the S6 and a few have it in the S2. The actual GBS location is less important than its full implementation. By this, I mean that it can perform all of its functions over a network as long as knowledgeable personnel configure and maintain it properly. Unfortunately, the tendency at the majority of units with the GBS assigned to the S6 is to view it simply as a receiver of video feeds and entirely ignore the data downlink capability which is one of the primary functions of this system.

For example, an average image to download is 1 gigabyte. Would you rather have that come over your S6 Joint Network Node which impacts the entire brigade, your Trojan Spirit which impacts your entire S2 shop, or the GBS that impacts no one? (See Figure 2) When most S6 shops are presented with this, they usually are more than happy to connect the DTSS and the IWS directly to the GBS so the traffic does not even cross their network. We teach that the GBS is an integral part of a GEOINT Cell and should be incorporated into its configuration as an organic element managed by the analysts.

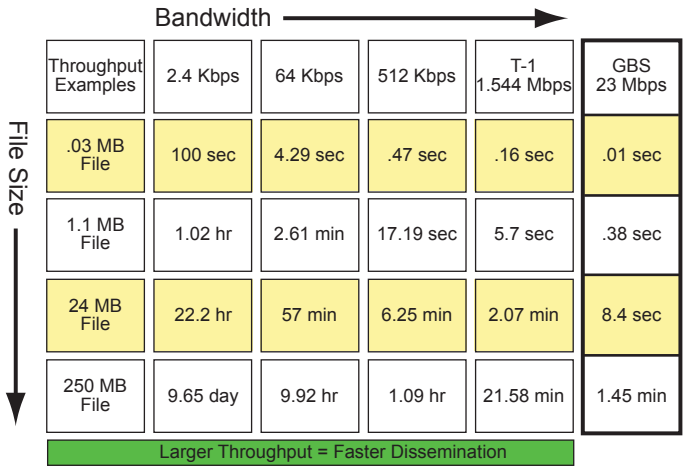


Figure 2. Bandwidth versus file size.

What is this GEOINT Cell of which You Speak?

This brings us to the next area where we regularly see a need for improvement, the GEOINT Cell. I have used the term GEOINT Cell throughout this article in an effort to emphasize its importance and how it impacts every element of GEOINT support to intelligence and the brigade. The initial concept of the GEOINT Cell has been around for a few years, and last year a formal memorandum was signed by MG Custer, Commander, U.S. Army Intelligence Center (USAIC), Fort Huachuca, Arizona, reiterating the configuration.

As the GEOINT community has developed more capabilities and software, we have seen an overlapping of capabilities and a benefit from terrain, imagery, and CGS analysts being located together to encourage collaboration and efficient division of work on requests for information (RFIs), intelligence problems, and mission planning. All too often, if these sections are separated there will usually be a duplication of effort because you will have the same RFI being worked on by two sections at the same time. Or when an RFI is given to one section, other disciplines under GEOINT who may have part of the solution will not be considered when answering the question/problem.

With a GEOINT Cell, you consolidate your RFI management for all GEOINT related products rather than Terrain being managed by the S3 and Imagery being managed by the S2. It also places all products for consideration in the Military Decision Making Process under the observation of the S2 making standardization and completeness easier to accomplish rather than having them under two different staff elements.

Although it makes all the sense in the world, and emphasis has been placed on this concept from USAIC, we still see units arriving at a CTC in the legacy configuration of the terrain element separate and under the S3 and the CGS analyst outside the fusion section in vehicles. We usually spend the first few days convincing the brigade staff of the benefits of the new configuration which simply takes away from time that could be better spent on smoothing out other internal processes within the fusion and GEOINT sections.

That brings us to the final observation we see as a trend with RTUs at the CTC: A lack of established procedures prior to arriving at the CTC. Ideally every unit has an established set of standard operating procedures (SOP) on which it can base its operations, but with the fluidity of personnel in Army units today, maintaining continuity is a major problem and institutional knowledge tends to stay in the mind rather than being committed to paper. If units come to their MRX with at least personnel identified for each position, a job description, and a 24/7 coverage plan for each; they will be ahead of the game and the procedure can be easily massaged into tactics, techniques, and procedures (TTPs) and codified into an SOP during the command post exercise portion of the MRX.

Some basic questions which the RTU S2 shop should be able to answer before they arrive are:

- Who is the RFI manager?
- Who is the Collection Manager?
- How are you synchronizing your intelligence, surveillance, and reconnaissance?
- How are you planning to distribute products?
- Who is directing, watching, and reporting on the unmanned aerial system?

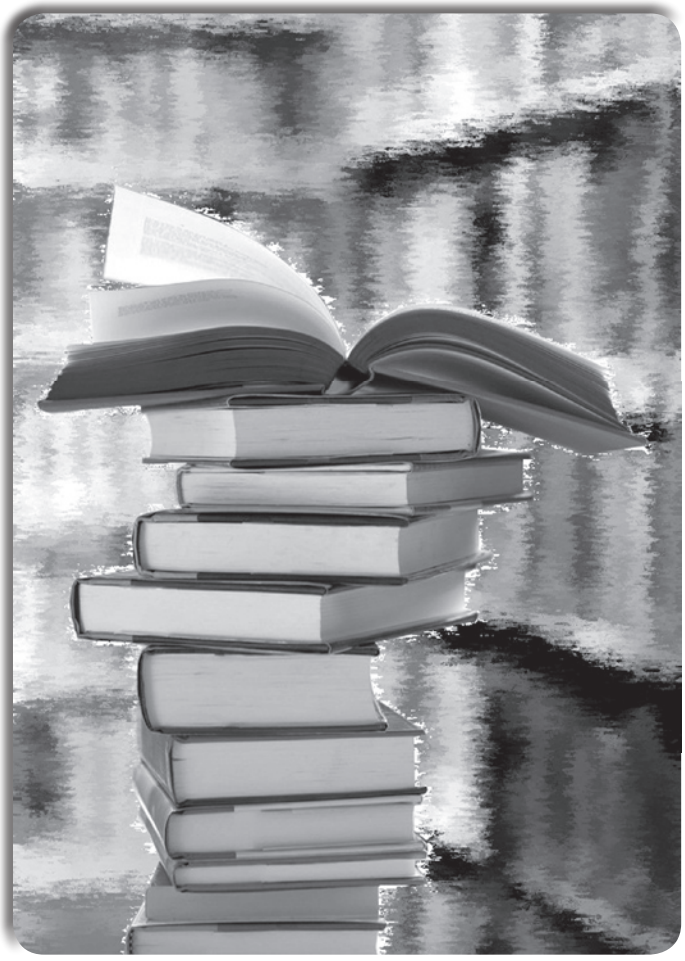
And a few simple things done before arriving at a CTC can set you on the road to success:

- Get training ahead of time, don't wait to get trained at your MRX.
- Pre-combat inspections.
- Does your architecture make sense, where is your GBS?
- Consider the flow of information and RFIs. Keep in mind the Who, What, When, Where, Why, and How?
- Develop a plan which you can modify at the CTC if you don't already have TTPs and SOPs laid out.

Conclusion

The purpose of this article was to let the Intelligence Community as a whole, and brigade S2 shops in particular, know what GEOINT Foundry MTT personnel have seen over the last year and where we think the most frequent problems exist. Our intent is to inform and give suggestions for units to consider to improve processes within their sections; thereby providing them a better foundation before they arrive at their MRX and are expected to be able to perform their mission at combat speed and efficiency. For leaders, this seems simple; however, do not underestimate or overestimate your personnel's understanding of your answers to these questions. I hope this information proves useful to your unit before its next MRX but more importantly before you deploy.

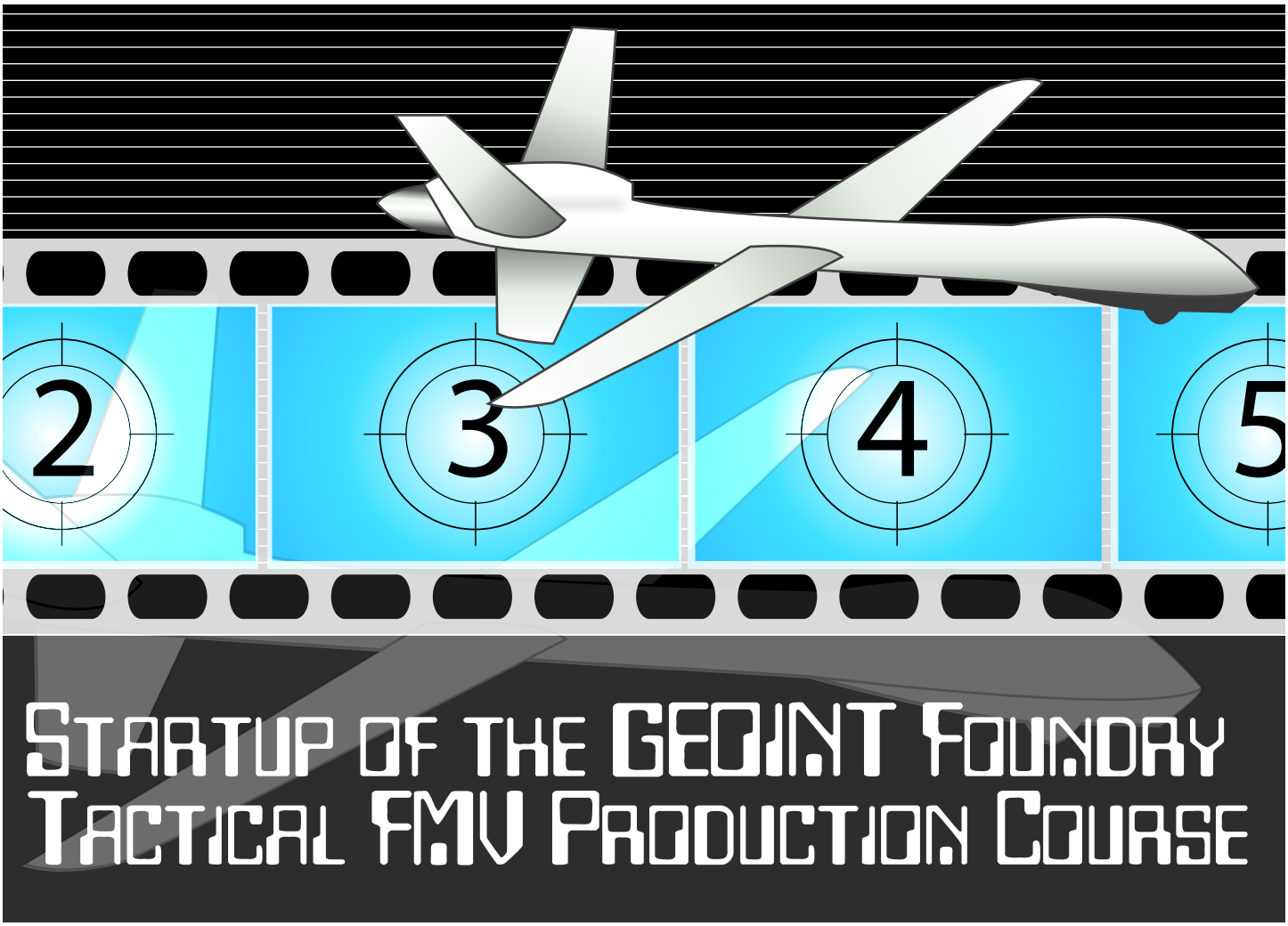
Chief Warrant Officer Three Martin Schwerzler is currently assigned to 3d MI Center, NGIC, in the GEOINT Sustainment Branch as JRTC MTT Chief. His previous assignments include 3d Infantry Division, 101st ABN DIV (AASLT), and V Corps G2 working in various intelligence sections culminating as the Collection and Requirements Manager during OIF 3 and 5 for 3ID. He instructed at Fort Huachuca, Arizona for the MOS 96H CGS Operators Course. CW3 Schwerzler has an associates degree from Cochise College and will complete his Bachelors degree this summer with Excelsior College. He has published numerous articles in this and other professional publications and was named the Writer of the Year for MIPB in 1999. He can be contacted at martin.schwerzler@us.army.mil.



Read any good books lately?

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

Email your book reviews along with your contact information to sterilla.smith@conus.army.mil.



Startup of the GEOINT Foundry Tactical FMV Production Course

by James T. Cummins

U.S. Army 3d brigade combat teams' (BCT) S2/ Intelligence Cells are now deploying to missions with Imagery Analysts (MOS 35G); Imagery Workstation Systems (IWS); and Shadow RQ-7 equipped Tactical Unmanned Aircraft Systems (TUAS) platoons. The IWS has full motion video (FMV) data exploitation capabilities and the BCTs' Imagery Analysts are being tasked with providing Motion Imagery processing, exploitation, and dissemination (PED) support in conjunction with traditional Imagery Intelligence (IMINT) products.

While fielding the IWS and supporting BCTs during combat training center deployment preparation rotations, the National Ground Intelligence Center (NGIC) 3d Military Intelligence (MI) Center's Foundry contact teams noted that the S2 Imagery Analysts had little or no FMV training/experience prior to their combat deployments. Based on this information and having the mission to prepare Army Intelligence Soldiers for their deployments the 3d MI Center initiated and developed the Tactical FMV Production Course within the U.S. Army Security and Intelligence Command's (INSCOM) Foundry curricula to satisfy this important requirement.

The Tactical FMV Production Course (Course Number GI-083) is designed to prepare and train analysts, FMV team members, and unit decision makers assigned to deploying Army BCTs and throughout the Intelligence Community to maximize FMV exploitation for mission success. FMV data and applications gleaned primarily from TUAS along with other area of responsibility (AOR) intelligence, surveillance, and reconnaissance platforms/methods will be utilized to solve counterinsurgency (COIN) intelligence challenges within a geospatial context. This newly es-

tablished course will enable students to generate tactical products utilizing the newly fielded IWS FMV exploitation software suite. The five day FMV course will provide Soldiers with a tactical applications approach for FMV data analysis and ready their participation in the UAS/FMV mission operational cycle. Ultimately, the course will facilitate the integration of FMV real time information stream with other Theater data sources to enhance the BCT's ability to identify targets and trends; discern and discriminate threat activities; identify cultural infrastructure; patterns-of-life analysis, and exploit other sensor-unique signatures either during in-flight operations or post-mission production.

This Geospatial Intelligence (GEOINT) Foundry course was developed and implemented to train deploying FMV imagery analysts to do what their job title implies (to "analyze" imagery in motion.) Specifically, it means more than just developing an ability to identify equipment or run software. It uniquely means developing an FMV analyst's ability to "rapidly understand the meaning of what they are observing through the UAS sensors" so they can provide timely and accurate direct PED support during ongoing live combat operations. For this reason, roughly half of the course's training materials incorporate video clips of actual Operations Enduring Freedom/ Iraqi Freedom FMV missions. These missions can range from attempting improvised explosive device detection; route reconnaissance; convoy security overwatch; AOR persons, weapons, vehicles, and equipment recognition; area search/ surveillance; building and facility identification through pattern-of-life analysis, and more.

The remainder of the tactical FMV training develops the supporting range of skills/tasks that will enable/enhance FMV PED operational support such as, learning FMV acronyms, terms, and brevity code; using proper chat/communication etiquette; providing accurate coordinates; producing timely, legible graphics, and applying appropriate report writing/briefing methods. The hands-on/eyes-on and practical exercise training methods and materials are kept simple and focused to enable the FMV analyst to develop speed and accuracy while supporting COIN/irregular warfare operations. The end of course CAPSTONE exercise allows the students to apply and demonstrate their grasp of FMV tactical applications.

In fiscal year 2010, the 3d MI Center intends to implement an additional, tack-on week of FMV intelligence exploitation training to the original course, concentrating on enhancing the analysts' mission planning and intelligence production skills prior to their deployments. This second week of the course will emphasize and mimic the Soldiers' future FMV crew roles in mission planning; target folder development; COIN applications; and detailed Motion Imagery product development. Although the targeted audience for the second week of enhanced training will be MOS 35Gs, all other Soldiers assigned as members to deploying FMV exploitation teams are certainly encouraged to attend.

Another important aspect of this BCT FMV team oriented course is the continued familiarization of the FMV analysts on the IWS with its robust capabilities and software suite specifically tailored for FMV exploitation and other IMINT applications. NGIC's 3d MI Center has recently wrapped up an IWS fielding project that entailed contact teams delivering systems and initial operator training to BCT S2 elements scheduled for deployments. The IWS was designed as a small, portable, scalable, and environmentally ruggedized suite of hardware and software primarily for the BCT S2 elements with tactical FMV/IMINT forward fielded exploitation missions. These IMINT focused systems enable the assigned BCT intelligence personnel to produce relevant and immediate support to combat planning and operations. The IWS consists of a Windows-based personal computer platform and is designed for SIPR networking using both local and reachback functionality. It enables exploitation of FMV direct feed; National Technical Means; standard geospatial information; Theater imagery input, and moving target indicator data. Packaging available COTS/GOTS technology, the IWS was quickly developed and issued to fill the void until a sufficient mobile imagery capability is fielded with the Distributed Common Ground System–Army for BCTs across the force.

The 3d MI Center's mission is to conduct GEOINT operations in support of Army, Joint and Coalition

full-spectrum operations and contingency planning, and provide GEOINT sustainment training to the Army under INSCOM Foundry. This includes the following training and production tasks:

- Conduct IWS fielding and new equipment training in coordination with Army Space Program Office.
- Provide GEOINT mobile training teams in support of deploying BCTs.
- Conduct GEOINT training courses at Foundry Multi-Discipline Platforms located at Corps/ Division posts.
- Operate the GEOINT Sustainment Training Facility (GSTF), Washington Navy Yard.
- Support Corps and Division exercises.
- Provide federated GEOINT production support.
- Produce GEOINT in support of deployed forces' requests for information.

The 3d MI Center intends continued efforts for the expansion, improvement, and enhancement of its responsive support to the Warfighter's GEOINT training and operational needs.

The first standard Tactical FMV Production Course was conducted 27 April to 1 May 2009 at the 3d MI Center's GSTF located within the National Geospatial-Intelligence Agency's (NGA) Washington Navy Yard-Building 213, Washington, D.C. The class was the result of a crash course development process that included a "murder board" evaluation of course content by 3d MI Center veteran FMV analysts and a shakedown pilot course in March with seven students of various backgrounds and FMV experience. Feedback from deploying Soldiers in the first standard class has been encouraging and, along with the excellent advice received from the experienced FMV Soldiers, enabled 3d MI Center training cadre to focus class materials and objectives on the real world requirements and applications the course's targeted audience will need to meet during their deployments.

Those Soldiers assigned as FMV exploitation team members in deploying BCTs desiring Tactical FMV Production Course slots are encouraged to contact their installation's Foundry Manager or the 3d MI Center's GSTF staff at the Washington Navy Yard at Commercial (202) 284-4600, DSN 484-4600 or via email: WNY_GSTF@mi.army.mil.

Jim Cummins is currently a courseware development contractor for the 3d MI Center's GSTF at NGIC's GEOINT Support Office located within NGA's Bldg. 213, Washington Navy Yard. Prior to his October 2008 start in Project Foundry, Mr. Cummins had supported NIMA/ NGA deployment and exercise operations since 9/11. His long service and mission commitment began as an Infantryman (Vietnam, 1968) and continued through retirement as a Terrain Analysis Warrant Officer in 1999. He can be reached at DSN 484-4732, commercial (202) 284-4732, James.Cummins@mi.army.mil.

Shadow UAS Tactics and the Communications Relay Package

by Captain Priscella Nohle

In 2006 the Shadow 200 (RQ7B) Tactical Unmanned Aviation System (TUAS) was reflagged under Aviation, effectively removing the system from the Military Intelligence (MI) umbrella.[1] As the system struggles to find its place in the ever restructuring Army, the MI community tasks this asset and holds the keys to its success and failure on the battlefield. Integration of new capabilities, particularly the communications relay package (CRP), makes this system invaluable to combat commanders during maneuver operations. MI officers, specifically, have a responsibility to maintain consistent communications with maneuver commanders to create new tactics, techniques, and procedures (TTPs) for the ever growing assets of the MI community.

The CRP for the Shadow system was fielded for the first time in 2007 with mass distribution in theater in 2008.[2] This system enabled a UAS at the brigade combat team (BCT) level to simultaneously observe *and* communicate with maneuver units in urban, mountainous, or otherwise unreachable terrain. The CRP eliminated the line of sight issues associated with ground communications as well as the reliance on higher level UAS assets for this type of relay that are not organic to the BCT. However, with this new capability came misunderstanding and was met with indifference by units due to lack of TTPs and collaboration.

There are several factors that produced the indifference toward the Shadow's CRP function, the first of which was lack of guidance. When the system was fielded by AAI Corporation, the contracting company for all Shadow systems, the consensus was that the CRP would be used for extending communications in place of a retransmission station with the benefit being that it would not have to be manned. Retransmission stations are used for long term communications that last more than the average Shadow flight time. This inaccurately made the CRP seem not applicable to the current fights in Afghanistan and Iraq. Utilization of a Shadow to fly 24/7 in all weather conditions to keep lines of communication open is not a feasible use of the Shadow system. The question remained: How do we use this new gadget effectively? Being newly fielded technology, there was not a lot of information from adjacent units as to how they were implementing the CRP. TTPs needed to be developed by leaders in the field to maximize the impact of the new technology on the current fight. Contractors are experts in technical support, not tactics. It is our responsibility to employ our equipment effectively on the battlefield.

Another contribution to disinterest and lack of use was the absence of collaboration between MI staff and maneuver units regarding the new capability. Maneuver commanders could easily have developed TTPs that enabled the CRP to truly be an invaluable resource, but the communication in some units never materialized. In other units where there actually was collaboration to develop TTPs and effective use of the system, operations implementing the system proved successful. The 4th Brigade, 3rd Infantry Division standardized their use of the CRP by "having a frequency loaded in their Shadow every time they launched" according to SFC Baker of 3rd Brigade, 101st Airborne Division who served as the NCOIC of the launch and recovery site at FOB Kalsu during 2008.[3] According to SFC Baker, the 4th Brigade was the only unit of the four supported Shadow UAS platoons that consistently loaded a frequency in the CRPs. This TTP enabled the unit to communicate with units on the ground wherever the Shadow was located.

UAS Training

Increased training opportunities could have a positive impact on asset usage in theater. A contributing aspect to the lack of training is that the CRP is currently only being fielded in theater and it is con-

sidered theater property book equipment, meaning it stays in Iraq/Afghanistan. Systems are not being fielded to units stateside including the UAS training facility at Fort Huachuca, Arizona where advanced individual training (AIT) is received. Soldiers and units cannot train with the CRP during AIT, at the Joint Readiness Training Center, or at their home stations prior to stepping into combat. This is not as detrimental to the Shadow operators themselves as it is to the maneuver units who are practicing utilization of all of their assets during these training phases.

Having the CRP asset on the Shadow system can create multiple issues if TTPs are not established. This ability can cause units to request the asset for more maneuver functions, pulling usage away from the traditional observation missions of intelligence gathering. The CRP could also entice the BCT commander to play platoon leader by communicating directly with troops on the ground. While the ability to directly communicate with troops on the ground is desired, and sometimes crucial, it can be abused.

Units who are not already effectively using the CRP on their Shadow UAS should consider establishing a similar frequency loaded for each mission. Since the UAS can be dynamically re-tasked between battalions, the brigade frequency or a separate frequency purely for Shadow operations should be utilized for every mission. This is best for three reasons: simplicity from the higher command's perspective, familiarity from the ground unit, as well as being easily loaded by the Shadow maintainer. Having a different frequency for each mission complicates the process on all ends and can waste valuable time if a critical situation unfolds.

While the Shadow platoon is task organized in the MI company (MICO) of the Special Troops Battalion of the BCT, the platoon is beginning to see the effects of its new alignment with Aviation. This includes MOS identifiers being aligned with Aviation and the annual Aviation Resource Management Survey inspections which are designed for an Aviation unit, not a platoon in a BCT. It is apparent that a change is in the works to possibly move the platoon to be task organized in an Aviation unit rather than the MICO. According to Tim Hodges, the UAS Program Manager for Fort Huachuca, it is possible that with the creation, fielding, and establishment of the Extended-Range Multi-Purpose UAS in 2010 that the birth of a purely UAS unit may be established housing multiple platforms to include the Shadow system. However, by standardizing the maintenance, training, and supply with this change, it also effectively eliminates the platoon as an organic asset within the BCT, in turn negating the BCT concept.

With these possible changes in mind, the BCT's further consideration should be given to the function of the Shadow system given this added advantage. Since the asset has been used historically for intelligence gathering, and knowing that the new package can influence communications coverage of the battlefield, how does the BCT rectify priorities of the Shadow system? Does the intelligence staff find it appealing to downplay the CRP because it diverts the focus from their collection mission? Since the asset is in the process of possibly moving to Aviation; has the MI supervisor written them off? Answering these questions may determine if the Shadow platoon remains in the BCT or finds a new home in an Aviation unit.

Conclusion

In closing, the Shadow system CRP has the potential to give tactical maneuver units unprecedented situational awareness and dynamically extended communications on the battlefield. It is, at this time, the charge of MI officers and noncommissioned officers to ensure this asset is not only used properly but to its fullest potential in combat operations. While our priority is intelligence collection, our assets are dynamic and can be utilized to give our fighting forces the edge necessary to win battles now and in the future.

Endnotes

1. Tim Hodges, UAS Program Manager, Fort Huachuca, Arizona, Interview 3 June 2009.

2. Harris, "*Drone Relay: PRC-152 Radios + RQ-7 UAVs = Front-Line Bandwidth,*" 25 February 2009, accessed 10 June 2009 from Defense Industry Daily at http://www.defenseindustrydaily.com/Drone-Relay-PRC-152-Radios-RQ-7-UAVs-Front-Line-Bandwidth-04753/.

3. S. Q. Baker, 1SG B/3STB/3BCT, Interview 5 June 2009.

Captain Priscella Nohle served as the UAS platoon leader, as well as company executive officer for the MICO, 3rd Brigade, 101st Infantry Division (AASLT) during OIF 2007-2008 in Camp Striker, Iraq. Currently she is a student in the MI Captains Career Course and will be assigned to the 1st BCT, 1st Infantry Division in Fort Riley, Kansas after completion of the course.

Targeting at the Battalion Level: What the Combat TIO Should Know

by Captain Christopher J. Christiana

Introduction

In the contemporary operating environment (COE), the single most rewarding task performed by our warfighting function is the process by which we, the U.S. Army, kill or capture our enemies. It is the most current evolution of the targeting process, often referred to interchangeably as lethal targeting or kinetic targeting, and it falls to the tactical-level intelligence officers (S2s) to facilitate this process. In March 2007, I deployed with my unit, the 2-69 Armor Battalion, as the assistant S2. I was also fortunate enough to be given the lead on this process as the Lethal Targeting Officer in Charge (OIC). I realized this was perhaps the best job in theater, as my shop put together the pieces required to bring known enemies of the U.S. Army to justice.

When thinking of the broad targeting horizon, it is useful to think of the process from a law enforcement position more so than traditional S2 tasks. You will identify the worst elements of the insurgency, track their whereabouts, and then move to apprehend them. The cycle is continuous, but each criminal taken off the street keeps the population and your unit that much safer.

As a new second lieutenant reporting to your first unit, your experience in garrison will be nothing like your experience in theater (deployed). While it is no doubt important to maintain the physical security of your arms' rooms, it is trivial compared to the responsibilities in theater, where intelligence truly does drive operations. The purpose of this article is to prepare you, the new Tactical Intelligence Officer (TIO), to lead the targeting effort.

The Targeting Methodology

Although it may seem self-explanatory, the first step to being a good Targeting OIC is to understand the doctrine and the processes. The targeting process is encapsulated in the acronym D3A (Decide, Detect, Deliver, Assess). But in the COE, a more suitable method is F3EA (Find, Fix, Finish, Exploit, Assess) (See Figure 1).

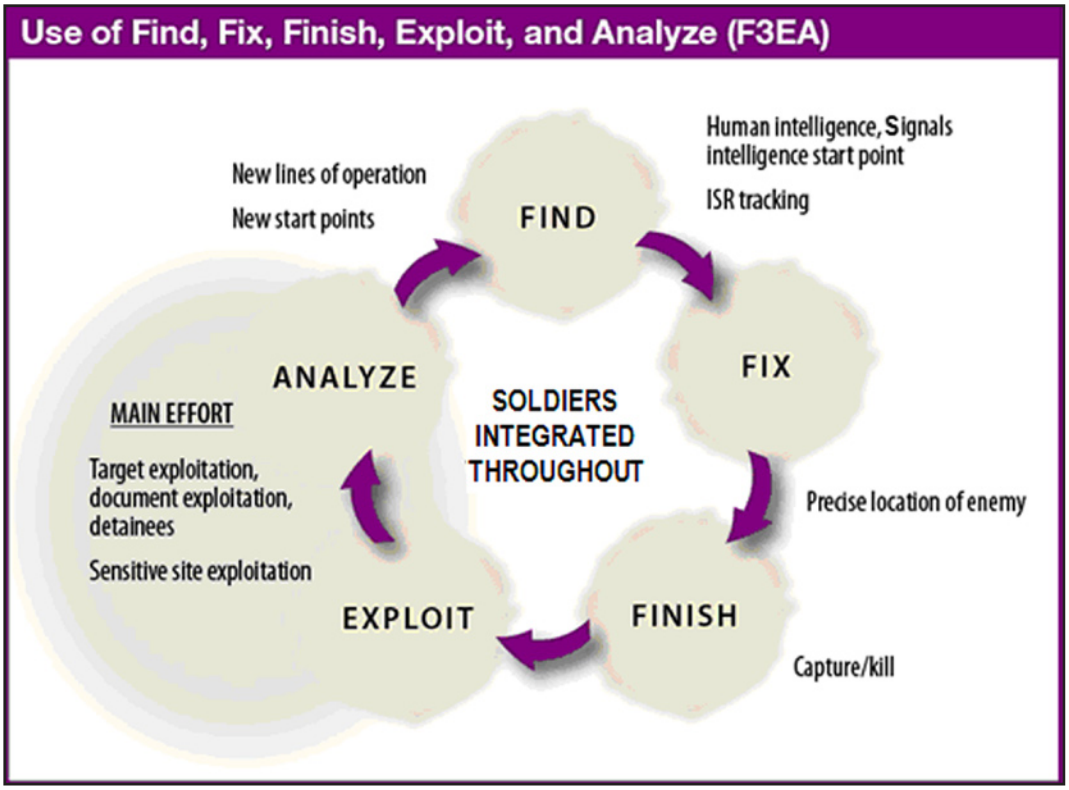


Figure 1. Adapted from "Employing ISR: SOF Best Practices," JFQ, Issue 50, 3rd Quarter, 2008.

On the surface, this is a slight difference, but one that highlights the importance of aggressive targeting and exploitation–the sub-step by which intelligence professionals analyze the findings of the previous operation to drive the subsequent operation.

Find. In the Find phase we, in the S2 Targeting cell, identify the highest level enemy threats within our area of operations (AO) in the form of a High Value Individual List (HVIL), reviewed constantly, updated daily, and recommended by the S2 and approved by the Battalion Commander weekly. Targets are maintained in the form of target packets. A good target packet is a stand alone product, complete with background information on the individual, what his role is in the terrorist/insurgent/criminal structure, his location, his associates, and all supporting reports. Standardization is essential, there were many occasions when we called upon adjacent units to action *our* battalion targets because they had departed the AO. If every unit uses the same format, the hand-off is seamless and the operation is that much more likely to succeed.

Fix. The Fix phase consists primarily of tasking or allocating assets to collect on the agreed upon HVIs. Fixing targets means constructing a good intelligence, surveillance, and reconnaissance (ISR) plan, and at the battalion level the ISR Manager is likely the TIO. All assets must be given specific guidance in order to maximize pertinent collection. The battalion assistant S2 should be familiar with the ISR assets organic to your unit and their capabilities and limitations. You should also take advantage of the assets found at brigade and echelons above brigade (EAB). Knowing who to contact at higher or adjacent units to requisition the right collection asset can make all the difference in the targeting process.

Finish. The Finish function is the actual mission conducted to capture/kill the individual being tracked. Many times, higher sensitive assets will aid in locating the HVI. Then a dedicated element will move to the site, kill or capture the target, and begin exploitation. This is the fruit produced by the Targeting Cell's efforts. From both the intelligence and maneuver perspectives, these are the most rewarding operations conducted.

Exploit. During the Exploitation phase, dedicated assets manipulate all materials taken from the objective in order to produce as much refined intelligence as possible. This process begins with sensitive site exploitation (SSE). If the SSE element is trained and competent, the materials collected will pay great dividends within the F3EA cycle. They must know how to search, what to search, and where to search. Before deployment, my section coordinated training by the Asymmetric Warfare Group with each maneuver platoon in order to synchronize methods and ensure effective search and seizure. As the detainee was processed at the Detainee Holding Area (DHA), my section found it very useful to produce a source-directed requirement in order to shape and focus the questioning by interrogators. This step also included all document and media exploitation (DOMEX), conducted by a dedicated DOMEX element collocated with the DHA.

Analyze. The Analyze phase includes all analysis after the kill/capture of an individual and then using the knowledge gained to identify follow-on targets and advance the targeting process.

The Targeting Process

Our battalion targeting battle rhythm consisted of two weekly targeting meetings, a brigade targeting meeting, and often one to three lethal targeting operations per week.

The first meeting (Pre-Targeting) was held on Tuesdays and laid out a basic collection plan for the week ahead. Attendants at this meeting were the S2, S3 Operations, S3 Plans, the S5, company fire support officers (FSOs), and representatives from our enabler elements. I would cover any updates to our HVIL and discuss their level of readiness to action. Our Effects OIC (S5), a Field Artillery major, would discuss upcoming non-lethal targets such as medical civic action programs, tactical PSYOPS teams' and Civil Affairs' efforts, and governance targets.

The second meeting (the actual Targeting Meeting) was held later in the week on Thursdays. Further targeting development updates were covered but the primary purpose of the session was to dedicate assets to

either continue collection or plan to action prepared targets. The presence of the S3 Plans was essential to this meeting because he constructed the weekly mission matrix and was able to easily designate platoons to conduct the actual raids. These meetings were chaired at first by the battalion FSO, then the S3 Plans, and finally myself.

Another targeting meeting was also held at the brigade level each Thursday evening. This meeting was attended by the Brigade S2, the Fusion Cell OIC, the S2X, various Brigade enablers, and the battalion targeting OICs. The primary purpose of this session was to synchronize collection efforts and allocate Brigade or higher assets to the battalions for upcoming operations.

During the targeting operations, often referred to as time sensitive targets (TSTs), an additional ISR plan was put into place to support the maneuver element. Usually, unmanned aerial systems or the persistent threat detection system was employed as overhead Imagery Intelligence to identify any potential route obstacles or "squirters" (those enemy individuals attempting to evade capture). EAB Signals Intelligence (SIGINT) was also used to a great extent in order to aid in geolocation. In all cases, a Human Intelligence Collection Team (HCT) member accompanied the maneuver unit in order to conduct tactical questioning on site. If possible, the HCT would also provide the appropriate source that ideally would positively identify the target prior to movement to the DHA. On operation day, the incorporation of every possible intelligence discipline must be brought to bear by the Targeting OIC in order to ensure a successful mission.

Dedicated TST Platoon

At this juncture, it may be helpful to consider implementing a dedicated on-call TST platoon. With three missions per week, we found it extremely useful to employ our Mortar Platoon as the planned element in targeting. Many times, the hectic patrol schedule will not allow for the flexibility to task other platoons from the maneuver companies; but this platoon, acting as a battalion asset, was ideal. The relationship with the platoon was excellent, and the platoon itself became highly efficient in TST operations. As an added benefit, it was well versed in SSE and became, in essence, a platoon battle drill. Upon completion of SSE, it was responsible for transporting the detainee to the DHA annex and as a result became familiar with and remarkably effective in detainee operations (DETOPS).

Targeting Enablers

The battalion was supported by several enablers including one four-person HCT, a dedicated SIGINT analyst, a law-enforcement professional contractor, an Air Force Joint Terminal Attack Controller team, a TPT, CA, and of course a full complement of interpreters, two of whom were Category II interpreters. I, one of the junior noncommissioned officers (NCOs), one of the junior enlisted Soldiers, and often most of the enablers were dedicated to the battalion's targeting effort. All of the enablers with one exception maintained a physical presence in our battalion Tactical Operations Center. The exception was the SIGINT analyst who was collocated with the Brigade SIGINT cell in order to generate products which required higher classifications. However, either I or my NCO maintained daily communications with the SIGINT analyst in order to ensure he understood the battalion's targeting priorities. In this regard and in many other aspects of the targeting process, the most essential skill an officer must display remains interpersonal proficiency. Picking up the phone in order to request a pattern of life product, a technical asset from brigade, or just providing guidance to your enablers requires a keen talent for establishing rapport and maintaining good relationships with any and all personnel who can facilitate your targeting.

The HCT, at first, lent only general support to our Battalion's operations. This was not ideal and eventually our Brigade assigned them under tactical control to the 2-69 AR. This enabled us, in turn, to dedicate one HCT member per company with a "floating" team leader. This measure was largely responsible for any successes we experienced in the targeting process. In order to ensure focus, situational understanding, and efficient source operations, one HCT member should be dedicated to each

maneuver company if at all possible. I believe this concept can be further improved upon if the detachment of HCTs is ordered much earlier in a unit's lifecycle. Under this system, I would recommend distributing HCTs from the Military Intelligence Company at least four to six months out from the deployment date. This would ensure a good working relationship during train-up, for example at the National Training Center, and allow the HCT members to become familiar with the organizations they are expected to work with in theater.

In the COE, the commander's priority intelligence requirements (PIRs) may focus on whether or not an adopted course of action is affecting the populace. One way to gauge the sentiments of the people is to employ TPT and CA. These enablers are trained to influence and measure the behaviors, attitudes, and ideas of the population. Although they are largely managed by the Effects cell, they should be considered non-traditional ISR assets that can answer the commander's PIRs.

Targeting Support to Effects

Intelligence must also support non-lethal targeting. Although the Effects cell is the proponent for atmospherics, governance, information operations, public works projects, and much more, the S2 will often recommend the best employment of these effects based on the enemy's disposition and the PIRs. For example, higher headquarters may direct subordinate units to reward grants to local businesses in order to stimulate the local economy and create jobs. The Effects cell will undoubtedly be the proponent of this action. But the Intelligence section, and often the Targeting OIC, will recommend what businesses and what neighborhoods will benefit most by the effort. A neighborhood rife with insurgent activity or businesses with known ties to the insurgency will likely not receive the grant. Platoon leaders in good units will complete patrol debriefs for each combat patrol. The Targeting OIC must examine each debrief and use the information therein to support non-lethal targeting.

Conclusion

As the assistant S2, you will very likely perform essential targeting tasks. In the COE, targeting means figuring out who the bad guys are, building a solid evidence packet against them, detaining them, then exploiting the results. If practical, the S2 section must schedule the appropriate classes and training *before* deployment in order to ensure essential task proficiency and thus success. This includes language training for leadership across the board, SSE and DETOPS tactics, techniques, and procedures, report writing (such as patrol debriefs and sworn statements), employment of biometrics equipment, and much more. Once in theater, the TIO himself must be aware of all assets at the battalion's disposal to conduct targeting, to include higher echelon assets.

Leveraging those assets, staying organized, and maintaining good interpersonal relationships with all facilitators will guarantee a successful targeting system. Rooting out the irreconcilable elements of the population in our AO paid large dividends toward advancing the security line of operation for the 2-69 AR Battalion and the surrounding area.

Bibliography

Flynn, Michael T., Juergens, Rich, and Cantrell, Thomas L. Employing ISR: SOF Best Practices." *Joint Forces Quarterly* 50 (3rd Quarter 2008): 56-61.

Pray, Jeremiah. "Kinetic Targeting in Iraq at the Battalion Task Force Level: From Target to Detainee." *Infantry Magazine* July-August 2005.

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

Intelligence Support to Effects, 96B Student Handout, August 2006.

Threats in Southern Iraq Ahead of a U.S. Withdrawal

by Lieutenant Colonel John Johnson, U.S. Army

Introduction

In November 2008, the U.S. and Iraq signed a bilateral security agreement, which set two major deadlines leading up to the withdrawal of U.S. forces from Iraq: the withdrawal of all U.S. combat forces from Iraqi cities by 30 June 2009 and the withdrawal of all U.S. forces from Iraq by 31 December 2011.[1] Additionally, in February 2009, President Obama announced that all U.S. combat forces would be withdrawn from Iraq by 31 August 2010, leaving several advisory and assistance units and headquarters elements in Iraq and setting the force ceiling at 50,000 for those remaining at the end of August 2010.[2]

As was the case during the deployment of U.S. forces into Iraq in 2003, the majority of U.S. forces will likely exit Iraq through the south, moving equipment to Iraqi and Kuwaiti ports in the northern Arabian Gulf for loading onto ships and subsequent return to U.S. bases or to other theaters of operation. There are three primary threats to the combat forces drawdown in southern Iraq including: Shia militant groups opposed to the presence of U.S. forces; Iranian influence that ranges from helpful to disruptive and deadly to U.S. and Iraqi Security Forces (ISF); and intra-Shia violence, where Shia political groups compete for power and resources.

Southern Iraqi port of Umm Qasr. (U.S. Army photo by SPC Darryl Montgomery)

This article focuses on Shia militant groups and malign Iranian influence, and also briefly addresses the potential threat of intra-Shia politically motivated violence. Additionally, while the majority of violence in Iraq over the past six years has been concentrated in Baghdad, Anbar Province in western Iraq and in northern Iraq, the environment in southern Iraq described in this article highlights how the complex, multi-faceted nature of the southern region can affect the impending withdrawal of U.S. forces. This article also provides a description of the three major threats in southern Iraq, identifies several unlikely wildcard events which could alter the security situation, and concludes that while violence in the south is quite low when compared to historical trends and compared to the rest of Iraq, there remains several areas where U.S. forces should focus their efforts to ensure violence remains low ahead of the U.S. withdrawal from Iraq.

U.S. forces should focus on five areas including: maintaining active force protection measures during convoys and at U.S. bases; retaining the capability to conduct targeting operations against militant leaders; sustaining an Information Operations (IO) campaign which emphasizes U.S. compliance with the security agreement; supporting Government of Iraq (GoI) reconciliation efforts with militant groups, and countering Iranian influence through continued intelligence collection emphasis and border security improvements along the Iraq-Iran border.

Shia Militant Groups

The three major Shia militant groups in southern Iraq are Muqtada al-Sadr's Promised Day Brigade (PDB), and independent groups Asa'ib Ahl al-Haq (AAH) and Kata'ib Hizballah (KH).[3] They all share a common opposition to the U.S. presence in Iraq and by extension a common goal of having U.S. forces leave Iraq. All three groups use violence against U.S. forces as their intent is to hasten a U.S. withdrawal and to claim credit for forcing the U.S. departure. It is also likely some militants move between groups depending on factors such as availability of funding

and weapons, and whether or not their group leaders support reconciliation efforts.

Muqtada al-Sadr's PDB militia is a relatively new organization in name only. Sadr created PDB's predecessor militia group Jaysh al-Mahdi (JAM), or the Mahdi Army, in July 2003 to oppose the Coalition presence. From 2003 through 2008, JAM employed a variety of different attack mechanisms against Coalition Forces including improvised explosive devices (IEDs), explosively formed projectiles (EFPs) and indirect fire (IDF). Further, JAM staged two uprisings against the Coalition in April and August 2004,[4] and was also heavily involved in sectarian violence following the February 2006 attack on the Shia al-Askari (Golden domed) mosque in Samarra as Sadrists indiscriminately attacked presumed Baathists and Wahhabists.[5] In August 2007, after several Sadrist splinter factions emerged and Sadr's followers desecrated a major Shia religious festival in Karbala, Sadr ordered a freeze on JAM activity. In 2008, Sadr announced that the majority of JAM would be transitioned into a socio-cultural organization called the Mumahudun and a small number of fighters under a new name, the PDB, would be retained to continue the fight against Coalition Forces.[6]

Multi-National Division-South Explosive Ordinance Detachment finds rocket rail system following indirect fire attack. (U.S. Army photo by SGT Frank Vaughn)

AAH is a Sadrist splinter organization formed by senior Sadrist Qays al-Khazali who was detained by Coalition Forces in March 2007.[7] The group is currently led by co-founder Akram al-Kabi.[8] Like the PDB, AAH employs IEDs, EFPs, IDF and has publicly claimed over 6,000 attacks against the Coalition Forces and the ISF.[9] The AAH was initially formed in late 2004 as an elite JAM group with the support of Iran's Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF).[10] The AAH leadership split from Sadr in mid-2006 leading Sadr to publicly challenge the group's leaders for negotiating with the Coalition.[11]

Finally, KH is a small, but lethal Shia militant group that has actively opposed the Coalition since 2003. Additionally, KH condemned the signing of the U.S.-Iraq bilateral security agreement, and threatened Iraqis who signed the agreement.[12] The group previously claimed attacks under the name of the Shia Islamic Resistance in Iraq. The KH conducts attacks with advanced weapons from Iran, such as IEDs, EFPs and improvised rocket assisted mortars (IRAMs). In July 2009, the U.S. State Department designated KH as a Foreign Terrorist Organization and the U.S. Treasury Department designated KH as an "Entity Posing a Threat to Stability in Iraq." These designations prohibit all transactions between KH and any U.S. person and freeze any assets KH may have under U.S. jurisdiction.[13]

Iran's Malign Influence

Iran's influence on southern Iraq's political and militant groups runs the gamut from benign–as in the case of political engagements with Iraqi political groups, some of whose leaders reside in Iran–to overtly disruptive as in the case of providing lethal aid (weapons), funding, training and safe haven to Iraqi Shia militants. During the height of attacks against U.S. forces in 2007, U.S. military and diplomatic leaders in Iraq provided a litany of statements and some evidence displaying Iran's malign influence in Iraq including Iranian markings on weapons and evidence of Iran supplying technology and training to militants.[14]

In September 2008, a Defense Department quarterly report on stability and security in Iraq stated, "Malign Iranian influence continues to pose the most significant threat to long-term stability in Iraq. Despite continued Iranian promises to the contrary, it appears clear that Iran continues to fund, train, arm and direct [special groups] intent on destabilizing the situation in Iraq."[15]

In May 2009, the U.S. State Department released excerpts from its annual Country Reports on Terrorism. The following excerpt highlights Iran's involvement in Iraq.

"Despite its pledge to support the stabilization of Iraq, Iranian authorities continued to provide lethal support, including weapons, training, funding, and guidance to Iraqi militant groups that targeted Coalition and Iraqi forces and killed innocent Iraqi civilians. Iran's Qods Force continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, and mortars that have killed Iraqi and Coalition Forces as well as civilians. Tehran was responsible for some of the lethality of Anti-Coalition attacks by providing militants with the capability to assemble IEDs with EFPs that were specifically designed to defeat armored vehicles. The Qods Force, in concert with Lebanese Hizballah, provided training both inside and outside of Iraq for Iraqi militants in the construction and use of sophisticated IED technology and other advanced weaponry."[16]

Since 2003, the flow of lethal munitions from Iran to Iraq has resulted in the death or injury of hundreds of U.S. forces in Iraq.[17] In June 2009, General Odierno, Commanding General, Multi-National Forces-Iraq, stated Iran's support to Iraqi groups has slowed.[18] Additionally, General Odierno said Iran "might also be trying to do a bit more soft influence in Iraq as well," a reference to Iran's political, religious and economic influence versus lethal aid to militant groups. He indicated Iran's shift in strategy was due to several factors including the security agreement being signed, Iranian-supported candidates doing poorly in the 2009 Iraqi provincial elections, successful targeting of Iranian surrogates in Iraq, and pressure applied to the Iraq-Iran border by U.S. and ISF.[19]

In spite of Iran's recent and apparent shift in strategy, Iran is still providing training and some weapons to Iraqi militants.[20] Additionally, while Iran's focus ahead of the January 2010 Iraqi parliamentary elections appears to be on supporting Shia political groups, Iran retains the capability to increase training, funding and weapons flow to militant groups in Iraq should circumstances change, and thus necessitates further monitoring.

Intra-Shia Violence

The three major Shia political groups vying for power and resources in southern Iraq are Prime Minister Nouri al-Maliki's Islamic Dawa Party or State of Law Party, Sadr and his followers–often called Sadrists; affiliated with the Office of the Martyr Sadr (OMS), and the Islamic Supreme Council of Iraq (ISCI).[21] Among these political groups, only Sadr (presently in Iran) has consistently opposed the presence of U.S. forces in Iraq.[22] In November 2008, ahead of an Iraqi cabinet vote on the bilateral security agreement, he read a statement to thousands of supporters at Friday prayers saying, "I repeat my demand to the occupier to leave our land without keeping bases or signing agreements. If they keep bases, then I would support honorable resistance."[23] The Islamic Dawa Party and the ISCI generally have worked with U.S-led Coalition Forces and probably do not directly represent a threat to U.S. forces unless conditions change significantly.

The intra-Shia threat stems from potential violence perpetrated by competing political groups and their supporters that could spill over and affect stability in southern Iraq, thereby complicating the U.S. withdrawal during the post-election phase to the seating of the new Iraqi government in the May/June timeframe. In January 2009, even though the ISF proved to be capable of providing adequate security for election voting stations, the Iraqi provincial elections were marked by some violence and intimidation.[24] We can expect some attacks leading up to the January 2010 parliamentary elections, which will likely come in the form of targeted political assassinations and intimidation attacks; post-election violence is also a possibility.

Wildcard Scenarios

While wildcard scenarios are not necessarily threats, there are several unlikely but dangerous potential wildcard scenarios, which if they were to occur, would negatively impact the security situation in southern Iraq. The upcoming January 2010 parliamentary elections offer three such wildcard scenarios. The first is a scenario whereby the Iraqi public does not view the elections as free and fair. This scenario was typified by the June 2009 Iranian national elections, which were widely viewed as unfair and resulted in large-scale protests and violence in Iran. However, the prospects of such an election outcome in Iraq are belied by two previous highly successful election events; the 2005 Iraqi parliamentary elections and the 2009 provincial elections.

The second wildcard is a Bitter Loser scenario where certain political parties come out of the elections dissatisfied with the outcome and resort to violence as a means to voice their dissatisfaction.

The third wildcard scenario is related to the security agreement referendum. Originally scheduled for July 2009, there are signs that the Iraqi government

may approve a bill that calls for an Iraqi vote on the security agreement in conjunction with the January 2010 parliamentary elections. If Iraqi voters reject the security agreement in a referendum, U.S. forces could be forced to leave Iraq within one year. This outcome could hasten, and thereby complicate a U.S. withdrawal and could also provide additional justification for militant Shia groups to conduct attacks against U.S. forces.

The fourth wildcard scenario involves the Grand Ayatollah Ali al-Sistani, Iraq's Najaf-based senior Shia cleric. While there are no indications that Sistani is in ill health, his death certainly would result in large gatherings of mourners and probably a prolonged period of uncertainty over the Shia clerical leadership in Iraq as senior clerics in Najaf choose his successor.

The last wildcard scenario involves desecration of Shia holy sites. Specifically, southern Iraq is home to several important Shia shrines in Najaf and Karbala. As was seen after the 2006 attack on the Golden Dome Shia shrine in Samarra, there was a sharp increase in Shia-versus-Sunni sectarian violence across Iraq. A similar attack on one of southern Iraq's Shia shrines in Najaf or Karbala could set off a series of sectarian-motivated reprisal attacks, although this would not likely be on the same scale as was seen following the Samarra attack.

Further, while beyond the scope of this article, unemployment, effective rule of law and corruption are areas which bear watching closely as they have the potential to be "game changers" and drive instability.[25]

Conclusions/Recommendations

Based upon the analysis of the three primary threats in southern Iraq ahead of a U.S. withdrawal, there are four conclusions and associated recommendations:

Presence of U.S. Troops: Continuous Issue. Despite positive security trends, an increasingly capable ISF and the impending departure of U.S. forces, the principal grievance of the three major Shia militant groups in southern Iraq is the presence of U.S. forces. This suggests that low level attacks will likely continue for as long as U.S. forces remain in Iraq. Therefore, U.S. forces should maintain vigilance in their force protection posture during vehicle convoys and at U.S. bases, and should continue to put pressure on militant networks through lethal and non-lethal targeting operations partnered with the ISF against militant group high value individuals (HVIs).

Militants Planning Parting Blow. Despite a decrease in violence Iraq-wide, and in southern Iraq in particular, over the past 24 months Shia militants did conduct multiple attacks leading up to the June 30, 2009 departure of Coalition Forces from Iraqi cities. These attacks were likely done in order to claim credit for the Coalition's departure and to take advantage of lingering distrust over U.S. intentions in Iraq. These attacks also suggest that militants have the capability to conduct attacks against U.S. forces as they withdraw from Iraq. To counter this threat, U.S. forces should continue aggressive route clearance procedures, include mandatory ISF escorts with redeploying U.S. convoys and, at the strategic and operational levels, sustain an IO campaign which clearly conveys U.S. intentions to withdraw within established security agreement deadlines.

Reconciliation: An Effective Tool. As the ISF have become more proficient and the security situation in Iraq has improved, some Shia militant groups have engaged the Iraqi government in the reconciliation process.[26] From March to August 2009, reports have surfaced which indicated AAH and the GoI were involved in negotiations whereby AAH would agree to an unconditional cease-fire and move "towards peaceful integration into Iraqi society."[27] As part of the negotiations, Laith Khazali, a senior member of AAH, was transferred in June 2009 from U.S. custody to the GoI and subsequently released.[28] The decrease in violence in Iraq, and particularly Baghdad's International Zone recently, suggests reconciliation between AAH and the GoI has resulted in at least a temporary decrease in attacks. While a strategic decision, similar GoI efforts to engage southern Iraq's other two militant groups (KH and PDB) should be considered in order to persuade militants that the way ahead lays in political engagement with Baghdad and not in violence.

Countering Iran's Malign Influence. We should expect some Iranian influence in, and engagement with Iraq given their lengthy shared border; however, the analysis suggests that Iran shifted in 2008-2009 to more of a soft power approach in Iraq. Analysis also suggests a sizable force of Iranian

trained and equipped Shia militia. Iran has trained and provided lethal aid to Shia militants, funded their operations and provided safe haven to southern Iraq's Shia political and militant group leaders. Therefore, at the strategic, operational and tactical levels, U.S. forces should continue to work aggressively with their Iraqi counterparts to counter Iran's malign influence. At the strategic level, pressure from GoI leaders on Iran's senior leaders has proven effective and should continue.[29] At the operational and tactical levels, we should continue and possibly increase intelligence collection emphasis along the Iraq-Iran border coupled with border security improvements, specifically funding, training, manning and infrastructure for Iraq's Department of Border Enforcement.

Iraqi border guards conducting training exercise with U.S. Border Transition Team on Iraq-Iran border. (U.S. Army photo by SPC Darryl Montgomery)

Final Thoughts

Due to a number of factors including the success of the "surge" strategy, the Sons of Iraq (SOI) citizen security program, improved ISF proficiency, Sadr's freeze order, AAH reconciliation, and Iran's shift to a soft power approach, violence in Iraq is sharply down from its 2007 highs. And while it is highly unlikely that the security trends will reverse themselves, there remain in southern Iraq a number of threats and potential wildcards which could prove problematic during a U.S. withdrawal. Therefore, U.S. forces should watch these threats and wildcard scenarios closely and be proactive in multiple areas such as force protection, IO, reconciliation and border security to facilitate the successful withdrawal of U.S. troops and equipment through southern Iraq.

Key Dates

July 2003–Muqtada al-Sadr announced the formation of Jaysh al-Mahdi (JAM)

April 2004–First JAM uprising against the Coalition

August 2004–Second JAM uprising against the Coalition

Late 2004–AAH formed as an elite JAM group with support of IRGC-QF

January 2005–Iraqi National Elections

December 2005–Iraqi Parliamentary Elections

February 2006–Bombing of the al-Askari Shrine (Golden Domed Mosque) in Samarra

Mid 2006–AAH leadership split from Sadr

February 2007–Start of Baghdad "Surge" Security Plan

August 2007–Sadr ordered "freeze" on JAM activity

October 2007–U.S. Treasury Department named IRGC-QF a Specially Designated Global Terrorist

March 2008–Start of Operation Charge of the Knights (CoTK) in Basra

June 2008–Sadr announced JAM would be disbanded

November 2008–Sadr announced formation of Mumahudun and PDB

November 2008–U.S.-Iraq Bilateral Security Agreement (SA) signed

January 2009–Iraqi Provincial Elections; possible SA Referendum

February 2009–President Obama announced U.S. combat forces out of Iraq by 31 August 2010

February 2009–President Obama announced 50,000 U.S. troop ceiling by 31 August 2010

June 2009–AAH member Laith Khazali released as part of reconciliation talks with GoI

June 2009–SA deadline to withdraw U.S. combat forces from Iraqi cities

July 2009–U.S. State Deptartment designated KH as a Foreign Terrorist Organization

January 2010–Iraqi Parliamentary Elections

August 2010–Deadline to withdraw U.S. combat forces from Iraq; 50,000 U.S. troop limit

December 2011–SA deadline to withdraw all U.S. forces from Iraq

Acronyms

AAH–Asa'ib Ahl al-Haq

EFP–explosively formed projectile

GoI–Government of Iraq

HVI–high value individual

IED–improvised explosive device

IDF–indirect fire

IO–Information Operations

IRAM–improvised rocket assisted mortar

IRGC-QF–Islamic Revolutionary Guard Corps-Qods Force

ISCI–Islamic Supreme Council of Iraq

ISF–Iraqi Security Forces

JAM–Jaysh al-Mahdi

KH–Kata'ib Hizballah

OMS–Office of the Martyr Sadr

PDB–Promised Day Brigade

SA–Security Agreement

SOI–Sons of Iraq

Endnotes

1. Agreement Between the United States of America and the Republic of Iraq On the Withdrawal of United States Forces from Iraq and the Organization of Their Activities during Their Temporary Presence in Iraq, November 17, 2008.

2. *"Remarks of President Barack Obama–Responsibly Ending the War in Iraq,"* As Prepared for Delivery, Camp Lejeune, North Carolina, 27 February, 2009.

3. Multi-National Force-Iraq Press Release, *"The Insurgency,"* 30 April 2009.

4. Ibid.

5. International Crisis Group, *"Iraq's Muqtada al-Sadr: Spoiler or Stabiliser?,"* Middle East Report No. 55, 11 July 2006.

6. Multi-National Force-Iraq Press Release, *"The Insurgency,"* 30 April 2009.

7. Marisa Cochrane, *"Asaib Ahl al-Haq and the Khazali Special Groups Network,"* Institute for the Study of War, 13 January 2008.

8. Ibid.

9. Multi-National Force-Iraq Press Release, "The Insurgency," 20 April 2009.

10. Ibid.

11. Ibid.

12. Ibid.

13. "*Treasury Designates Individual, Entity Posing Threat to Stability in Iraq,"* Press Room TG-195, July 2, 2009.

14. Greg Bruno, *"Iran's Involvement in Iraq,"* Council on Foreign Relations, 3 March 2008.

General David H. Petraeus, *"Report to Congress on the Situation in Iraq,"* 10-11 September 2007.

Carol L. Bowers, *"Iran Playing 'Destabilizing Role' in Iraq, Crocker Says,"* American Forces Press Service, 11 September 2007.

Tim Kilbride, *"Blocking Flow of 'Accelerants' Critical to Baghdad Security,"* American Forces Press Service, 11 May 2007.

Barbara Slavin and David Jackson, *"Iran's Role in Iraq Met With Skepticism,"* USA Today, 5 February 2007.

15. Fred W. Baker, *"Report Says Iraq Security Improves, Fundamental Conflict Remains,"* American Forces Press Service, 30 September 2008.

16. U.S. State Department, *"Excerpts of Country Reports on Terrorism 2008: Middle East, Iraq,"* 4 May 2009.

17. James Phillips, *"Iran's Hostile Policies in Iraq,"* The Heritage Foundation, Backgrounder No. 2030, 30 April 2007.

18. General Ray Odierno, *"Press Briefing, 30 June,"* Multi-National Force-Iraq, 30 June 2009.

19. Ibid.

20. Ibid.

21. Anthony H. Cordesman, *"The Changing Situation in Iraq: A Progress Report,"* 4 April 2009.

22. Greg Bruno, *"Muqtada al-Sadr,"* Council on Foreign Relations, 16 May 2008.

23. Campbell Robertson and Suadad Al-Salhy, *"Cleric Call for Resistance to U.S. Presence in Iraq,"* New York Times, 15 November 2008.

24. Martin Chulov, *"Violence and Intimidation Mark Run-Up to Iraqi Elections,"* The Guardian, 30 January 2009.

25. Anthony H. Cordesman, *"The Changing Situation in Iraq: A Progress Report,"* 4 April 2009.

26. Multi-National Force-Iraq Press Release, *"The Insurgency,"* 30 April 2009.

27. Marisa Cochrane, *"Senior Shia Militant Released from Custody,"* Institute for the Study of War, 10 June 2009.

28. Ibid.

29. Alexandra Zavis, *"Iraq Sends Team to Iran to Discuss U.S. Accusations,"* Los Angeles Times, 2 May 2008.

LTC John Johnson is the Director of Intelligence, Multi-National Division-South, Basra, Iraq. He holds a BA from Texas Christian University, Fort Worth, Texas, an MA from Alliant International University, San Diego, California, and an M.M.A.S. from the U.S. Command and General Staff College, Fort Leavenworth, Kansas. He deployed to Iraq from March 2005 to March 2006 as an Intelligence Operations Officer for Multi-National Forces-Iraq and from April 2009 to present with the 34th Infantry Division. LTC Johnson has also served in various command and staff positions with the Army G2, U.S. Army Europe, III Corps, 1st Infantry Division, 1st Cavalry Division and 501st Military Intelligence Brigade.

Take Advantage of OSINT

by Walter R. Draeger

Introduction

You probably don't realize it but you already use Open Source Intelligence (OSINT). While OSINT has been around for a long time, it's a relatively new intelligence discipline for the Army. Unlike Human Intelligence (HUMINT) or Signals Intelligence (SIGINT), you won't find Army personnel with OSINT military occupational specialties or additional skill identifier. And when looking for an OSINT unit, only a handful will be found. Yet, within the Army interest is rapidly increasing due to the explosive growth of Information Age technologies. With 3.1 billion people accessing the Internet today, life as we know it is radically changing. Experts estimated in 2007 there were approximately 50,000 extremist and terrorist web sites consisting of forums, blogs, social networking sites, video sites, and virtual world sites (i.e., Second Life). For jihadists, the Internet is the perfect communication tool because it mirrors their framework–decentralized and anonymous, with fast communication to a large audience. In this article, we'll cover a brief introduction to OSINT, discuss its value, and provide training strategies on how to become more proficient, and perhaps an expert in OSINT.

Anyone can take advantage OSINT; it's not just for a Military Intelligence (MI) Soldier. OSINT's value applies across the board to all Soldiers, in any situation from strategic to tactical, it's for everyone. OSINT can provide general information, such as country studies, mapping, biographical, satellite imagery, and technical information about the operational environment. There is great tactical value for OSINT in the Army. Many commanders just don't realize how many intelligence requests are filled using OSINT.

Getting that information combines good analytical skills and the research tools needed to get to the "dark web." As you become more skilled and can combine it with both cultural understanding and a language, you'll be able to generate more specific and detailed information such as these OSINT source reports: [1]

- An OSINT was able to pull multiple terrorist bank-routing numbers and fund-raising accounts from public venues.
- An OSINT was able to use Google and other public Search Engine tools to locate the physical address, fax number, e-mail accounts, and resume of a Hezbollah Affiliate living in Africa.
- An OSINT was able to find several al Qaida-like cyber actors that recommended using social networking tools, such as Twitter and Facebook to conduct propaganda and recruitment activities.
- An OSINT was able to discern if specific rhetoric was being used to incite violence against U.S. Forces in an area of responsibility (AOR).
- An OSINT was able to use the Internet and U.S. government open source portals to track the bios and activities of a variety of people and/organizations that have posed a threat to U.S. Military Operations.
- An OSINT was able to assess and view counter-interrogation and counter-surveillance techniques that were being recommended by a particular terrorist organizations.
- An OSINT was able to locate several online terrorist nodes, how they communicated, their affiliates, and in some cases where they were physically located.

OSINT Lessons Learned.

Using OSINT

Learning how to use OSINT directly contributes to the Army's fight for information superiority. The Army faces a future of persistent conflict filled with uncertainty. This means that at all levels timely knowledge is essential. Soldiers who know and understand the diplomatic, information, military and economic elements will work smarter in an operational environment.

With OSINT, each Soldier becomes a more informed, dynamic, knowledge-based Soldier who can adapt to an agile adversary. For instance, in the past Soldiers used maps almost exclusively developed from the National Geospatial-Intelligence Agency and other sources. Maps produced by these agencies were (and still are) limited, not always providing today's needed tactical perspective, such as an alley way within a high-fidelity urban and complex environment.

Sadr City, Iraq using Google Earth.

Today's "knowledge Soldiers" will not wait for maps but seeks solutions on their own; they use products like Google Earth at http://earth.google.com or

Ask.com at http://www.maps.ask.com to gain situational awareness. The cumulative outcome of all "knowledge Soldiers" trained in OSINT is that both individuals and units can quickly self-synchronize and self-adjust to an agile adversary.

Ad hoc Army OSINT units successfully exploit OSINT in Afghanistan, Iraq, and throughout the world. In these counterinsurgencies, the key terrain is "the population" which is subjected to wave after wave of propaganda in the local open press, radio and television. The 10th Mountain Division organized an ad hoc OSINT cell in Afghanistan during 2005 that brought the capability to track enemy propaganda released in night letters, Internet, radio broadcasts, and local television. They published a daily product called the Mountain Sentinel which analyzed media sources, content and confirmed source assessments. OSINT cell activities were used to cue other assets for possible operations or changes in local sentiment that could have affected the area of operations. In Iraq, the 101st Airborne Division, created an OSINT cell to monitor the population's reactions through media. It combined an OSINT cell with the Information Office to create a media monitoring cell with a linguist, television, radio, antennae, and newspapers.

The Center for Army Lessons Learned published findings from Operation Iraqi Freedom that the "Army should authorize and resource the formation of OSINT companies with teams direct support to the brigade combat teams."[2] While this hasn't happened, units are still finding creative ways to take advantage of OSINT.

Benefits of OSINT

Benefits of OSINT.

OSINT has some clear-cut advantages over classified information.[3] First, the fact that OSINT can be shared makes it a highly valued commodity. It helps to create the fundamental glue that holds all relationships together–trust. When information is stamped "NOFORN" it is difficult to share, however, OSINT is a product that you can share with allies, coalition partners, non governmental organizations, international governmental organizations or first responders. Regular OSINT exchanges with counterparts help to build trust. On the other hand, a "close hold" environment with counterparts invariably invokes suspicion, doubt, and distrust. Second, OSINT is timely and fast. When a crisis erupts at home or around the globe, intelligence analysts and policymakers often turn first to the Internet, television set, and radio. Commanders need information fast too because their decision making time is compressed, based on OSINT, they can react quickly to readjust military operations. Third, there are far more bloggers, journalists, pundits, television reporters, and think-tanks in the world than intelligence analysts. Depending on the situation, odds are good that an OSINT report can often approach, match, or even surpass classified reporting.

Fourth, despite the large volumes of classified material produced by the intelligence community, the amount of classified information produced on any one topic can be quite limited and may be taken out of context if viewed only from a classified source perspective. OSINT gives the analyst another perspective to view an event, person, or series of events that are not classified. Fifth, OSINT is considerably less expensive to produce than classified information. With a diminishing budget, OSINT is a good bang-for-the-buck. You are simply extracting intelligence from what is already there: a book, a periodical, the Internet, satellite imagery and software. Finally, OSINT can be stored in huge quantities without security issues and over time provides a historical perspective, especially with the new visualization software being developed.

Pursuing OSINT Proficiency and Expertise

It is difficult to become proficient or an expert in OSINT. Although OSINT is an intelligence discipline, it is still relatively new with limited funding, training, and organization. Despite those challenges, with diligence you can achieve expertise. First develop a personal OSINT plan that combines institutional knowledge, web-based instruction, and on-the-job and formal training. Get Field Manual 2-22.9, *Open Source Intelligence*, a well written tactically oriented "how to" OSINT guide, at http://www.army.mil/usapa/doctrine/Active_FM.html. Spend time to trying to understand how OSINT applies to your par-

ticular intelligence discipline. Most importantly, find a seasoned OSINT user/producer or librarian who is willing to mentor you. The librarian community is one of the few professions that produce open source, due mainly to excellent inherent research skills. Another step towards expertise is to develop both a cultural understanding and language skill to apply to your research skills. Finally, attend available formal OSINT training programs.

There are many core OSINT guides you can use for a self-study. One was produced by retired U.S. Army warrant officer Ben Benavides, is the Online Quick Reference Handbook, 2009-04-23 OSINT Link Table (Ben Benavides); another is Robyn Winder's, Untangling the Web, 2007 Edition, at http://nipr.intelink.gov/nsa/UTW/index.html. These guides provide a wealth of information to gain proficiency. Other "starter" websites are listed below.

These websites are intended to familiarize you with OSINT:

www.intelink.gov

www.opensource.gove

www.intelink.gov/sharepoint

http://call.army.mil

www.earth.google.com

www.tec.army.mil

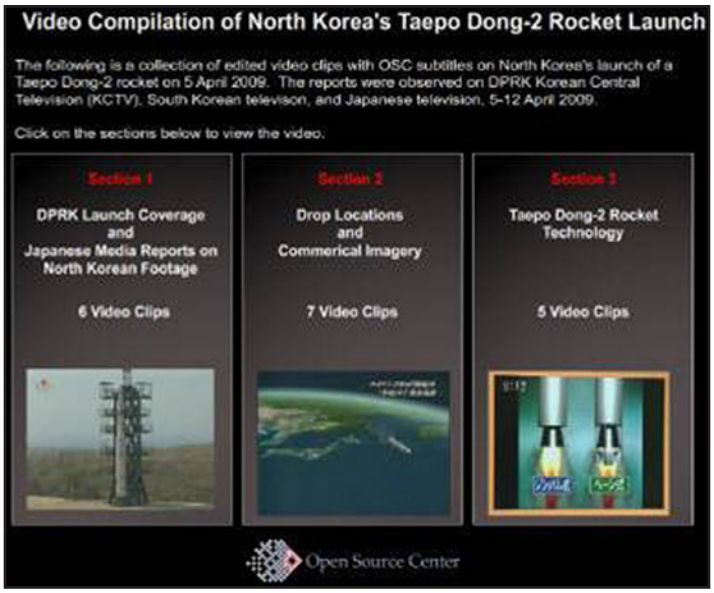
http://www.satimagingcom.com

www.extranet.nga.mil

Starter websites.

OSINT and the Other INTs

Let's take a look at how OSINT can be applied to a few of the intelligence disciplines. Of all intelligence disciplines, Imagery Intelligence products are found in abundance and are very useful. Good imagery and videos rank high on commander's want list. Satellite imagery such as Google Earth and videos provide excellent visualization and most are free. These images can help in identifying people, terrain, buildings and objects. Videos provide excellent understanding and insight. Here is a DVD/web product on the DPRK Taepo Dong-2 rocket derived from Japanese and ROK TV coverage of North Korea's launch on 5 April 2009, featuring 18 edited video clips. [4]



Video compilation of North Korea's Taepo Dong-2 Rocket Launch.

OSINT provides a treasure trove of information for HUMINT that can be used for interrogation. Through social networking sites like facebook.com, twitter.com, and Youtube.com you can build detailed biographical portfolios on individuals, non-state and state representatives you never knew existed.

OSINT provides SIGINT information for intelligence analysts. You can find radio types, signal frequencies, global positions satellite commercial off-the-shelf jamming equipment, software, encryption methods, keys, and instructions. The American University's Management of Global Information Technology Program at http://www1.american.edu/academic.depts/ksb/mogit/country.html publishes student produced analytical reports each semester on all aspects of one country's information technology. Many radio stations around the world now have audio feeds to permit users to listen to them over the Internet, and television is also making more and more of its content accessible over the Internet. There are a number of excellent sites that will help you locate these stations and find out which ones have Internet feeds, one of which is at http://www.radio-locator.com/

The picture shows a Kuwait child who reportedly supports Al-Qa'ida, in YouTube Video that was posted to a jihadist website which praises the child for his support. The young boy appears to be about eight years old and is shown in the video saying that he is a part of Al-Qa'ida and that Usama bin Ladin is his amir.[5]

Kuwait boy on Youtube who supports Al-Qaida and Usama bin Ladin.

The recent Iranian post–presidential election protests initiated an open source war of sorts. Protester command and control was driven mostly with electronic communication, cell phones, twitter.com, and facebook.com to assemble and protest the election. With all these electronic means you would think the Iranian government would simply shut off communications and the Internet. However, it had its own reasons for not shutting-off all electronic communications. The regime in Tehran is utilizing covert technologies to locate cell phone and Internet users who are protesting the theocracy and transmitting data to one another and to the outside world.[6] Once protestors discovered this through open source reports, they started destroying their cell phones. Reports from mobile phone vendors in Iran indicated that demand for Nokia handsets was halved. A boycott prompted some cell phone shops in Iran to remove Nokia hardware from their window displays.[7]

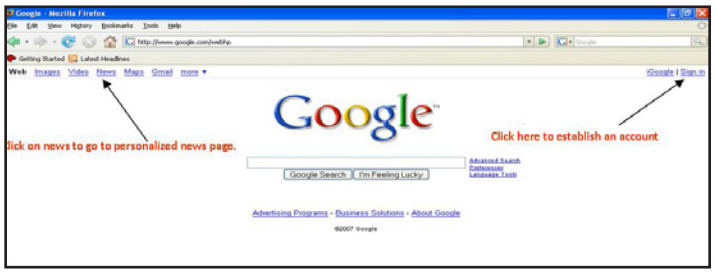
A recent manual for terrorist training camps (not yet published in Afghanistan) obtained from open sources gives extraordinary insight into the mind of the militant.[8] It is packed full of information for the terrorist with detailed diagrams on how to build bombs, how to identify different weapons, and even the ethics of fighting jihad (holy war). There are ten chapters which examine everything you would need to know about militant methods. There are chapters on the rules of jihad, different kinds of fighting techniques, security and intelligence, tactics, maps of fighting and weapons. While this is far from the first manual, it does provide a dynamic and historical perspective on the evolution of militants' methods.

New Taliban Rule Book.

Using Google

A good people finder search engine on the Internet is Google Groups at http://groups.google.com/?pli=1&safe=on.You can build link diagrams for mid- to upper- tier individuals in an organization, determine religious holidays, and gain insight on the local sentiment from newspapers, radio and television.

You can also setup Google to provide a customized open source information toolkit. Let's see how Google can do customized work for you. What you're looking at now is the traditional page. On the upper right is the "sign in" link. Click on this link to establish an account. Once you establish an account click on the news link to go to the personalized news page.[9]



Google setup.

Clicking on the news link brings up the following page (See Figure 1). You'll notice on the left hand side where all the keywords of interest are established. All the classical "INTS' along with some others of interest have been established. Clicking on a keyword, for example "explosively formed projectiles", brings up the latest search on that term. These same keywords can be used in other types of search engines like "Copernic.com." Most search engines have different algorithms and therefore produce different search results. By using two search engines to conduct research, you'll stand a better chance of getting more relevant results and thus more solid news from around the world.

Cautionary Advice

As you learn to work with open source information to produce OSINT, you will learn its limitations. Rarely, does it provide the key that unlocks the "100 percent intelligence solution." However, it almost always provides readily available and timely pieces to the intelligence puzzle. Another concern is the credibility of open sources. Because there are ever increasing number and types of news reporting sources, this doesn't make it more accurate. In fact,

Figure 1. Google news results.

both commercial and government reporting agencies can get duped into reporting inaccurate information. Sometimes this information is disinformation or misinformation. At times, OSINT will need to be verified against classified sources. There are also legal boundaries for what you can and cannot legally do in collecting OSINT; your training will address those limitations. Last, conducting research on open source information requires a protected government computer for operational security because an unprotected search leaves virtual footprints and a computer vulnerable to exploitation.

OSINT Training

Because the Army has no formal OSINT certification program, it does make it more challenging to become proficient, but with diligence it can be done. There are several OSINT programs available to you. As an MI Soldier you will probably receive a basic OSINT familiarization course at Fort Huachuca. This is good introductory training but you'll need to take it a few steps further. You have several options for OSINT programs: online or traditional training, or both. Realize that these programs have limited access and are highly sought after, so you may have to wait to get a slot. If you are deploying, the U.S. Army Intelligence and Security Command (INSCOM) gives a higher priority in providing mobile training team (MTT) support to those units. Keep an eye out for the new Army Knowledge Online web-based OSINT training due in 2010. For funding, try and line up Foundry funds to support your OSINT training. As your OSINT skills become more proficient, and information technologies continue to grow, you will find more and more information of value to aid the unit mission. Good luck on your journey to take advantage of OSINT.

Resources for gaining proficiency in OSINT:

- **The Foreign Military Studies Organization** at Fort Leavenworth, Kansas offers what many consider the Army's best all-purpose OSINT training course. The two week residential course, Open Source Intelligence Research and Analysis (or OSIRA), is offered ten times per year, instructed by experienced OSINT practitioners, and is fully accredited by the U.S. Army Intelligence School. You will find the course listing in the U.S. Army Training Requirements and Resource System. Their telephone is (913) 684-5946 http://fmso.leavenworth.army.mil/OSINT-Training.pdf

- **The Joint Military Intelligence Training Center** offers a host of OSINT courses through the Joint Intel Virtual University (JIVU), both on SIPRNET and JWICS. Users can self register and apply for course dates, many are online. POC is John Fisher, (202) 231-3406, or (202) 231-5488. SIPRNET http://jivu.dse.dia.smil.mil , JWICS http://jivu.dodiis.ic.gov

- **The Open Source Academy (OSA)**, **Open Source Center (OSC)**, Office of National Intelligence offers some of the latest OSINT methods as well as multiple tradecraft, *analytical methods, and regional and problem-focused workshops and MTTs. Newly developed courses are now available using Project Foundry Funds. Foundry* POC is Ron Eggleston, (703) 706-2625. *OSA Registration is* (703) 476-7000, Provost (703) 787-2176, and Mobile and Outreach Training (703) 787-2103 or you can register at the OSC website and view courses online at https://www.opensource.gov/

- **Asian Studies Division (ASD)**, 500th MI Brigade, Camp Zama Japan with over 50 years of OSINT production, far surpasses all other OSINT units in collective production. Deploying units have sent personnel TDY to

observe and glean the latest OSINT techniques from the ASD that have proven effective during Operations Iraqi Freedom/Enduring Freedom. POC is Mr. David Reese, david.reese@ugov.gov.

- **INSCOM, Department of the Army Intelligence Information Services,** (DA IIS) offers a range of opportunities. It has a full-time contractor at ITRADS, Fort Huachuca who can train open source introduction and basics as well as in Iraq (Slayer) and Afghanistan (Bagram) (though primarily Distributed Common Ground Station-Army) who can also address open source. DA IIS will send out an MTT to Army units on request, priority to deploying units. POCs are Dave Drawdy (Open Source Collection Requirements), (703) 706-1279, DSN 312 235-1279, and Sean Ellis (NAI) (703) 706-1159, (312) 235-1159.

- **304th MI Battalion, 111th MI Brigade, Fort Huachuca,** provides a range of activities. It has an open source cell under its S3 produces the "304th MI Bn OSINT Weekly News Summary," an unclassified OSINT product. Request this product by emailing the POC Sarah Wormer at sarah.e.womer@us.army.mil. The 304th also provides "Introduction to Open Source" blocks of instruction for the schoolhouse's basic, advanced, and functional courses, and can provide focused open source MTT courses. Send training requests to the 304th MI Battalion S3 at DSN 821-6515 or commercial (520) 533-6515.

- **The CW2 Christopher G. Nason Military Library (also known as the MI Library) at Fort Huachuca** provides familiarization training for open source information research and with over 50 Thin Clients, cable news, a SCOLA dish for foreign language broadcasts, WiFi, books, periodicals, journals, magazines and newspapers, along with a CyberCafe, it is an excellent location to conduct research. Most importantly, the Chief Librarian, Dr. Vee Herrington is renowned for her open source research expertise and passion to raise awareness. Contact her at (520) 533-4100, and online at http://www.universityofmilitaryintelligence.us/DOD_Authorization.asp

- **The DNI Open Source Intelligence Conference** is held annually and is completely unclassified. Attendees at this two day conference explore a wide range of open source issues and best practices for the Intelligence Community and its partners. Participants from the broader open source community of interest including academia, think tanks, private industry, federal, state, local and tribal entities, international partners, and the media are invited to attend through a free online registration process http://www.dniopensource.org/

Endnotes

1. Interview with OSINT Analyst who requests anonymity, May 2009.

2. Operation Iraqi Freedom, Initial Impressions Report, CALL, January 2004.

3. Stephen C. Mercado, CIA Analyst at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.htm.

4. Open Source Center, 5-12 April 2009.

5. Open Source Center, Jihadist Websites–*OSC Summary* in Arabic, 9 February 2008.

6. Jamsheed Choksy, Huffington Post, Iran, Protest, and Intelligence: Why Strategic Reports Often Get it Wrong, 22 July 2009, accessed at http://www.huffingtonpost.com/jamsheed-k-choksy/iran-protest-and-intellig_b_243052.html.

7. Will Park, Intomobile News, Nokia Sees Demand Halved in Iran-Wary Iranians Boycott Nokia in Protest, 15 July 2009, accessed at http://www.intomobile.com/2009/07/15/nokia-sees-demand-halved-in-iran-wary-iranians-boycott-nokia-in-protest.html. Jamsheed Choksy, Huffington Post, Iran, Protest, and Intelligence: Why Strategic Reports Often Get it Wrong, 22 July 2009, accessed at http://www.huffingtonpost.com/jamsheed-k-choksy/iran-protest-and-intellig_b_243052.html.

8. Alex Crawford, Sky News "Terror Textbook: A Step-by-Step Guide to Jihad", 17 August 2009, accessed at http://news.sky.com/skynews/Home/World-News/Afghan-Terrorist-Training-Manual-Is-Step-By-Step-Guide-To-Jihad-Sky-News-Sees-Militant-Textbook/Article/200908315362664.

9. Ben Benavides, Online OSINT Quick Reference Handbook New Table of Contents

Ray Draeger is a retired Army Major and employee of Northrop Grumman. For comments please call (520) 533-4524 or email walter.draeger@us.army.mil

Cyberspace Challenges for the Army Intelligence Community

by Captain Brian Olson

"Cyber security is one of the most serious economic and national security challenges we will face in the 21st century... The battle in cyberspace is just beginning."

–Mr. Paul Kurtz, Member of the CSIS Commission on Cyber Security in Testimony to the House Permanent Select Committee on Intelligence

Introduction

Cyberspace is a powerful place. It is a virtual stream of ones and zeros that brings the world together like never before in history. People across the world have become dependent on its suite of services that guide commerce, share ideas, and broadcast media. The U.S. Army is no exception. Consider Army Knowledge Online (AKO) and all the content that is now provided through this cyberspace conduit to grasp how network dependent the Army has become. Defense business, from daily to strategic, depends on the reliability and security of cyberspace and Army networks. In such a connected environment, every aspect of the Army's exposure to cyberspace is now a potential weakness. Enemies no longer have to exploit firewalls, routers, and massive servers to have lasting and grave impacts on Army operations. One only needs to compromise a single user, a single computer, an Army issued blackberry, or a low-level network device to capture sensitive data and wreak havoc. This problem extends beyond the relative safety of internal Army networks themselves. With users of all types able to access something as dynamic as AKO, even the home systems of Soldiers and their families can be considered part of the extended Army enterprise. Further, the amount of content we extended to Soldiers at home is growing in capability and depth as the Army becomes more and more super-connected to cyberspace.

Our enemies are not ignorant of the situation, nor have they spared any efforts in exploiting it. The situation is precarious, and the Army is not currently equipped to deal with the complete nature of the theat. Enemies can attack and exploit at will in relative anonymity and safety at a distance. Thankfully, however, the enemy has become just as connected and network dependent as the Army. This "enemy" is not simply nation states or rogue hackers. Terrorist organizations of all flavors now use cyberspace to conduct media campaigns, communicate, and plan and coordinate lethal and non-lethal operations.

Given the scope and nature of the threat, and the totality of the problem; why has more not been done to address this grave issue? Almost certainly, senior Army leaders recognize the digital age in which the Army lives and the evolving expansion of the Army's exposure to cyberspace. This is not to say that *something* has not been done. Education initiatives have been spawned, the Army has an extended enterprise vulnerability response system, and there are myriads of Computer Emergency Response Teams and Network Operation Centers. Even the extended enterprise is given a degree of protection through the offering of free anti-virus and firewall solutions through customer relationships with private industry. The Army has focused much of its attention on plugging of the holes inside the Army and shielding it from the dangers of the wilds of cyberspace. These efforts have great merit, yet they are all defensive in nature.

While, the Army network defenders have engaged themselves from national level down to the tactical level, the Army Intelligence Community (IC) has yet to see this type of sweeping movement. The National Security Agency (NSA) remains, in a large part, the only bastion of the IC fully engaged in dealing with the cyber threat. NSA, chartered with strategic full spectrum Signals Intelligence responsibility for the U.S., was once the appropriate one stop shop for cyberspace issues when the characteristics of this medium were narrow in size and U.S. based targets were few.[1] Now, with cyber-targets in the U.S. being abundant and potentially devastating from both military and economic perspectives, more power and effort must be realized. Only recently (July 2008) did the Army establish the Army Network Warfare Battalion at Fort Meade, Maryland within the 704th Military

Intelligence Brigade.[2] It is also momentous that LTG Keith B. Alexander (current NSA director) is heir apparent to become the U.S. Cyber Czar and use an 8 billion dollar budget to engage on cyberspace issues for President Obama.[3] These events are indicative of the Army and Joint ICs coming to recognize the expanding and dynamic nature of threat. They are good forward-leaning endeavors, but they have yet to come to full fruition and may not for years.

The Void: Cyberspace and National Leadership

The fact that there exists little realized effort in the Army IC is not entirely its own fault, nor should the lion's share of the blame be placed there. The truth of the matter is that there has been very little, in terms of definitive legislation or executive directive, that has been forthcoming at the national level in the last eight years. In testimony in September of 2008 to the House Permanent Select Committee on Intelligence (HPSCI), three witnesses: Paul Kurtz, John Nagengast (members of the Center for Strategic and International Studies' Commission on Cyber Security), and Amit Yoran (former Director of the National Cyber Security Division) testified that the U.S. lacks a comprehensive cyber security strategy. They each also addressed the issue that the IC and the military faced unique challenges that will require national attention and new resources.[4] President Bush did establish the Comprehensive National Cyber Security Initiative, which was charted to develop the way ahead for and establish a national cyber security plan. This implicitly included developing the roles for the IC in cyberspace operations. However, in December 2008, The Center for Strategic and International Studies (CSIS) in its report, *Securing Cyberspace in the 44th Presidency*, stated that while this was a major step forward, it was not comprehensive and over secrecy greatly reduced its impacts.[5] Additionally, President Bush's administration issued a publication entitled *The National Strategy to Secure Cyberspace* where the word "intelligence" appears precisely 18 times (mostly in the description of titles such as Director of National Intelligence) and never truly addresses guidance for the IC. Sadly, even the Department of Defense did not have a unified definition of cyberspace or cyberspace operations until the middle of 2008.[6]

From a legislative perspective the HPSCI, to its credit, has been attempting to lead the way on intelligence cyberspace issues. The committee held hearings in 2008 on cyber security and the Fiscal Year 2009 Intelligence Authorization Act compels the President to submit to them recommendations for forming a new Comprehensive National Cyber Security Panel, chartered explicitly to address the issues faced by the IC on cyberspace.[7] Comments made recently by a HPSCI staff member indicate that modernization of the nation's cyberspace posture will be on the forefront of the committee's agenda.[8] Complementing the efforts of HPSCI, the House Committee on Homeland Security's Sub-committee on Emerging Threats CSIS report's findings are comprehensive, practical, and specifically address the issues that are facing the military with regards to the establishment of coherent and dynamic doctrine to face the cyberspace threat. Among the recommendations are the establishment of a government career path dedicated to the cyber arena, building effective partnerships with private industry, and increased government regulation in the virtual world.[9]

Despite the work of legislature, none of these efforts has yet been realized into effective change to help the Army IC (or for that matter the IC at large) to cope with the new reality of a dangerous and persistent cyberspace threat. In the absence of guidance from the national level and authorization for expansion in terms of manpower and dollars, all IC efforts to modernize to face this threat are forced to be done with the current level of forces and monetary resources. Amidst two wars, the modernization of standing conventional forces, and other competing national security priorities, this proves to be a daunting and significant problem. Furthermore, it will remain difficult for the Army and other members of the IC to answer more fundamental questions about their role in cyberspace in the absence of guidance.

For example, while the Army has taken upon itself to create a battalion dedicated to cyberspace challenges (the aforementioned Army Network Warfare Battalion), this does not mean that national leaders will charter the Army to be responsible for the conduct of its own full-spectrum cyberspace operations (even with respect to Army missions.) Void of such charter, how can the Army expect or demand the resources to meet these challenges? Should the

Army spend millions to posture and develop doctrine for intelligence operations national leaders do not intend for it to perform? To members of the Army the intuitive answer to these questions may be 'certainly the Army should perform cyberspace operations,' but what if the national leadership develops a separate cyber-force or agency chartered for full spectrum cyberspace operations? Then any significant internal investment in cyber operations now would be money poorly spent, presenting a tragic situation for senior Army Intelligence leaders with heavy cyber operations monetary commitments.

Leaning Forward: Tough Questions for the Army

Even if charted and resourced to answer this threat, the Army IC would have to answer questions about developing cyberspace into a career path, generating an effective cyber-force, and addressing whether current Intelligence doctrine provides adequate guidance for cyberspace. Beyond cyber-force specialists, as a second and third order effect, the Army would have to develop Soldier, warrant officer, and officer training for intelligence professional to utilize cyber based intelligence sources effectively. Thankfully, forward thinking leadership at the U.S. Army Intelligence Center (USAIC) at Fort Huachuca, Arizona, has already been addressing this complicated issue. In interviews and conversations with senior leaders, I found they are striving to create a glide path to make cyber aware leaders and convert cyber intelligence into one of the core disciplines of intelligence professionals from an all-source perspective. From developing informational classes to the development of a complete training and education apparatus, senior USAIC leadership and subordinates are spearheading significant efforts to answer the cyber threat questions for Army intelligence professionals. A general belief persists throughout USAIC leadership that even if the Army does not receive the resources to generate a large scale cyber-force, prudence demands that Army intelligence professionals grasp, at least, cyber derived intelligence and capabilities. These efforts appear dynamic and general enough to be integrated in the near term, with maturation coming in a few years if they become realized.[10]

In other corners of the Army IC, the general opinion appears to be that the cyberspace responsibility, while not currently fully funded, is inevitable; whether it be for the Army to have its own dedicated responsibility and/or provide forces for a much larger joint force. In conversations at intelligence conferences and other specialized forums, it is almost universally held that the Army needs to prepare itself through the sweeping modernization of training, doctrine, and redirection of resources (most critically in force generation) to address the threat.[11] While there appears to be consensus that *something* needs to be done, there seems to be little consensus on *how* these elements should be realized. This should come as no surprise, with the aforementioned competition of resources created by the numerous responsibilities faced by the Army IC in the War on Terror and the lack of a guiding national strategy to follow.

The contrast between the Army IC at large and USAIC leaders is one of scope and direction. USAIC's focus (and rightfully so) is the integration of cyberspace training throughout all intelligence professional ranks, whereas that at large community is addressing the development of highly specialized cyber intelligence Soldiers. These efforts are not mutually exclusive, nor should they be considered in competition with one another. They are mutually supportive and both equally critical. What good would be the resourcing of a highly specialized class of cyberspace intelligence professionals, if the greater community did not understand the fundamentals of cyberspace? USAIC's efforts also seem to be geared toward integrating cyberspace into the traditional intelligence process model of F3EAD (Find, Fix, Finish, Exploit, Assess, and Disseminate). This is entirely appropriate for general intelligence professionals consuming the fruits of cyberspace intelligence information. Work remains to be done, however, to discover if the F3EAD intelligence process is appropriate for single source cyberspace intelligence professionals.

This problem has indirectly received national recognition. Again referencing the testimony to the HPSCI in September 2008, Mr. Paul Kurtz addressed three critical issues faced by the IC via cyberspace–the technical nature of the threat, the problem of assigning attribution to activity, and the sheer scope of the problem. A simple summarization of his testimony is that the IC will have to discover how we protect American interests and properly at-

tribute enemy action to state or non-state actors in an environment where amazing technical depth will be required of Intelligence professionals, and enemies can hide in the faceless anonymity of cyberspace.[12] Each of these issues addresses intimidating concerns in the Find and Fix elements of F3EAD. Mr. John Nagengast also testified as to the issues with what should be the simplest of phases, Dissemination. He summarized that current law and classification guides would simply prevent many key individuals (including private industry) from being privy to the appropriate information in a timely fashion.[13] This poses serious problems in an environment when the time of discovery of attacks and final exploitation of these attacks can be measured in seconds and minutes. Furthermore, the Army will have to develop doctrine dynamic and general enough to meet the challenges of an environment that evolves continuously and at an exponential rate. These are only three of the numerous examples of the doctrinal and policy issues that will be faced by the Army in redefining itself to handle cyberspace threats.

Conclusion

The Army faces significant and fundamental issues to address in this new realm. The future presents a world more connected, a world where the Army and others share a volatile and vital medium. It is a world where the enemy cannot hide behind lines–but is everywhere and suddenly nowhere. The Army cannot operate or plan in a vacuum or, for that matter, in the void of a national directive on such a resource intensive problem. Without national leadership and a commitment to resources, the Army's response to the cyberspace threat will be slow–even though senior Army leaders already recognize the problems and are laying a framework to deal with the threat as best they can. Hopefully, through legislation and presidential leadership, the efforts of these forward thinking leaders in organizations such as USAIC, the Army Cryptologic Office, the Army Network Warfare Battalion, and LTG Alexander as cyber czar will fully be realized. The next Congress and President hold the future of cyberspace and America's role there in its hands–let us hope they are hands that recognize the criticality of the issue and respond with immediate action; lest our enemies gain more on their unprecedented and powerful advantage.

Endnotes

1. *NSA/CSS Mission*, at http://www.nsa.gov/about/mission/index.shtml, accessed December 2008.

2. "Army Activates Network Warfare Unit,*"ARMY.MIL,* 2 July 2008, accessed December 2008 at http://www.army.mil/-newsreleases/2008/07/02/10569-army-activates-network-warfare-unit/.

3. John Stokes, "Obama Administration to Form New Cyber War Doctrine," *The Spectator*, 23 December 2008, accessed December 2008 at at *Information Warfare Monitor* at http://www.army.mil/-newsreleases/2008/07/02/10569-army-activates-network-warfare-unit/.

4. U.S. House of Representatives, Permanent Select Committee on Intelligence, *Cyber Security*, 18 September 2008, accessed December 2008 at http://intelligence.house.gov/OpenHearings.aspx?Section=31.

5. James R. Langevin, et al., Center for Strategic and International Studies, "*Securing Cyberspace for the 44th Presidency,"* December, 2008.

6. Christopher J. Castelli, "Defense Department Adopts New Definition of 'Cyberspace,'" *Inside the Air Force*, 23 May 2008, accessed December 2008 at http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm.

7. H.R. 5959: Intelligence Authorization Act for Fiscal Year 2009, accessed at http://www.govtrack.us/congress/bill.xpd?bill=h110-5959.

8. These comments were made during an Army conference on Intelligence, and are re-enforced by the Committee's Chairman, Representative Silvestre Reyes, in public statements and indicators in law (i.e., the FY 2009 Intelligence Authorization Act). HPSCI's efforts do represent the most significant work done by national leadership, even considering the CSIS commission on Cyber Security for the 44th Presidency.

9. Langevin.

10. This assessment should not be construed as an official position of USAIC. It is an assessment made by myself, and only reflects the observations made in conversations with USAIC leadership (whether in formal interview or in forum style settings). The assessment also reflects my own knowledge of efforts being led within USAIC by senior and junior officers. I would like to add in this context, that USAIC's efforts appear to be the most mature and forward leading on the issue of cyberspace, given the current resource constrains placed on the Army IC imposed by the War on Terror priorities.

11. This assessment was made through the attendance of several intelligence conferences and through close work on the issues of cyberspace in a national context throughout 2008. The assessment should not be construed as an official Army IC position, and I am, in no way, a spokesperson for any Army Intelligence entity, these are strictly the Author's observations.

12. Testimony of Mr. Paul Kurtz to the House Permanent Select Committee on Intelligence, 19 September 2008

13. Testimony of Mr. John Nagengast to the House Permanent Select Committee on Intelligence, 19 September 2008

The Importance of Sleep for Intelligence Analysts

by Lieutenant Colonel Chris Tatarka

Introduction

Are you a good Intelligence Analyst? Read the scenario below. A pencil and paper can be used if desired. The only other requirement is that before you begin reading the scenario, you must hold your breath and not inhale or exhale during the test. *If you inhale or exhale before solving the problem, you have failed the test.*

> ***"Years ago, during a foreign war, a desert fort occupied by troops lay under siege. The fort was square in shape with 8 defensive positions, one at each corner and one in the middle of each side.***
>
> ***The fort commander, General Gregorie LeVangie, knew that the enemy would not charge as long as they could see 15 active defenders on each side, so with 40 troops under his command, he stationed 5 in each defensive position. When one of his men was wounded he arranged the rest so that the enemy could still see 15 on each side. How did he do this?***
>
> ***Further casualties occurred. Explain how, as each man falls, LeVangie could rearrange his troops around the fort to prevent a concerted attack. Reinforcement arrived just as the enemy was about to charge. How many active defenders did they find left?"***

(The answer is provided at the end of article.)

Most individuals attempting to solve the problem under the conditions listed above fail to do so. The reason for this is not based on the complexity of the problem, but rather the inability to overcome the biological need to breathe. Inevitably, as one attempts to solve the problem the need for oxygen becomes both psychologically and physiologically compelling such that one either gives up and breathes, or simply becomes unable to cognitively focus on the problem and either gives up or passes out–with the former being both more likely, and less emotional, than the latter.

Thankfully, no one is required to conduct analysis, or other types of Military Intelligence (MI) functions, in conditions where no oxygen is present. Unfortunately, however, being oxygen-starved is analogous to, and an excellent metaphor for, an equally worrisome physiological and psychological state experienced consistently by many MI professionals: chronic and/or acute sleep deprivation.

Sleep and the Army

The U.S. Army has long made the claim that it "owns the night".[1] Likewise, modern military operations have shown the need and importance of conducting continuous operations such that twenty four hour operations are a routine and normal part of our environment. These around-the-clock requirements, coupled with an Army culture which emphasizes stamina, selfless service, and physical fitness create an environment in which the need and requirement for the critical biological function of sleep is frequently minimized.

This means that for MI Soldiers in operational environments, at least some degree of sleep deprivation is almost inevitably the norm rather than the exception. Because of this fact, and the unbreakable link between sleep and cognitive functioning, it is inherently critical that intelligence professionals, whose success relies almost completely on their cognitive abilities and problem solving skills, understand the ramifications of sleep loss on their ability to process information and solve complex problems. Likewise, MI professionals must be able to prevent, or at least minimize, the effects of sleep loss.

What Constitutes Sleep Deprivation?

Sleep deprivation is a highly relative concept. Researchers suggest that even small amounts of sleep loss (such as one hour per night over many nights) have subtle mental impacts which appear to go unrecognized by the individual experiencing the loss.[2] Additional research suggests that if an average individual gets less than seven hours of sleep a night for a period of 3 to 4 days or longer, he or she will exhibit the effects of sleep loss. As Colonel (Retired) George Belenky, a former Army Researcher notes, "7-8 hours of sleep each night are *necessary* to sustain high levels of performance over days and weeks."[3] Therefore, *at least seven* hours of sleep in a twenty four hour period is likely to be a benchmark for MI professionals and leaders of organizations to utilize in assessing sleep requirements.

Unfortunately, most Soldiers in the Army strongly believe themselves to be those who do *not* require 7 to 8 hours of sleep per night and claim to be one of those who are immune from the general rule of getting this amount of sleep. However, while research has been unable to completely identify the exact percentages of individuals who can perform optimally with less than 7 to 8 hours of consistent sleep, recent research from the University of Pennsylvania suggests that less than 10 percent of the population can perform optimally with less than 7 to 8 hours of regular sleep.[4]

Despite the rule of thumb and a large volume of research concerning the importance of sleep and performance, Soldiers are still victims of a lack of sleep. A recent survey of a Division level G2 section in Operation Iraqi Freedom (OIF) 2009 highlights that many MI soldiers do not get enough sleep. Over 90 soldiers were presented a brief survey asking them to assess the amount of sleep they received on average over the previous three days. Across the deployed G2 section, soldiers reported an average of 5.71 hours average sleep per 24 hours. When asked if they found themselves falling asleep during duty hours, 43 percent claimed they did have difficulty staying awake. This brief and rather informal survey suggests that MI soldiers are clearly sleep deprived.

How many hours of sleep have you averaged the last 3 nights?

Rank	Average Hours of Sleep	Number of Participants
E1-E4	5.77	26
E5-E9	5.67	31
O1-O3	5.88	16
O4-O5	5.50	13
Warrant Officers	5.75	4

Do you find yourself falling asleep during the duty (in briefings, meetings, at your desk)?

Rank	% reporting falling asleep during duty
E1-E4	46%
E5-E9	26%
O1-O3	63%
O4-O5	54%
Warrant Officers	50%

Effects of Sleep Loss

Research from both civilian and military settings has yielded a wealth of information concerning the effects of sleep loss and deprivation of sleep. While, broadly speaking, the effects of sleep loss are intuitive (as it is well known that sleep deprivation causes a decrease in mental functioning), scientific findings suggest that effects of sleep deprivation are far more complex than "common sense" notions imply and impact on mental abilities in an equally complex manner. Therefore, determining the effects of not getting enough sleep is equally complex.

An important factor which must be addressed in any discussion concerning sleep loss and de-

privation for MI Soldiers is the well-established fact that sleep loss affects cognitive (mental) performance far greater than it does physical performance. That is, generally speaking, sleep loss does not hinder physical endurance or stamina nearly as severely as it does cognitive functioning.[5] Thus, even a significantly sleep deprived MI soldier can be expected to retain near normal levels of ability to conduct tasks involving physical strength, stamina, and even physical dexterity. For example, Army researchers have found that a soldier can shoot as tight of a "shot group" at a fixed target after 90 hours without sleep as he or she can when well rested. However, if shooting at "pop-up" targets on a firing range, this same soldier's performance drops to below 10 percent of normal, well-rested, ability.[6]

Likewise, most experienced Army Soldiers can attest to being able to conduct lengthy, difficult foot marches under conditions of sleep deprivation, but almost all Soldiers universally mention cognitively "droning" through them. This unequal distribution of effects between our physical and mental performance creates a paradox within our human biology such that while we are *physically* capable of completing tasks under conditions of sleep loss or deprivation, we are not nearly as mentally capable. In essence, this causes humans to tend to perceive themselves as feeling more alert and capable than they often are. Further, this can create over confidence in our ability to perform mentally and to "drive on" despite the potential for significant lapses in decision making and problem solving.

Research suggests that sleep deprivation or sleep loss affects a variety of specific cognitive functions to include such things as increased omissions when performing a task; reduced motivation to complete tasks; lapses in long term memory; deficits in attentiveness, and significant mood swings. For MI professionals, this degradation of cognitive functions impacts on overall problem solving skills and our ability to communicate ideas.

Sleep and Problem Solving

Most psychological models of human problem solving suggest that to complete a complex mental task such as intelligence analysis, the human brain must conduct, synchronize, and synthesize a variety of specific cognitive functions. For example, humans must be motivated to receive stimuli and be motivated to actually conduct some type of analysis. Likewise, we must attend to information being presented; utilize long term memory to develop hypotheses about the situation we are attempting to solve; creatively develop possible solutions, and cognitively test these possible solutions through some type of selection process. Lastly, we must be able to communicate our "solution" or act upon it in some manner.

Sleep loss has been shown to impact virtually every one of these specific cognitive processes. For example, motivation and attentiveness have both been shown to be negatively impacted while we are sleep deprived. This suggests our ability to receive information (much less process it) is reduced when we are sleep deprived. Likewise, long term memory, or at least the ability to produce items from our long term memory is also reduced.

These specific functional detriments under conditions of sleep deprivation, which are in and of themselves detrimental to the effectiveness of an analyst, are even more problematic when one considers the importance of all of these functions to problem solving.

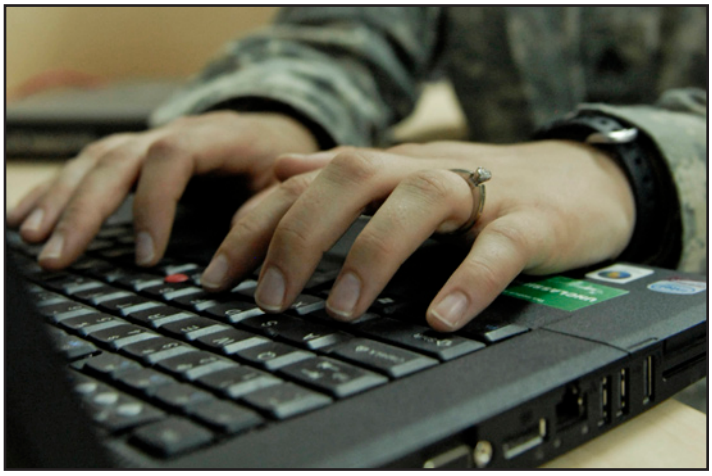
While sleep deprivation impacts a number of structures in the brain, for MI professionals the most important area impacted is the brain's frontal lobe which is associated with the ability to conduct novel and creative thinking. Research in laboratory and field settings suggest that when the frontal lobe is confronted with a lack of sleep, individuals tend to have difficulties thinking of imaginative ideas, a more difficult time reacting to unpredicted changes, and do not have the speed or creative abilities to cope with making logical decisions.[7]

The reduction in creativity is an area which sleep deprivation can cause catastrophic effects for MI professional. When facing sleep deprivation, an individual will still normally be able to react to a scenario but will usually choose a very unoriginal explanation or solution to the problem or situation presented. Likewise, individuals tend to anchor on the original solution regardless of new information and tend to become highly rigid in their thought processes and solutions. This inevitably means that old solutions continue to be applied to new analytical challenges with significantly negative outcomes.

For example, rather than take in the new information received from a Human Intelligence report or fuse the new intelligence with other "INTs" in a novel manner, the sleep deprived analyst is likely to either mentally miss the new information or anchor the information to an old assessment or analysis. So, unless the new data, information, or problem set serendipitously conforms to a previous solution or template, the cognitive effects described above will almost certainly lead to incorrect analysis. This adds to the dangerous problem of many analysts' inability to deny or alter their own previously created templates.

Sleep Deprivation and Communication

Because of its impacts on brain functioning, a second key area of concern for sleep-deprived MI professionals is the effect sleep deprivation has on speech and written communication skills. Researchers have found that sleep deprived individuals tend to have great difficulty expressing complex ideas and tend to become somewhat rigid in how they communicate in terms of word usage. For MI professionals, these research results suggest that when sleep deprived, we tend to have difficulty articulating our thoughts or ideas. Thus even if we have valuable intelligence or even raw data to pass on to a consumer of our analysis, we are likely to be highly ineffectual in doing so.



Similarly, when sleep deprived, research subjects who are tasked to read aloud children's books containing emotive expressions tend to read and speak in a highly monotone manner with little voice inflection. So, sleep deprived individuals tend to speak in a manner which is not likely to help convey important ideas. Ironically, this suggests that because of a lack of voice inflection or creative language usage by a sleep deprived MI analyst, the audience subjected to being briefed by this analyst may itself fall asleep.[8]

Overcoming the Effects of Sleep Deprivation

While the effects of sleep deprivation are exceedingly complex, the solution to the problem is relatively simple. Individuals need to sleep 7 to 8 hours during each twenty-four hour period to maintain optimal levels of cognitive functioning. This is a basic biological fact that research continually supports. The bottom line is that a failure to reach this level of sustained sleep will lead to reduced cognitive effectiveness over time. This also means that those who work in intelligence, who rely on the human brain as their primary "weapon system" require this level of sleep to perform at optimal levels.

Obviously, to maintain this level of sleep, the U.S. Army and its intelligence professionals (and the author) need to come to terms with this biological fact. To do this, the Army and MI must collectively revamp cultures to ones which place value on the importance of sleep. This can only be done through leadership and training.

The Army has long prided itself on the value and importance it places on leadership. To maximize the effectiveness of the MI Corps, leaders must make sleep happen within the ranks. Leaders at all levels must enforce sleep discipline through inspection, planning, and the basic leadership tenet of "setting the example." Leaders must conduct planning so that there are adequate sleep cycles built into operations and a plan for surges in operational periods. While not every MI soldier will get eight hours of sleep every night, leaders should know the level of fatigue of their personnel and manage this so that 7 to 8 consistent hours of sleep per Soldier per night is the standard, and only by critical operational exceptions is this violated. MI leaders must also set the example in this regard. While selfless service is one of the Army's values, a failure to take care of oneself is inconsistent with Army values of duty and mission. The cultural belief that sleep is for the weak is destructive to the effectiveness of the MI Corps.

The second critical element which must occur is proper training. MI professionals should be trained in how sleep loss impacts their ability to perform. MI units and professionals must ensure that unit

personnel are cross-trained in various functions and skills which can then allow for "battle handoff" for various intelligence missions and functions. This implies not only a need for resources (i.e., time and money) to be spent on cross-training, but also suggests the need to leaders to both train and empower subordinates to be able to take charge and make decisions in their absence.

This also implies the need for well-practiced and trained tactics, techniques, and procedures for "battle handoff" and shift change briefings between individuals. A novel approach from the civilian world involves registered nurses in hospitals who, during the one-on-one shift change brief with their counterpart, will often use voice recorders to make a record of the briefing that occurs between the outgoing and incoming nurse. This technique allows the incoming nurse to have both a voice and written record of critical items which occurred in the previous shift in the event there is a need to go back to find pertinent information. Lastly, as both a training and leadership measure, MI leaders at all levels should always establish "wake-up" criteria which make it very clear to subordinates when to wake up the appropriate leader or analyst in the event something occurs which requires that individual's presence.

Conclusion

While it is true that the U.S. Army "owns the night" it is clearly *untrue* that ownership of the night means we can somehow alter our inherent biological limitations regarding sleep. As noted earlier, MI analysis inherently requires the most optical conditions for mental process and cognitive functioning. Despite our cultural tendency to perceive sleep as a weakness, MI soldiers must have the discipline to get enough sleep, and as importantly ensure fellow analysts do the same.

Author's Note: *Perhaps the best source on the effects of sleep on performance in the U.S. Army is that done by Colonel (Ret.) George Belenky. Most of the material contained in this article is a result of conclusions drawn from articles, discussions, and second hand sources related to his work on sleep and performance for the U.S. Army. Additional reading can also be found at the Walter Read Army Institute Website at http://wrair-www.army.mil/.*

Endnotes

1. FM 3-06.11 Combined Arms Operations in Urban Terrain, 28 February 2002, B-8.

2. M. Suzanne Stevens, "*Normal Sleep, Sleep Physiology and Sleep Deprivation,*" October 2008 accessed 10 June 2009 at http://emedicine.medscape.com/article/1188226-overview.

3. Colonel Gregory Belenky, "*Sleep, Sleep Deprivation, and Human Performance in Continuous Operations," 1997 accessed* 17 June 2009 at http://www.usafa.edu/isme/JSCOPE97 /Belenky97/Belenky97.htm.

4. Jim Gorman, "*5 Sleep Myths Busted*," Men's Health Magazine, 2009 accessed 17 June 2009 at http://www.menshealth.com/

5. Belenky.

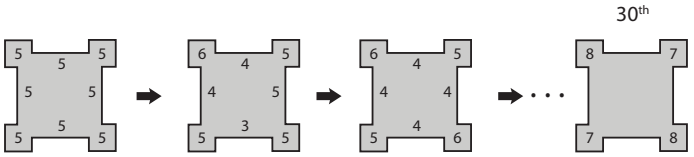
6. D.R. Haslam and P. Abraham, G. Belenky, ed., (1987) *Sleep Loss and Military Performance*, Contemporary Studies in Combat Psychiatry (New York: Greenwood Press, 1987), 165-184.

7. Sarah Ledoux, *"The Effects of Sleep Deprivation on Brain and Behavior,"* 2001 accessed 12 April 2009 at http://serendip.brynmawr.edu/exchange/node/1690 and Daniel DeNoon, *"Lack of Sleep Takes Toll on the Brain,"* WebMD, 9 February 2000 accessed 10 May 2009 at http://www.webmd.com/news/20000209/lack-of-sleep-takes-toll-on-brain-power.

8. Ledoux and Ellen Kahn-Green; Erica Lipizzi; Amy Conrad; Gary Kamimori, William Killgore, "Sleep Deprivation Adversely Affects Interpersonal Responses to Frustration," *Personality and Individual Differences*, Volume 41, Issue 8, December 2006. 1433-1443.

Word Problem Answer:

The analytical problem at the beginning of the article is from Saint Frances Xavier University in Canada at http://www.stfx.ca/special/mathproblems/grade11.html. See problem 47.



When the general jumps into the corner.

When the reinforcements arrive as the enemy is about to charge there are 29 active defenders left.

Lieutenant Colonel Chris Tatarka is a 1990 ROTC graduate of Gonzaga University. He has served in a number of Infantry, MI, and Information Operations assignments in the Regular Army and as an Active Duty Army National Guardsman. He holds a BA and MA in Psychology, an MA in Administration, and is currently a Doctoral Candidate for a PhD in Business Administration. LTC Tatarka is currently serving as G2, Multi-National Division-South in Operation Iraqi Freedom.

Intelligence Philatelic Vignettes

by Mark Sommer

A Forerunner to the Vietnam War

Sent from "Milano, Italy" on April 1, 1960, this nondescript aerogram from an agricultural machine manufacturer was addressed to "U.S.A. OPERATIONS MISSION to VIETNAM c/o American Embassy, S A I G O N (Vietnam)."

This was an early address for C.I.A. operations. It has a red crayon "CP" (possible censor marking), and was received on April 7, 1960, with a "RECEIVED CONTRACTS & GOVERNMENT OFFICE" stamping.

UK Intelligence Corps Unit–After the War

A 1948 example of correspondence between a British Intelligence Officer in Hong Kong to his wife back home in London.

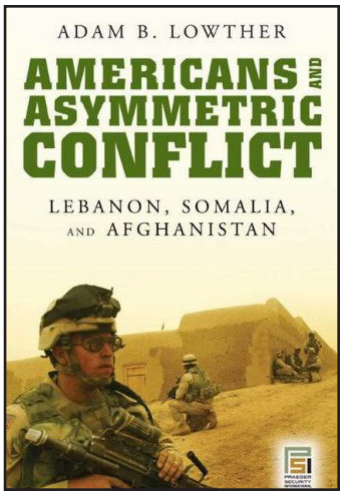
It was sent properly, with correct postage amounts, with a Hong Kong circular date stamp postmark and manuscript "Forces Mail" with blue oval cachet, "Field Security Section–Hong Kong," in lower left corner.

It is back stamped "HONG KONG 71 11AM"–with the same "Field Security Section–Hong Kong" cachet, and preprinted Intelligence Corps insignia on reverse envelope flap. These markings indicate that the letter was reviewed by a military censor.

Professional Reader

Americans and Asymmetric Conflict by Adam B. Lowther

(Praeger Security International, Westport, CT, 2007), 233 Pages, $75.00 ISBN-13: 978-0-275-99635-2



Asymmetric approaches to conflict are the focus of an increasingly large body of publications. This has been a positive development as U.S. Army doctrine seeks to improve the adaptability and flexibility of its intelligence gathering, dissemination, and tactical and strategic planning. The current Counterinsurgency (COIN) Field Manual (FM 3-24) has successfully addressed previous deficiencies in COIN doctrine and notable other works fill what was a dearth of 'big picture' views on current asymmetric warfare, COIN, and guerrilla warfare. One of these is Adam Lowther's *Americans and Asymmetric Conflict.*

Lowther focuses on gathering lessons learned from cases in which the American Military confronted asymmetric tactics in order to further develop a better understanding of how to flexibly counter such tactics in future conflict. The cases considered consist of chapters on U.S. involvement in Lebanon (1982-83), Somalia (1992-93), and Afghanistan (2001-present). These case studies provide the reader with short, but solid, historical overviews of each conflict; however, the analyses of the cases are relatively shallow. There is a preponderance of thought given to the strategic aspects of each scenario rather than a detailed analysis of the tactics utilized by U.S. Forces' adversaries.

It is notable that the development and the use of asymmetric tactics are entwined with strategic considerations. Importantly, distinctions in asymmetric warfare are complex but critical to clarify. For example, the author carefully distinguishes between guerrilla warfare and asymmetric warfare by pointing out that, "The grand strategy of the guerrilla seeks the overthrow of the current government and/or political system. The asymmetric fighter, however, generally seeks to force a change in his adversary's foreign policy." (Page 57) The specifics of asymmetric warfare usually entail strategic considerations which end up being a noticeable focus of the author's work, even though it is claimed that the book focuses on "drawing lessons at the tactical level and often saying little about higher levels of strategic analysis." (Preface, xi) A fundamental challenge of COIN is that the tactical and strategic are closely related. The intelligence a battalion S2 provides company commanders has potentially profound consequences at the international level.

The most worthwhile sections of *Americans and Asymmetric Conflict* are the first two chapters of the book. These two chapters articulate the historical development of warfare doctrine and lead to the types of asymmetric warfare exemplified in the follow on chapters that involved the U.S. in Lebanon, Somalia, and Afghanistan. The author successfully traces the growth of asymmetrical warfare in both eastern and western doctrine and the advantages and disadvantages of each. There is much in this historical account that may be of use to Soldiers who are already familiar with the 'greats' (Herodotus, Thucydides, Livy, Sun Tzu) and Napoleonic-era theoreticians Clausewitz and Jomini. For example, the 4 A.D. Roman Flavius Renatus Vegetius' work *Epitoma Rei Militaris* (*A Summary of Military Matters*) is given a solid look. Vegetius' work was a guide on how to use asymmetric warfare against the Roman Empire's more powerful enemies since, at that time the Roman Empire was in decline. In conclusion, since there is truly an endless amount to learn about asymmetric warfare, Adam Lowther's work is worthwhile, especially as a primer on this approach to conflict.

Reviewed by First Lieutenant Nathaniel L. Moir

CONTACT AND ARTICLE
Submission Information

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

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

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

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

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

What we need from you:

- **A release signed by your unit or organization's information and operations security officer/SSO stating that your article and any accompanying graphics and photos are unclassified, nonsensitive, and releasable in the public domain OR that the article and any accompanying graphics and photos are unclassified/FOUO (IAW AR 380-5 DA Information Security Program).** A sample security release format can be accessed at our website at https://icon.army.mil.
- A cover letter (either hard copy or electronic) with your work or home email addresses, telephone number, and a comment stating your desire to have your article published.
- Your article in Word. Do not use special document templates.
- A Public Affairs or any other release your installation or unit/agency may require. Please include that release(s) with your submission.
- Any pictures, graphics, crests, or logos which are relevant to your topic. We need complete captions (the Who, What, Where, When, Why, and How), photographer credits, and the author's name on photos. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg and note where they should appear in the article. PowerPoint (not in .tif or .jpg format) is acceptable for graphs, etc. Photos should be at 300 dpi.**
- The full name of each author in the byline and a short biography for each. The biography should include the author's current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications. Please indicate whether we can print your contact information, email address, and phone numbers with the biography.

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

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

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

Contact phone numbers: Commercial 520.538.0956 DSN 879.0956.

3d Military Intelligence Center

The 3d Military Intelligence (MI) Center traces its lineage back to the U.S. Army Intelligence Threat and Analysis Center, commonly referred to as ITAC, which was organized in 1975. Effective 1 October 1977, ITAC was provisionally established by Headquarters, U.S. Army Intelligence and Security Command (INSCOM). It was created as a major subordinate command of INSCOM and was collocated with the Defense Intelligence Agency at Arlington Hall Station. On 30 April 1985, ITAC was placed under the control of the Army Intelligence Agency until April 1991, when it was again placed under INSCOM.

In 1995, ITAC was realigned as the Training and Contingency Directorate of the National Ground Intelligence Center (NGIC). During this time, the 3d MI Center, located at Fort Shafter, Hawaii, had been deactivated and its colors retired for three years.

On 16 October 2001, ITAC, now under the colors of the 3d MI Center, was formed into the Imagery Assessments Directorate of NGIC, and subsequently, the 3d MI Center was re-activated at the Washington Navy Yard, Washington, D.C. Over the last eight years the directorate underwent several name changes, first to the Imagery and MASINT Assessments Directorate and later to the Geospatial Intelligence Directorate, as it remains today.

Since its origins in ITAC, the 3d MI Center has provided Geospatial Intelligence (GEOINT) in support of all the major U.S. campaigns. Combat operations supported over the last 20 years include Operations Just Cause (Panama), Desert Storm (Kuwait), Uphold Democracy (Haiti), Restore Hope (Somalia), Support Hope (Rwanda), Joint Endeavor (Bosnia), Allied Force (Kosovo), Enduring Freedom (Afghanistan), and Iraqi Freedom (Iraq).

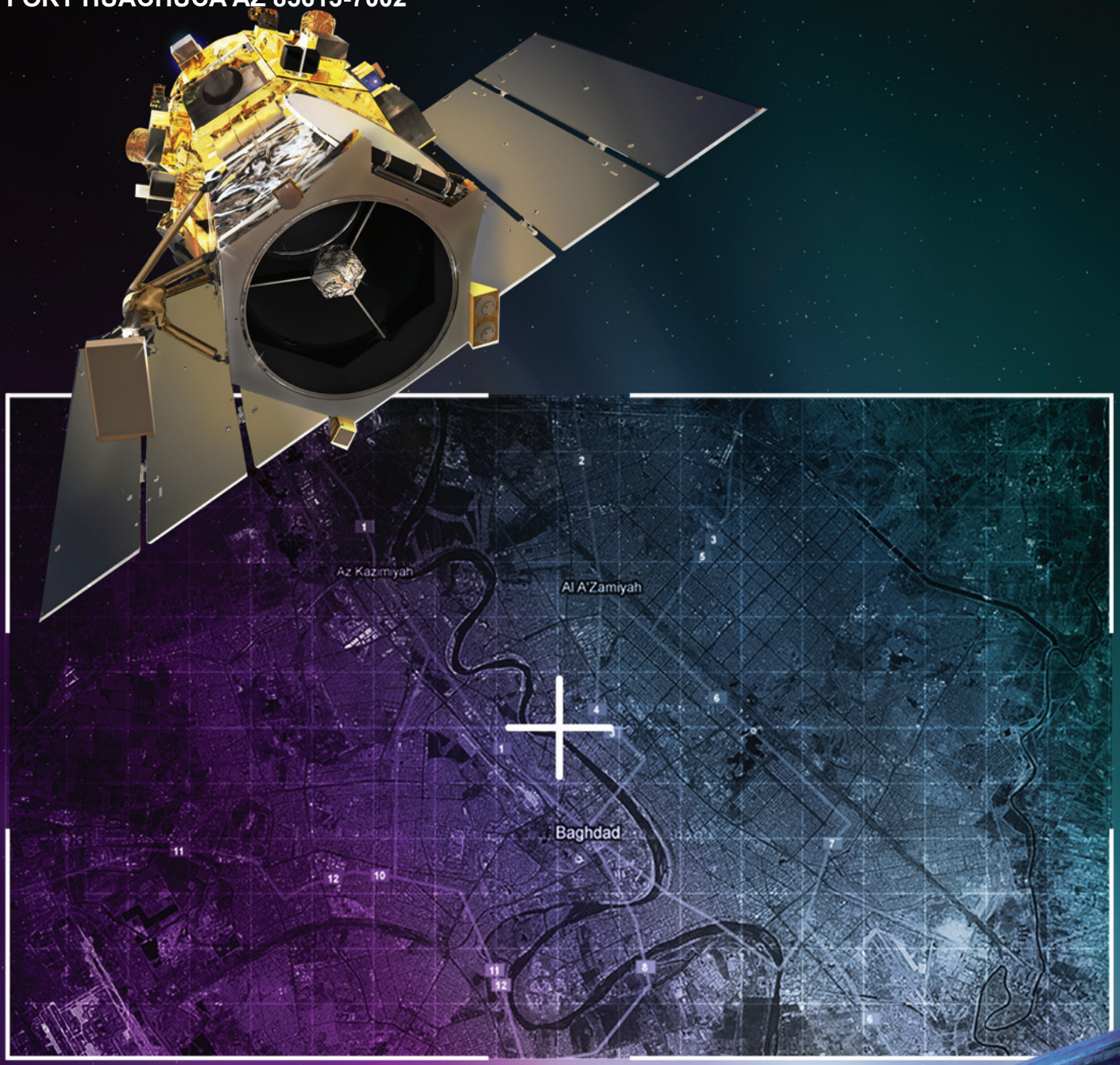
The 3d MI Center's mission is to conduct GEOINT operations in support of Army, Joint, and Coalition full-spectrum operations and contingency planning, and lead GEOINT sustainment training to the Army under INSCOM Foundry Program.

As the Army's only GEOINT battalion, the 3d MI Center continues to support all Combatant Commands with GEOINT production and training, to include focused support to Operations Enduring Freedom and Iraqi Freedom. It is INSCOM's lead for GEOINT Foundry and trains five separate GEOINT related courses: Imagery Orientation Course, GEOINT Production Course, Advanced GEOINT Production Course, Tactical Full Motion Video Production Course, and Global Broadcast Service System Users Course, training more than 200 Soldiers a year on site in the Washington Navy Yard. The 3d MI Center also conducts four Mobile Training Team engagements focusing on Leadership, Analysis, Equipment, and Exercise Support, reaching every unit deploying in support of Operations Enduring Freedom and Iraqi Freedom and training over 500 Soldiers per year at deploying units' home stations.

The 3d MI Center produces Imagery derived products in large numbers for deployed units around the world, supporting standing GEOINT targeting requirements, providing answers to specific requests for information, and assuming Imagery Exploitation for Multi-National Force Iraq's CACE during their Reliefs in Place/Transfers of Authority.

EYES ON THE WORLD!

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: 085852-000