# MIPB

Military Intelligence Professional Bulletin
July - September 2011                    PB 34-11-3

## Enabling Intelligence Analysis
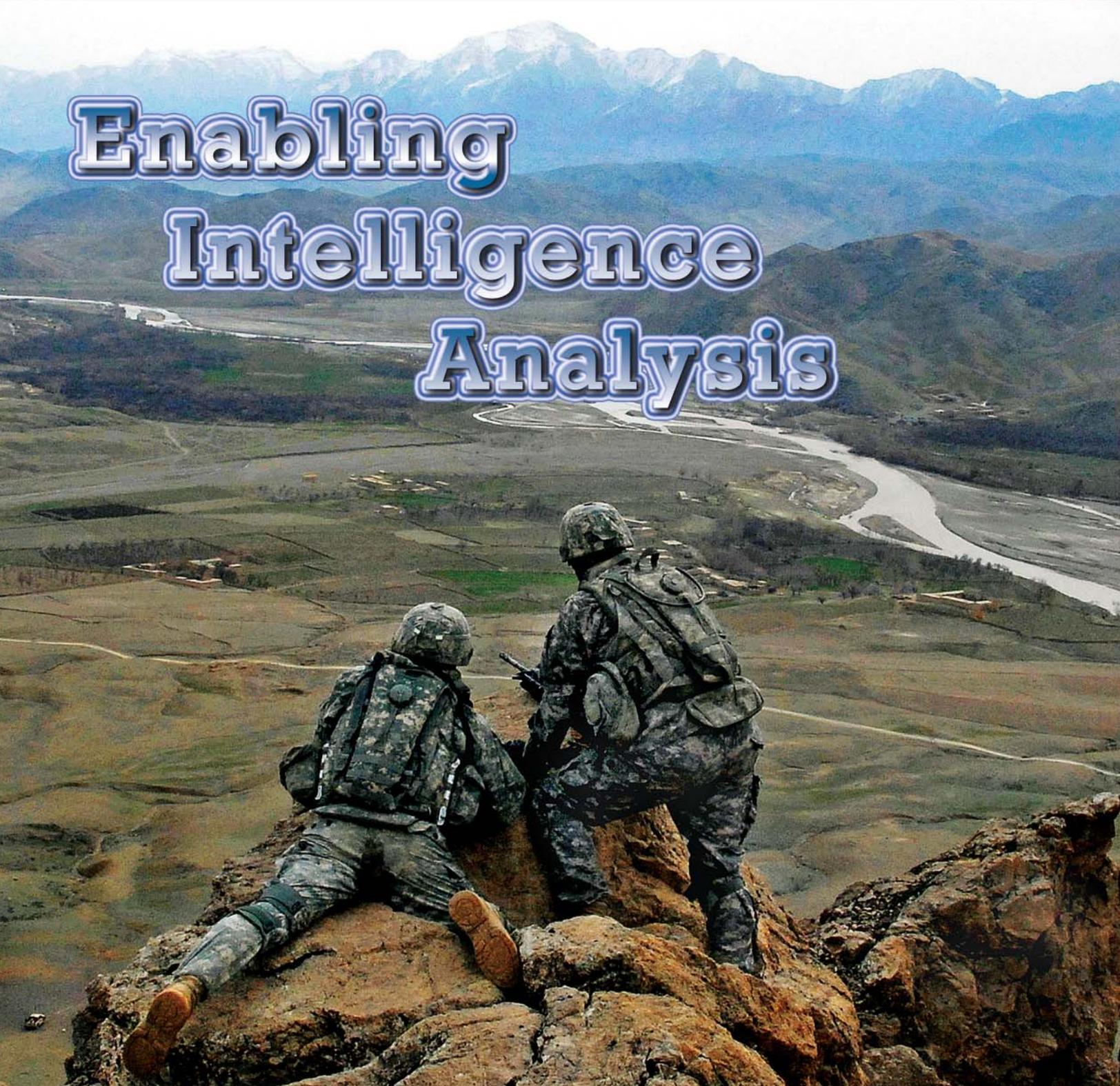
# FROM THE EDITOR

This issue features articles discussing various perspectives and methods and processes for enabling intelligence analysis. From the modeling and simulation arena, the U.S. Army Materiel Systems Analysis Activity (AMSAA) describes developments in its intelligence, reconnaissance, and surveillance (ISR) modeling tools and discusses AMSAA's current and planned contributions toward improved modeling with the MI domain.

From Fort Huachuca, the TRADOC Capability Manager Biometrics and Forensics Team (TCM-BF) reports on developments in virtual environment based training to fill the gaps in pre-deployment training in biometrics and forensics. From TCM Intelligence Sensors we learn about the Joint Direct Support Airborne ISR initiative which will place these assets in direct support of tactical operations at the brigade combat team level.

Several authors discuss methods, based on personal experience, to include the Human Terrain (in all its many variations) in the intelligence preparation of the battlefield and offer templates and processes for refining, analyzing, and reporting intelligence gleaned in this arena.

Two authors discuss the need to get back to the "intel" basics of developing an "analytical framework" and the need for critical thinking in intelligence analysis from thought provoking perspectives. With an eye to the future, we are offered some thoughts on developing a framework with which to create conditions for reconciliation, education, and ecomomic growth in Afghanistan.

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

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

| | |
|---|---|
| January March 2012 | Special Issue |
| April June 2012 | S: 30 January 2012 |
| July September 2012 | Commemorative Issue MI Branch |
| October December 2012 | S: 30 August 2012 |
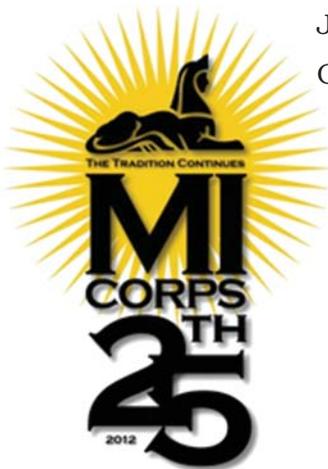
*Sterilla A. Smith*

Sterilla A. Smith
Editor

# MILITARY INTELLIGENCE

**July - September 2011**        **Volume 37 Number 3**        **PB 34-11-3**

## FEATURES

## Departments

# ALWAYS OUT FRONT

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

## Leading the MI Force of 2020

*Engaging Your Subordinates–Coaching, Teaching, and Mentoring*

As we move to the Army of 2020, we in the MI Corps must more effectively coach, teach and mentor our Soldiers and leaders. I often hear about the lack of mentors and professional development within the MI Corps. General Cone, Commanding General of the U.S. Army Training and Doctrine Command, surfaced a similar Army-wide concern during the recent Maneuver Warfighter Symposium. So I challenge everyone across our branch to help address this shortfall; every leader is a teacher and coach as well as a potential mentor to a subordinate. Engaging your subordinates in face to face dialogue, in order to professionally develop them is vital and applies to all of you: officers, warrant officers, NCOs, junior enlisted, and Army civilians.

Throughout history, mentorship has contributed to the development of some of the most influential American military leaders. General Marshall studied under Pershing, Eisenhower under MacArthur, and MacArthur under his own father. Today, leaders continue to help talented young leaders realize their full potential. In my current position I take considerable effort and pleasure in engaging our young leaders on their future and the future of MI. A few minutes of your time means the world to someone struggling with self-improvement, professional development, or a career decision.

We often use counseling, professional development and mentoring interchangeably. I believe a mentor is a leader, usually outside the chain of command, who has an informal relationship with a subordinate for the purpose of professional development. I believe mentorship is a critical part of a leader's development. It is one way we prepare leaders for the uncertainties of combat and the complexities of positions of higher authority. Mentorship improves our profession and strengthens our competitive edge. It is more than charting a career path; it helps strengthen competence, values, and our ethos.

Army Field Manual 6-22, Army Leadership, is a sound doctrinal publication that addresses mentors and mentorship. I encourage everyone to read Chapter 8. The manual places the responsibility for finding a mentor on the subordinate's shoulders. However, mentorship really starts with leaders engaging and communicating with their subordinates. While the relationship can vary from informal advice through a very structured relationship, mentorship is about honest two-way communication. Leaders must know the desires, strengths and weaknesses of subordinates. The goal is to provide everyone the advice they need, even if it is not always what they want to hear. Everyone deserves an opportunity to reach their full potential. Leaders should seek opportunities to mentor subordinates.

While everyone deserves the opportunity to have a mentor, not everyone will have a formal and long-term mentor relationship. The mentoring relationship can be intensely personal; therefore, it must be built on mutual trust. Young leaders need our help in discovering the various roadmaps to success. Your time and sincerity is essential to building a strong mentoring relationship

We all must continually strive to improve our coaching, teaching, and mentoring of our subordinates. It all begins with knowing your subordinates and face to face dialogue. Mentorship is not about replicating your own success; it is a two-way exchange involving a balance of tact, candor, and respect.

The Army's culture is one of selfless service, and young leaders deserve our help. We must perpetuate professionalism and excellence within the intelligence community. As leaders, one of the most important aspects of what we do is to help others realize their own potential and support their long-term success. If we call ourselves professionals, we must take an interest in those we serve. Please take the time to reach out and become involved with your subordinates—be a teacher, coach, and a mentor. ✳

### Always Out Front!
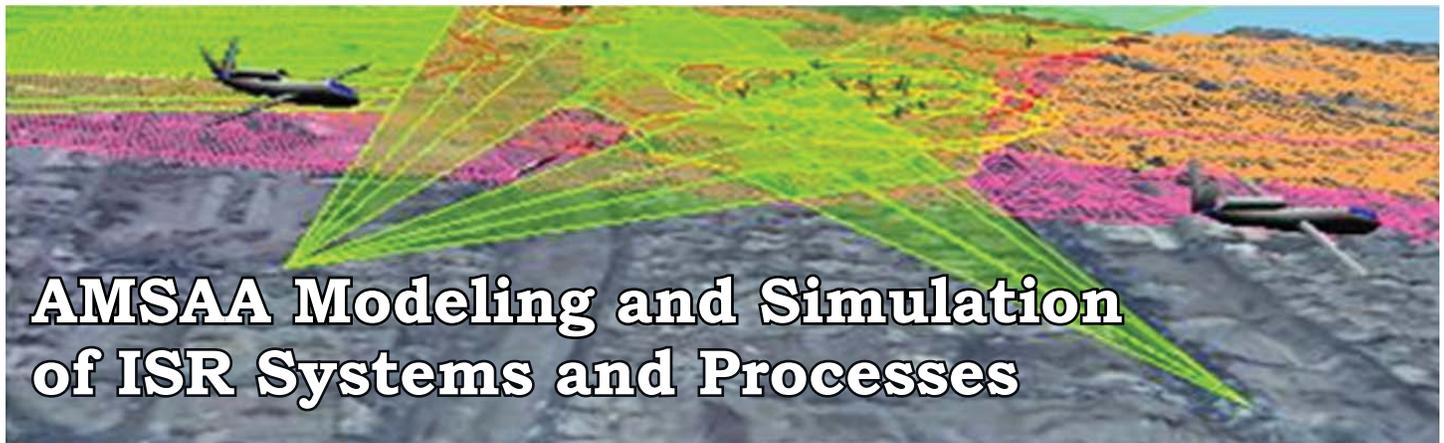
# AMSAA Modeling and Simulation of ISR Systems and Processes

by Ms. Elizabeth A Jones, Mr. Stephen L. Colegrove, and Stephen B. Chaney, PhD

## Introduction

One certainty in current and future operational environments is that the fluid nature of the threat; the global availability of low cost technology, and the continuous advances in wireless telecommunications will present increasingly difficult challenges to intelligence professionals. Relatively sparse military Intelligence, Surveillance, and Reconnaissance (ISR) assets play a key role in defeating such elusive threats, thus the ability to improve the performance of these assets while optimizing their utilization is essential to the defeat of future threats. The U.S. Army Materiel Systems Analysis Activity (AMSAA) has created Modeling and Simulation (M&S) tools that enable robust analyses on ISR performance and asset optimization.

In this article, we will describe one of AMSAA's ISR modeling tools and discuss some of AMSAA's current and planned contributions toward improved modeling within the domain of Military Intelligence (MI). Specifically, we will discuss improvements concerning representations of Signals Intelligence (SIGINT) through the use of operational data, planned improvements to Human Intelligence (HUMINT), and tactical decision making processes within M&S.

## AMSAA Overview

For over forty years, AMSAA's independent and unbiased analysis has led to savings in materiel spending through reducing risk, increasing reliability, and improving effectiveness of equipment. AMSAA provides responsive analysis to support the equipping and sustainment of current and future Army forces with superior weapons and materiel systems. AMSAA provides analyses of military systems in order to aid decision makers as they acquire new capabilities for our Warfighters. The types of analysis performed range from logistical supply chain optimization to determining the correct mix of biometric intelligence collection capabilities.

In addition to performing analytical studies, AMSAA is the sole provider of certified systems performance data for all Army analytical studies. These data include sensor performance for ISR assets that are equipped with wide area surveillance (i.e., Radar, SIGINT, etc.) and Electro-Optical/InfraRed imaging sensors. The continual advance of sensor technologies requires AMSAA to research and update sensor information incessantly as well as to update predictive performance analyses using high fidelity M&S tools.

## Fusion Oriented C4ISR Utility Simulation (Focus)

One M&S tool developed and used by AMSAA for ISR studies is the Fusion Oriented C4ISR Utility Simulation (FOCUS) which represents individual dismounted Soldiers, air platforms, ground platforms, and their associated sensors. FOCUS models C4ISR processes with detailed models of sensor scanning and performance, terrain, weather, environmental features, man-made features, battlespace factors, improvised explosive devices, and organizational elements to simulate performance in an operational context. Sensors include thermal, visible, radar/SAR, image intensifier, video, SIGINT and other types of sensors. FOCUS has supported several Army and Joint studies including the SUAS ISR Mix Analysis and the Joint Cooperative Target Identification-Ground Analysis of Alternatives.

Recently completed work has provided opportunities to improve the modeling of SIGINT in FOCUS. These improvements include, but are not limited to, frequency spectrum and spatial scanning, lines of bearing processing, and physics based probability of detection versus range based on signal propagation through a detailed battle space. For specific systems, these models may be very high fidelity representations of both the performance of the system and the realistic employment of the system in a valid operational context. FOCUS supports the two methods to approximate path loss in a mixed urban/non-urban terrain. The methodology incorporates a set of physics-based algorithms accounting for free-space spreading, reflection, diffraction, surface-wave, troposphere-scatter, and atmospheric absorption to approximate the point-to-point median propagation loss between ground-based and air-borne transmitters and receivers. This implementation allows accurate representation of SIGINT performance in mixed complex terrain.

Within the FOCUS suite, density mapping fea-
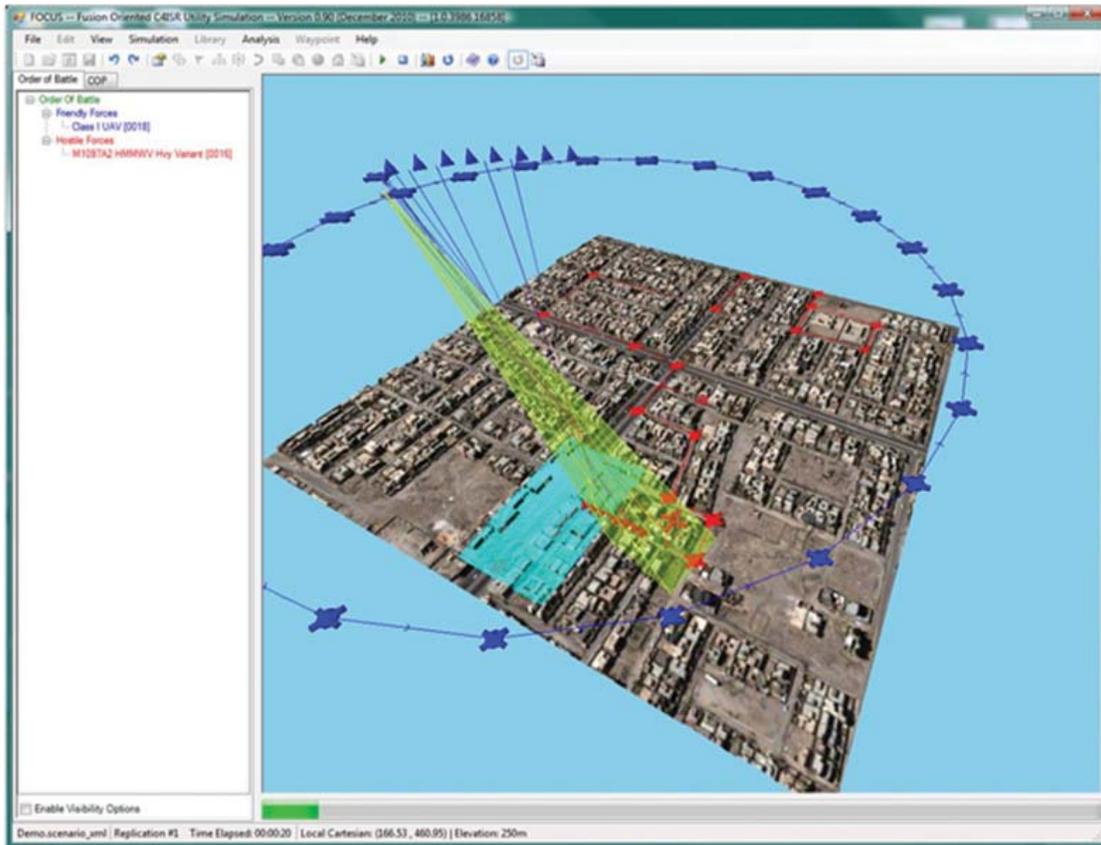


**Planning an ISR Mission in FOCUS**

scripting of many platforms, dismounts and associated sensors/emitters, while allowing multiple allegiances to exist between entities. The objective of a recently funded study used FOCUS to model current and/or future ground and airborne sensors acting in concert as part of a SIGINT sensor constellation. This included modeling improvements for the detection and tracking of radio frequency (RF) emitters in the context of Afghanistan's eastern and southern regions.

To improve upon predictions of SIGINT detection that use the one-way RF range equation, we implemented a weighted RF propagation path loss model in FOCUS. The model calculates a weighted sum of

tures effectively illustrate ISR coverage capabilities with the goal of optimization over a selected terrain region.

✦ **Line of sight (LOS) density map** demonstrates a flight pattern's ability to provide LOS observation to points on 3D terrain. This is displayed as an image that illustrates regions that are most susceptible to ISR coverage because of LOS, and also regions that are less accessible for a specified flight path(s).

✦ **Coverage analysis density map** allows the user to combine a platform, flight path, and one or more sensors to demonstrate ISR coverage of a

named area of interest. Custom options allow the user to filter the scan data by sensor and simulation time.

✦ **Detection/Time density map** illustrates the perceived target location based on all sensor detections over the course of a simulation throughout a terrain region. This feature allows the user to observe how effective an ISR network is at tracking the movements of a high value target over a defined geographical region. The analyst can vary ISR assets, flight patterns, and time on target to find the best configuration for tracking a specific target.

## SIGINT Modeling and Operational Data

Regardless of the improvements to the algorithms and concepts mentioned above, a model is only as good as its input data. The common phrase, "garbage in, garbage out," is 100 percent accurate when complex ISR systems involving hundreds of variables are evaluated using computer simulations. Thus, there is a need to ensure that the data used to generate results is accurate, complete, and predictive. The initial performance characteristics are derived from requirements and system specifications, but those idealized values are rarely sufficient to guarantee satisfactory system performance in an operational environment. Quality data based on real world performance that analysts can use to establish the validity of a model is needed to ensure that the model is accurate, robust and predictive. A model validated with proper input data can then be used to assess the performance of systems; optimize collection plans; perform after action reviews (AARs) of ISR missions; assess the effectiveness of systems; predict the effects of different capability mixes, and assist in training the future force of ISR collectors. Ongoing operations in theaters of war provide a unique source of experimental data in a relevant operational context.

Operational data contains many of the data elements necessary to characterize the performance of ISR systems for a given mission, in a given area of operations. Flight paths, collection activities, significant events, and mission results are often available; however, they are not collected by a single organization with the intent of providing complete data for post event analysis. Instead, they must be pieced together by operations research analysts and military advisors. This process is challenging and costly but the reward of having data that characterizes the true nature of ISR systems performance in a real world operations is invaluable to the ISR M&S community and should be to other intelligence professionals also.

Recently, a first-of-a-kind experimental data collection occurred when the Army Test and Evaluation Command (ATEC) was tasked to evaluate the effectiveness of Task Force Observe, Detect, Identify, and Neutralize (ODIN)-Afghanistan (TFO-A). ATEC delegated this task to the Army Evaluation Center and later AMSAA was identified to lead the analysis and assessment of TFO-A SIGINT systems. Data was collected, stored, managed, analyzed, and reported via CONUS SIPRNET and other sources with the help from Night Vision and Electronic Sensors Directorate. The data provides a look across the full spectrum of warfare from Afghanistan as it directly relates to TFO-A. This assessment occurred during October 2010 and emerging results have been shared with some members of the intelligence community already, with a formal capabilities and limitations expected to be released by ATEC by this article's release.

For those unfamiliar with ODIN, TFO-A is currently a battalion sized support element composed of Active Duty Army, Army Reserve, National Guard, DA Civilians, and contractors that manage and operate a constellation of manned and unmanned airborne intelligence platforms to provide direct support to Warfighters. It is an amorphous and fluid unit that fields new and sometimes experimental ISR equipment as dictated by the Army. Not only do the materiel systems constantly change, so does the command and control of the organization as it is spread across the complex battle space that exists in Afghanistan. Determining the effectiveness of such a family of systems is challenging to say the least, but analysis of the full spectrum data provides the system performance and system utility information necessary to determine the effectiveness of ODIN. System performance is the day to day tasking, collection, processing, exploitation, and dissemination characteristics. It is synonymous with measures of performance.

System utility is determined by the perception that a consumer has about the ability of a system to perform a specific task and is qualitative.

System utility is essentially a measure of effectiveness (MOE). These data are crucial to the validation of ISR modeling. Because there is a lack of SIGINT performance data available in the form of requirements and specifications or test data collected in an operational environment, these data are in some cases the only information we have to support our modeling tools.

So, how can the use of operational data create more effective M&S tools? As stated earlier, the first step is to take existing models and test them against this data. Once completed, the options to predict the performance of systems, optimize collection plans, execute AARs of ISR missions, assess the effectiveness of systems, determine capability mixes, and assist in training the future force of ISR collectors can be explored.

The performance of SIGINT sensors in operations presents a unique challenge for M&S. While there are a few tools available that claim to provide high fidelity representations of real time SIGINT, these tools often focus on engineering level design of sensors or training and thus either assist with detailed sensor design considerations, or illustrate lessons learned. Such tools do not address the questions that a decision maker may have about the effectiveness of a system-of-systems. FOCUS provides the capability to fly multi-intelligence platforms in a virtual, high fidelity, irregular warfare environment with threat courses of action (COAs) and activities to determine the throughput of intelligence collection. This gaming includes the cueing of sensors and can account for Processing, Exploitation, and Dissemination (PED) processes, thereby improving the odds that simulation results more closely match reality. This allows performance estimates to be made for theoretical platforms and hypothetical scenarios while operational data provides the basis for the validation of those results. In addition, these performance estimates can be used to develop robust test plans for new ISR systems.

AMSAA is also using M&S to examine the optimization of ISR assets in an irregular warfare environment. Given a fixed number of collectors and a defined area of interest for the SIGINT collector, a collection plan can be designed to provide the optimal coverage of that area. Again, the effects of sensor cross-cueing and PED cycles can be included in this analysis. Potential what-if questions might

include: What is gained by changing the receiver sensitivity? Or what if the trajectory of the platform flight path is altered? How do those changes affect the performance of a specified sensor or the value of the intelligence that is collected? There are an endless number of situations and variables that can be manipulated to test performance. Instead of relying solely on the experience of operators and collectors to provide estimates based on experience, the analysis of operational data has provided estimates for times related with PED and cross-cueing as well as ranges of movement for insurgents and targeting cycle timelines.

AMSAA has recreated a few TFO-A missions within the FOCUS model. To date, this has been done to assist in analyzing the effectiveness of TFO-A SIGINT processes. The potential for this process to serve as a method for a unique ISR AAR is high, but this has not been utilized by any MI units so far. Perhaps this is already being done with another tool or is unnecessary, but it is more likely that the military intelligence (MI) community does not know this capability exists.

Models utilizing operational data have the highest potential to improve the training of soldiers in the collection and integration of SIGINT at the tactical levels. Through M&S the environment can be altered, the performance of systems changed, and the trainees skill set can be properly tested and evaluated. Using M&S, every metric of system performance can be tracked. Operational data streams can be used as message traffic, cueing events, target descriptions, communications interruptions, video losses, signal losses and clutter. This technique offers the trainee a realistic environment and would adhere to the paradigm to "train as we fight." Furthermore, the soldiers in training can provide direct feedback on the MOEs for the system.

As AMSAA continues to press forward on the accurate modeling of MI systems, we are in need of requirements, system specifications, and operational sensor performance data for all ISR sensors and platforms. We are actively engaging the Army G2, U.S. Army Intelligence Center of Excellence (USAICoE), M&S labs, and other organizations to begin the process of consolidating Army ISR systems information at AMSAA. **Readers of this article are strongly encouraged to push ISR data to AMSAA.**

AMSAA's mission is to store, organize, validate, and share this data; however, we are reliant upon the broader intelligence community being aware of and recognizing this need to share. The use of operational data greatly enhances the ability of M&S to predict the performance of systems, optimize collection plans, execute AARs of ISR missions, assess the effectiveness of systems, determine capability mixes, and assist in training the future force of ISR collectors.

## Future HUMINT Modeling

The next step that AMSAA is taking towards relevant M&S in intelligence is contributing to the challenging problems of modeling HUMINT and human cognition. In the current asymmetric fight, HUMINT is often the sole source of information that permits discovery of threat networks, key personnel, roles, funding streams, planned operations, and campaigns. However, in the analysis domain, M&S tools often ignore HUMINT while focusing on the more easily represented materiel systems–sensor systems and platforms that often play a limited role in the intelligence process during irregular warfare. In the future, we would like to create realistic modeling of the HUMINT collection and dissemination processes and to implement this into an existing holistic ISR simulation: the FOCUS model. We are currently funded to model collectors, sources, and the process of intelligence flow on real world intelligence flow at the levels of brigade and below. This effort will utilize previous studies, especially "Ambiguity and HUMINT Methodology Development," a technical report released in 2006 by the TRADOC Analysis Center under sponsorship from the Army G2, with assistance from AMSAA.

A collector in the M&S sense is not exclusively the specifically certified and trained HUMINT collector defined in FM 34-52; it is any element of the force structure that initiates or participates in collection efforts. This could be unit commanders during operational planning, designated HUMINT collectors (e.g., MOS 97E, 351M/E, 351Y/C, 35E/F), but also MOS 11B, 19D, 31B, 97B and any other Soldiers performing routine duties that place them in contact with sources, as well as other civilian personnel acting to develop intelligence networks to facilitate national security objectives. Collectors initiate the process of collection, interact with sources, and report information to other intelligence nodes that eventually report information to military reporting channels.

Actual information comes from another class of entities–sources. Sources are any entities in contact with organizations, persons, or information of interest to the collector. There are many examples of potential sources: friendly soldiers conducting presence patrols, refugees, detainees, diplomatic reporting channels, cultivated local sources, paid anonymous sources, official contacts with host nation government personnel, key members of non-government organizations, media, and so forth. Sources are modeled as repositories of information, of varying accuracy, with dynamic attributes such as motivations, intent, and willingness to cooperate with the collector. Sources should be capable of providing intentionally deceptive information, of being amenable to a particular collection approach but not another, and of becoming more or less cooperative over time based on changing allegiances, events, and actions of collector(s) or other entities.

The process by which intelligence is processed and disseminated throughout the battle-space must also be explicitly represented within the simulation in such a way that is both doctrinally correct, and which reflects current operational reality. This begins with the collection process itself, followed by reporting from the collector, to eventual dissemination to the tactical commander/maneuver element entities. It is our desire that this work be transferable to other Army M&S tools throughout the analysis and to the MI community. To ensure validity of the basic approach and transferability, development of HUMINT modeling representation will be performed in conjunction with, and based on previous guidance from USAICoE and Army G2.

## Future Decision Making Processes in FOCUS

Another key improvement area is the representation of decision making within the M&S environment. In the domain of tactical decision making, there are two areas that clearly have a major impact on outcomes, but which have received little attention in M&S efforts to date.

The first of these areas is the human cognitive ability to fuse complex information. At the levels of brigade and below this can occur in a number of situations. For example, when an entity report

is generated, both the intelligence elements of the command staff, and often the maneuver elements themselves, interpret that entity report. These interpretations occur in the context of other entity reports, perception of force disposition, unit mission, perception of threat COA, and other factors in the battle-space environment. By fusing information and contextual cues, they take an informed action that is based on a complex understanding of both their unit's mission and the adapting threat. AMSAA intends to begin modeling this process by comparing timelines, accuracies, and target location errors of perceived target locations to ground truth associations produced by human cognition for simple sets of entity reports. Over time, additional sources of data and more complex behavioral responses will be added in an attempt to more properly represent the human fusion of information.

The second area in decision making is a force multiplier that is not typically modeled explicitly; the function and effect of the command staff at the tactical level. Specifically we would like to focus on the effects of COA development and warfighting functions (WFF) synchronization, since this drastically multiplies the combat effectiveness of a unit. In addition, this process gives the tactical unit the ability to effectively allocate ISR assets in order to adapt to threat behavior and successfully accomplish their mission. We propose to create a simulation architecture that represents staff actions, including representation of Intelligence Preparation of the Battlefield, mission analysis, COA refinement, Priority Intelligence Requirement definition, WFF support, mission branches and sequels, and collection requirements and satisfaction.

## Conclusion

AMSAA provides responsive analysis to support the equipping and sustaining of current and future Army forces with superior weapons and materiel systems. Progress has been made in making SIGINT modeling more relevant and AMSAA is working diligently to improve the representations of HUMINT and decision making processes. These are difficult tasks that we aim to tackle in the next decade, however to accomplish these advances we will require data and assistance from many organizations, especially the intelligence community. AMSAA is contributing and will continue to contribute to the MI community through performance predictions, data creation and M&S tools that enable robust analyses on ISR performance and asset optimization.

**Bibliography**

TRADOC Analysis Center. Ambiguity and Human Intelligence (HUMINT) Methodology Development Final Report. 2006. TRAC-TR-06-003(R).

FM 2-22.3 Human Intelligence Collector Operations, September 2006.

Pernin, Christopher G., Moore, Louis R. and Comanor, Katherine. The Knowledge Matrix Approach to Intelligence Fusion. Santa Monica: RAND Corporation, 2007. As of May 6, 2011 at http://www.rand.org/pubs/technical_reports/TR416. TR-416-A, 2007.

FM 3-0 Operations, February 2008.

*Ms. Jones, USAMSAA, has served as an operations research analyst for eight years in a number of assignments in the ISR domain. She is currently serving as the team leader for the Intelligence and Fusion Team. She holds a BS in Mathematics from the University of Delaware and an MS in Applied and Computational Mathematics from Johns Hopkins University. She may be contacted at elizabeth.a.jones252.civ@mail.mil.*

*Mr. Colegrove, USAMSAA, has served as an operations research analyst for nine years in a number of ISR related assignments. He is currently the senior analyst on the Intelligence and Fusion Team. He holds a BS in Physics from Old Dominion University, and an MS in Neurosciences from Case Western Reserve University. He may be contacted at stephen.l.colegrove.civ@mail.mil.*

*Dr. Stephen B. Chaney, USAMSAA, has served as the SIGINT subject matter expert at AMSAA for the past two years. His current responsibilities include the analysis of ISR system payloads and research into the effectiveness of SIGINT systems. He holds a BS in Physics from Augusta State University, and a PhD in Physics from the University of Georgia. He may be contacted at stephen.b.chaney.civ@mail.mil.*
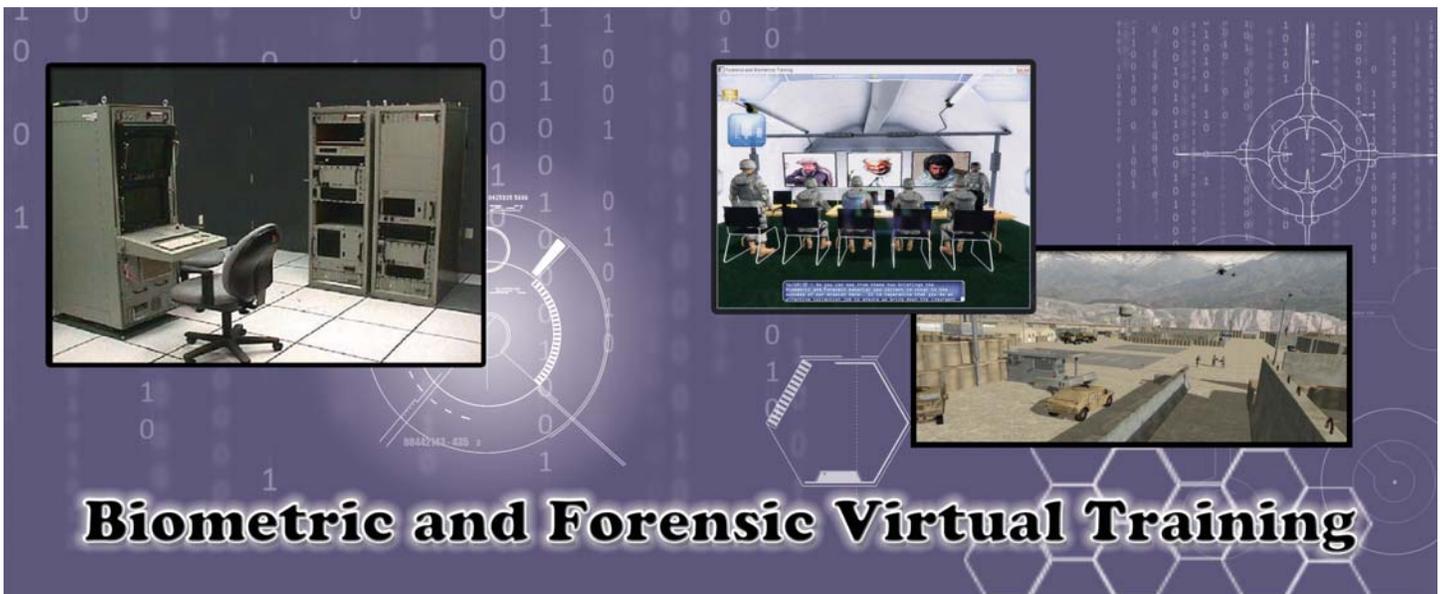
# Biometric and Forensic Virtual Training

## by the TRADOC Capability Manager Biometrics and Forensics Team

The high operations tempo experienced by today's military units has made a significant and lasting impact on initial and recurring training as commanders, evaluators, instructors, and operators struggle to find the time, materiel resources, and personnel to conduct quality Biometric and Forensic training. The problem is further compounded by the rapid introduction of new technologies, equipment, concepts of operations (CONOPS), and tactics, techniques, and procedures (TTPs) required to do battle with an elusive and evolving enemy.

Numerous studies including the 2010 Department of Defense (DOD) level Forensic Capabilities Based Assessment (CBA), the 2007 DOD Biometrics CBA, 2010 Site Exploitation DOTMLPF Assessment, ongoing Counter-Improvised Explosives Device (C-IED) Attack the Network assessment, and recent feedback from theaters of operations have exposed many gaps in pre-deployment and recurring Biometric and Forensic training, including leadership education, home station equipment for training, and an overall understanding of Biometric and Forensic capabilities across the Warfighters' spectrum.



Published U.S. Forces and Central Commands' directives require all deploying Warfighters receive training on Biometric and Forensics equipment, concepts, and procedures prior to deployment. Instruction conducted at home station by Biometric and Forensic mobile training teams (MTTs) and at combat training centers (CTC) currently provides the best pre-deployment training opportunities. However, the limited availability of MTT-based training coupled with the lack of home station equipment negatively impacts both the Army's ability to adequately train the majority of the Warfighters during the ARFORGEN cycle and our Warfighters' ability to sustain the rapidly perishable skill sets taught by the MTTs. To keep pace with changing enemy tactics, biometric and forensic technology advances, and battlefield-proven practices and lessons learned, units are squeezed as they try to "do more with less." That is why it is important to note that just as new technology is part of the challenge, it is also a big part of the solution.

Virtual environment based training is proving to be immensely effective in helping fill these gaps. It provides the Warfighter with the ability to train on collective, individual, and leader tasks for biometric and forensic virtual equipment and learn, practice, and hone the procedural concepts and latest TTPs at home station. This can be done either prior to a CTC rotation or as refresher/sustainment training, post deployment, following a CTC rotation, or as a part of recurring Mission Essential Task List training.

Army Learning Concept 2015 (ALC 2015) identified "tailored, outcome-oriented" learner-centric training and education as a more effective means of delivering quality training; this is a core characteristic of virtual training. The Army's current learning model, ALC 2015 notes "routinely assumes risk in the institutional Army in terms of personnel and equipment, but learning models have not adjusted to fit within these seemingly permanent constraints. Cumbersome training development policies and procedures cannot be supported with the number of training developers assigned or the skill sets available, resulting in outdated courses and workload backlogs." ALC 2015 goes on to point out, "Schoolhouses typically receive new equipment later than operational units and in insufficient quantities, yet alternative virtual training capabilities are slow to be adopted and there is a lack of connection to the Operational Army." These challenges are even more pronounced in a declining budgetary environment.

One way of meeting the challenge of operational adaptability identified by ALC 2015 is to "dramatically reduce or eliminate instructor-led slide presentation lectures and begin using a blended learning approach that incorporates virtual and constructive simulations, gaming technology, or other technology-delivered instruction." ALC 2015 also states the need for emerging virtual training capabilities that enable students to experience full spectrum challenges through a balanced mix of live, virtual, constructive, and gaming environments, providing the Army the "capacity to evaluate and integrate rapidly expanding learning technology capabilities to keep the learning system competitive and responsive. Adaptive learning, intelligent tutoring, virtual and augmented reality simulations, increased automation and ar-

tificial intelligence simulation, and massively multiplayer online games (MMOG), among others, will provide Soldiers with opportunities for engaging, relevant learning at any time and place."

The TRADOC Capability Manager Biometric and Forensic (TCM-BF), in collaboration with the Joint IED Defeat Organization (JIEDDO) and TCM Gaming, is leading the development of such cutting edge virtual training, overseeing the design and delivery of several unique virtual training tools to provide a current, accurate and adaptable cost-efficient Biometric and Forensic (BIO/FOR) training solution.

The key to the TCM-BF's success is a blended solution that incorporates cinematic visualization tools, interactive multimedia instruction (IMI) programs, and serious games technology; all developed using the commercial-off-the-shelf virtual environment engine Unity.

An avatar-driven animated video, the cinematic is especially useful for graphically illustrating CONOPS and complete mission sets. IMI programs are an effective means of teaching "buttonology"–for both hardware and software–providing the student detailed information on a system's capabilities and use and the ability to learn and practice on virtual replicas, negating the need for scarce equipment. Finally, serious games provide a fully interactive 3D training environment to teach TTPs and individual, collective and leader tasks in single and multi-player settings, making it an ideal method for learning procedures, critical thinking skills and coordinated, collaborative efforts.

This BIO/FOR virtual training package is being developed to be completely compliant with Army Gaming and Virtual standards, enabling the end product to meet required DOD specifications for training in a simulated environment. That, combined with the worldwide distribution of the virtual training programs either by CD/DVD or digitally via the web (MilGaming web portal), will provide the DoD the flexibility to train users on BIO/FOR equipment, concepts and TTPs anytime, anywhere. This training product can be used by active, reserve, National Guard and other Services to reduce the pre deployment training burdens (time and cost) for these units. Plans also include deploying this capability with U.S. Army gaming Virtual Battle Space 2 (VBS2) and USAICoE Learning Technology Directorate Learning Management System.

Since the start of Operations Iraqi and Enduring Freedom, BIO/FOR technology capabilities have rapidly made their way to the most forward edge of the battlefield as an exponential mission enabler. Attaining identity dominance plays a crucial role in an effective counterinsurgency mission by working to reduce and ultimately eliminate the anonymity an insurgency requires to conduct its operations. Properly training our Warfighters on the advanced equipment and evolving TTPs required to achieve this identity dominance is an enormous undertaking. Effective BIO/FOR virtual training allows users to train wherever they are, be it in a deployed location or at home station where scheduling conflicts often preclude the use of MTTs and relegates a unit to minimal exposure at a CTC 90 days before a deployment.

Through the proper development and implementation of advanced virtual training tools, users will experience BIO/FOR training in an immersive 3D training environment. Additionally, their performance data, including validation results, dates, courses, etc., will be tied to the user's log-in and digitally stored, providing the unit's training management on-demand real time situational awareness of all assigned Soldiers' training status and results.

TCM-BF has contracted Janus Research Group to construct this virtual training solution and environments that make use of a "crawl, walk, run" approach, providing students with concept familiarization, skills acquisition and practice, and embedded Checks on Learning (validation) to regularly demonstrate comprehension and retention of the course material.

Within the serious game, initial training is conducted on a virtual forward operating base that contains all lesson material and immerses Soldiers in an environment very similar to what they will encounter while deployed. Cinematics, first-person character game play and some IMI (to teach basic procedural equipment "buttonology") are blended to maximize the students' training outcomes. Key training areas within the virtual environment include a virtual MOUT Site, Tactical Operations Center training and mission, villages, and a Detention Center. From start to finish, Soldiers are led step by step by an avatar Instructor Character through all 20 modules to ensure every Soldier successfully completes each training sequence.

JANUS is developing the total package in increments, and has delivered several modules to the TCM-BF, including the Military Decision Making Process, Leader and Staff training, Mission Preparation Considerations, Post Mission Activities, Site Exploitation Kit, Exploitation Site Management, Biometrics Gathering, Building and Vehicle Search, Forensic Material Handling, IED Components, Document and Media Exploitation (overview), Cache Detection, and Home Made Explosives.
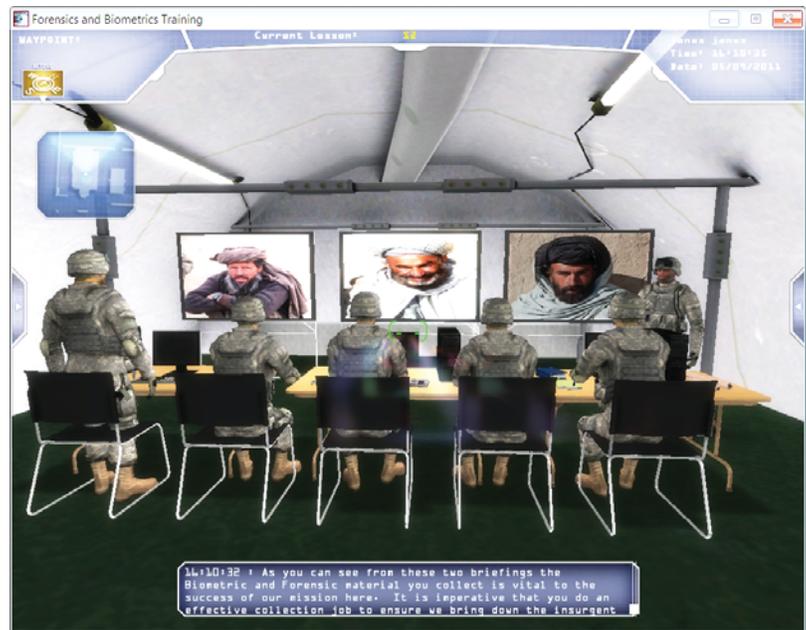


Other modules currently in development include but are not limited to: Targeting, Emerging

TTPs/Standard Operating Procedures, Emerging Technology, Enabler Integration and Equipment Operations, Last Tactical Mile, Biometrics and Forensics in Support of Security Operations, and Weapons Technical Intelligence Biometric and Forensic Enable Intelligence (BEI/FEI). All modules support the objective to attack and defeat networks that continue to attack U.S. and Coalition deployed forces.

requiring a team of trained Soldiers to properly execute their duties on the team in accordance with the BIO/FOR TTPs.

As the nation's pursuit of terrorist and insurgent organizations continues and expands worldwide, the Army's BIO/FOR training and deployment demands also grow, leaving its units with difficult obstacles that can be overcome through effective use of technology. The TCM-BF virtual environment



The Learning Events are individually playable and provide skill familiarization, acquisition and practice, while skill validation occurs within the embedded missions. However, before a student can embark on a mission, he/she must successfully complete all prerequisite lessons. Each mission is progressively more difficult than the last, and the game itself culminates in multi-player serious game-play exercise

based training delivers vital information in an effective manner in pre-deployment time constrained environments. This solution offers the benefits of being cost effective, highly capable, and widely distributable, empowering units to get through the challenges of equipment and funding shortages and instructor and student availability in today's high operations tempo environment.

# BACK TO BASICS: INTELLIGENCE FOR BEGINNERS

by Captain Trent Perkins

## Introduction

After interviewing numerous junior enlisted Soldiers and lieutenants coming out of the schoolhouse (as well as having gone through a few courses myself), I have become convinced that as an institution we have become so focused on teaching the "How to" that we have completely missed the "Why" of Military Intelligence (MI). It is my contention that spending a little bit more time developing an analytical framework or "hooks to hang hats on" *before* teaching all of the "hats" would result in a much better MI analyst, and thus, a much better intelligence product.

Doctrine is essentially a summary of what has been determined to be best practices developed over time–our collective MI 'tribal wisdom.' Unfortunately, it is so dry that most people never actually read it in the first place. It is taught in much of the same way as it is written, in a piecemeal fashion without proper context.[1] Doctrine is essentially a time tested way to "crack the nut" and as such is effective. However, I have spoken with students who do not have the foggiest idea of what the "nut" is, nor do they have a view of what might be the "big picture." As a result, they are unable to remember and use the simple concepts they were taught in the school house. Then again, the components of doctrine were presented in such a way that students did not realize that they *were* simple concepts.

I think we have jumped to the details too quickly before creating a sense of context. Discussing why Intelligence exists and how it is used in a unit's conduct of war would be extremely beneficial. I went through 11 months of training to become a 35T (MI Systems Maintainer/Integrator). After graduation, I spent a year in an MI company and still had no clue regarding what Intelligence actually was. One could say that I did not need to know, but I would contend that understanding the overall purpose for the equipment I was charged with maintaining would have been very beneficial. It would have required 30 minutes at the beginning of an 11 month long course to explain that the purpose of MI is to tell the Commander who the bad guy is, where the bad guy is, and what the bad guy is going to do next. It would not have been wasted time.

So with these thoughts in mind, here is an overview of MI and how it all works together. It is written for the young and uninitiated MI Soldier.

## The Staff

To put MI in context, a brief word about how a staff works for the Commander is in order. It is a given that there are more staff components at higher echelons, but I will stick to a battalion sized structure which covers the staffing basics. With that said, the basic principles discussed in this article generally apply to most echelons of intelligence although, as discussed later, the focus will change depending upon the size of the area for which your Commander is responsible.

The Commander is responsible for everything in the unit and has the ultimate say for everything the unit does. A lot of information needs to be processed in order to successfully accomplish the unit's mission so the Commander maintains a staff to assist him.

The S2 is the MI component of the staff and tells the Commander what he needs to know about the enemy situation. The S2 also presents the Commander with the various challenges that the environment will pose to his mission. The S3 (Operations) recommends to the Commander what should done about the enemy situation and manages the fight. The S1 (Personnel) tells the Commander how many Soldiers are available to accomplish the mission, and the S4 (Logistics) tells the Commander what other resources are currently available, what will be required in order to continue the fight, and when new resources will be available both to the commander and to subordinate units. The S6 (Communications) enables everyone to communicate with each other.

Beyond these primary functions is additional specialty staff. The Fire Support Officer (FSO) works closely with Operations, but also works closely with the S2, especially when it comes to targeting. The S9 (Civil Affairs/Information Operations) works closely with the S2, S3, and the FSO with non-lethal targeting.

## Intelligence Preparation of the Battlefield (IPB)

Essentially, the practice of MI can be broken into two concepts: IPB and intelligence, surveillance, and reconnaissance (ISR).[2] My contention is that you can't do effective ISR unless you have done your IPB, so let's start with IPB. I will address ISR later in this article.

**Step 1: Where are we going?** While it is a popular belief that Intelligence drives Operations, more often than not it is Operations driving the Intelligence process. Why this matters is that current and future Operations seriously impact Step One of IPB as the first thing you need to know is where you are, and where you are going and this gives you the scope of your analysis. How you prepare the battlefield for a brigade or battalion mission in a new area of operations (AO) covering multiple towns and hundreds of square kilometers will be very different than conducting IPB for the AO consisting of a single town, neighborhood or even house for a company or platoon level operation. Whereas you will want to know everything about every window and door in a house for a particular raid, tracking that level of information for an entire city would be pretty overwhelming. Of course, as detailed information becomes available, it must be adequately data-based so that it can be quickly referenced when it is time to drill down for a specific mission.

While answering this question, it is also important to understand the area around the immediate AO and how it could affect the Commander's mission which the area of interest (AI). The area of influence includes those areas that are not in the Commander's AO, but which he could potentially affect with weapon systems, media, engagements with Host Nation leadership, etc. Although this is more of an MI concern, it is important to understand how what your commander does will potentially affect an adjacent commander's AO and mission.

**Step 2: How is our AO going to affect both us and the enemy?** Now that we know where we are going, we can start addressing how where we are going is going to affect both ourselves and the enemy. The level of detail with which you address any of the following aspects will obviously be dependent upon the size of your AO for a specific mission analysis. This includes the weather and terrain and how the two interact with each other. An important aspect of the "terrain" is the population and its infrastructures and organizations and is called "Civilian Considerations" or "Human Terrain." Acronyms such as OAKOC (or a dozen other arrangements of those letters), PMESII(-PT), ASCOPE, and SWEAT-MS are utilized as tools to help address all of the variables introduced by the environment.[3] It is important to know what these acronyms stand for and to remember that while these acronyms are "tools" that can be utilized to thoroughly address a problem set, some aspects may or may not apply in all situations. As a general rule, I personally analyze weather and terrain (using OAKOC), and then apply ASCOPE to every aspect of PMESII (the –PT is covered elsewhere) depending upon the mission. SWEAT-MS is addressed under the infrastructure of PMESII, and I would address religion as either under social or add it to infrastructure (depending upon how much is known about the religious aspects of the AO).

The most important factor of this analysis is to answer the question, "So what?" How will these varied aspects of the AO affect the mission? How will they affect the enemy's mission? How do they help or hurt the enemy? How much is the enemy dependent upon any of these factors which can be an ad-

vantage or vulnerability? Ultimately, who has the advantage in this area and why? Of course, these questions cannot be answered in a relevant way unless you have some idea of what *the* mission is, and this is where again, Operations drives Intelligence (until ISR gives Operations the information needed to readjust the unit's plans.)
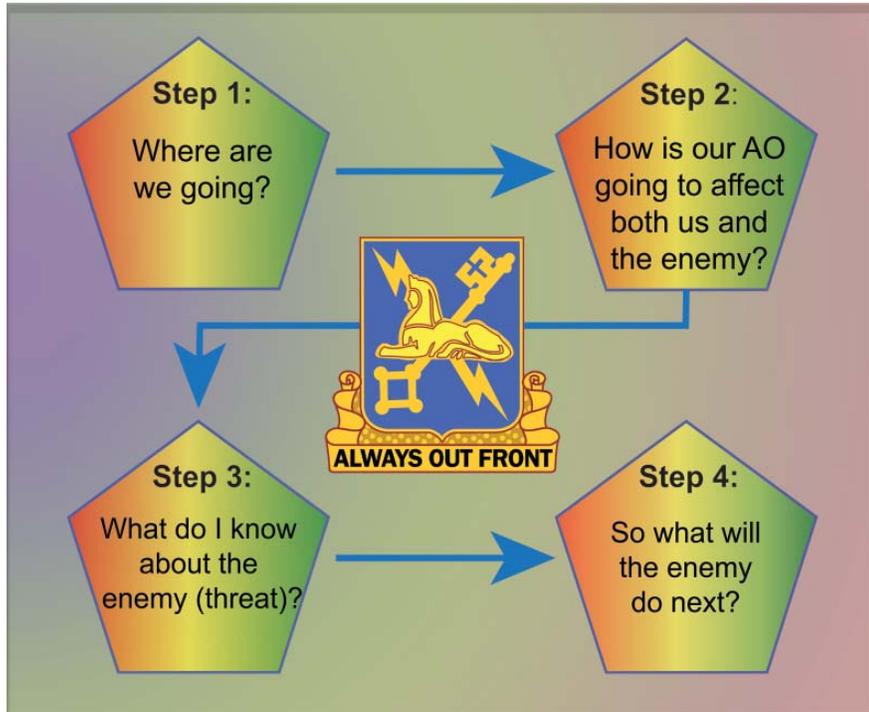


**Step 3: What do I know about the enemy (threat)?** This step involves answering what is known about the enemy, but it should be focused on the enemy as it exists within the AO. Whether that is the Kraznovians invading the country with tanks, artillery, air force support, and helicopter gunships or the insurgent cell living in a house you are about to raid, the principles are the same for all. Capabilities; composition; disposition; tactics, techniques, and procedures (TTPs); and strengths and weaknesses will give a pretty comprehensive picture.

✦ Capabilities addresses the specific details of the weapons systems (and other available resources) themselves and are again discussed by warfighting function (WfF).

✦ Composition addresses the number of personnel/units by WfF–Maneuver (trigger pullers), Fires (mortars, rockets, etc.), Protection (How do they defend themselves?), Logistics (beans, bullets, and transportation), Intelligence (How many of them are studying us?), Information

Operations (How are they getting their message out and what are they trying to communicate?), etc. Composition will usually include link diagrams or line and block diagrams.

✦ Disposition describes where those units are and what strength. This is a combination of known and estimated information and is a good place for Significant Activity history and analysis.

✦ TTPs address how the enemy utilizes their resources to accomplish their mission. This can be addressed by WfF and should highlight any unique ways in which the enemy employs its resources.

✦ Strengths are identified to inform the commander and the rest of the staff of the potential challenges they need to mitigate. Likewise weaknesses point out those areas where the enemy is potentially vulnerable. Both result from the analysis of all of the above aspects of the enemy. Determining strengths and weaknesses is not an afterthought; it is the most important component of the third step of IPB.

Depending upon the scope of the IPB, I will describe an Enemy Campaign plan (including political, social, military and information operations). Depending upon where it fits best, I will sometimes include the campaign plan under IPB Step 4. It is important to remember that there may be more than one threat group involved, especially in a counterinsurgency environment. I usually comprehensively address each threat group individually.

**Step 4: So what will the enemy do next?** This step is inevitably the first question that gets asked of Intelligence personnel. If you know where you are going, how where you are going will affect both you and the enemy, and something about the enemy, you can make an educated guess (based on your analysis) to answer the question, especially if you have some idea of what we are planning to do.[4] Essentially, this step involves overlaying what you know about the enemy and how he typically operates within the AO and the effects of the terrain, weather, and population. When addressing a large AO and a long period of time (a deployment for example), this may look like a campaign plan.

You can now flesh out the military aspects of the campaign plan by zone (or area, depending upon whose work you happen to be plagiarizing and the preference of your Commander/S3). This includes a support zone (SZ), disruption zone (DZ) (sometimes replaced by a security area), and a battle zone (BZ) or engagement area. It is helpful to break out these zones and place them on a map utilizing what you know of the physical and human terrain. How the enemy operates in each of these areas will differ, and those differences need to be addressed. Again, if you happen to be raiding a bad guy's house that is, in the big picture, considered to be in an enemy SZ, you can rest assured that on a micro level, there will still be a BZ, SZ, and DZ around that house. The size of your specific mission's AO matters as to the level of detail you need to address.

Another way to develop enemy courses of action (ECOAs), especially at the mission-specific level is to address the task and purpose (I like to include method and endstate) for each of the enemy's WfFs (by zone if appropriate). In the end, the most important question you have to ask yourself while developing these ECOAs is "Why are you developing them?" The answer is to enable the Operations planners to have the best idea possible of what they are getting into before arriving so that they can plan accordingly. No one really expects you to be 100 percent accurate; but obviously, the more accurate your concept of reality is, the more effective the plan can be going in, and there will be fewer surprises upon arrival. This level of detail also enables the accurate development of an ISR Plan.

## ISR

ISR is, in my opinion, very misunderstood. Everyone knows they want it, but not everyone knows why. There are a few basic mantras to remember. The first is, "If you don't ask the question, you *won't* get an answer–If you do ask the question, you *might* get an answer." On the other hand, "Ask a stupid or irrelevant question, and expect to receive a stupid or irrelevant answer (if you get one at all)." The axiom that addresses both statements is that "You can't do ISR without having first done your IPB."

Good IPB will determine what you don't know, and with the help of Operations, you can determine what you still *need* to know to successfully accomplish a

mission. This is why the Operations staff is actually the proponent for ISR. The "*need to know*" gaps are what the Commander's *priority* intelligence requirements (PIRs) are supposed to be. A PIR should *always* be tied to a decision point (If this, then that). All of the other information gaps needed to continue fleshing out the IPB (which is never "complete") are called information requirements (IR). IRs can be collected by whatever assets are available to answer them. Unfortunately, someone got the idea that the only way you could collect on anything was if it was related to a PIR, so most PIRs are so generic that the term has almost lost relevance. However, PIRs, like IPB, are related to the size of the AO for a particular mission (or operation).

## Intelligence Disciplines

A quick summary of the means capable of answering our questions is in order here. I will refer to a specific Intelligence discipline as an "INT."

✦ Human Intelligence (HUMINT) collects information through direct interrogation and questioning of people and through "tasking" others to get the information. How that is done is not important, but what is important is to know that only HUMINT Soldiers are authorized to handle "sources."

✦ Signals Intelligence (SIGINT) refers to the collection of signals. Communications Intelligence involves monitoring and analyzing radio, telephones, etc. Electronic Intelligence involves non-communications signals such as radar and other systems. How collection is done, what all can (and cannot) be collected on and the level of information available gets classified quickly. But you should know that you can sometimes find out what is being said, sometimes you can find out how it was being communicated, and sometimes you can find out about what systems are being used. A lot can be done with this information.

✦ Open Source Intelligence is relatively "new" and is related to both HUMINT and SIGINT. It is the analysis of readily and publicly available information.

✦ Imagery intelligence (IMINT) is probably the best known type of intelligence and is usually the first thing people think of. Electro-optical (EO) refers to camera type pictures (usually black and

white because that offers the greatest resolution at long distances). Infrared (IR) enables you to see things at night. Full motion video (FMV) is usually what your Commander means when he requests IMINT. It usually comes in both EO and IR.

✦ Measurement and Signature Intelligence (MASINT) is often a catchall of everything that does not neatly fit into the other categories. MASINT can be very good at detecting movement, and that can be very helpful both at the very local level and also with much bigger AOs.

There is much more to these INTs, but this quickly becomes classified and is not a critical part of this discussion. I strongly recommend going to a good ISR Top Off class for more information (a TS level class is best if available).

One last asset that I consider to be an INT, is the concept of *Every Soldier as a Sensor (ES2)*. I break this down into dismounted (ES2(D)) and mounted (ES2(M)) because mounted soldiers can see things that dismounted soldiers cannot and vice versa. Specifying these two categories as INT enable me to more effectively utilize their capabilities via the Collection Plan.

## The Collection Plan

A Collection Plan (CP) is a tool used to help organize (in theory) all of the various Intelligence requirements and taskings within an organization. It is often an Excel document, and historically may have many merged cells, and while they may look cool, they are so unwieldy that they are often not used as well as they could or should be. My recommendation is to make every row of the table unique using the filter function on every column.

Based on my experience and observations of how the Commander and the staff utilize them, I personally disagree with the latest doctrine's definitions and use of the next two terms, but regardless of how they are defined, the process is still essentially the same. New doctrine uses the term "Indicators" in place of specific intelligence requirements (SIRs), and indicators are no longer required to be phrased as a question (which I prefer). In the real world, PIRs tend to be too complex creating a need to use SIRs (as what doctrine would like to think PIRs are supposed to be.) For me, a SIR is a question that you can ask to help you break down a PIR or IR into

bite-sized pieces. Typically, I will make my SIRs INT specific although more than one INT can often answer the SIR.

A column called SIR-EEI has replaced what used to be the specific order and request (SOR) column. The term SOR has been replace by "ISR Task" and I utilize that term to describe an entire row of the CP.[5] Just remember that every field in the CP is simply a tool to craft an effective ISR Task.

Essential elements of information (EEIs) are a new addition to Army doctrine. The Air Force (which does a lot of collection for the Army) uses EEIs which the Army has finally adopted into its own doctrine. I think of these as indicators. Essentially, the more information you can provide to the collector, the better the information that you receive back will be. This goes back to Mantra Two about stupid questions. For example, if you tell the collector to look for cars in the AO, you will not get a very good product back unless you are in a really remote area where cars are a complete anomaly.

On the other hand, if you ask the collector to immediately inform you if they observe a small pickup truck with a mounted weapon system headed north along a particular route at a particular location within a certain time frame, there is a very good possibility that you will receive exactly what you are looking for. And if you go so far as to inform the collector why you care by sending them a Concept of the Operation (CONOP) which you developed with the S3, you will probably get a variety of other related and useful information back in return. How do you develop this level of specificity? By doing your IPB of course! (Notice a theme here?)

Indicators or EEIs are very INT specific and become part of the ISR Task. While multiple INTs can still collect on the same ISR Task, the indicators should be tailored to the INT. SIGINT will be able to answer PIRs completely differently than IMINT or HUMINT would (although HUMINT and SIGINT can overlap in the nature of what they can collect just as IMINT and MASINT do.)

As discussed above, knowing where to look and focus collection efforts is very important. As an example, with FMV it is like looking at the world through a soda straw. Granted, the camera can be focused nearly anywhere within kilometers of the asset, but it is only looking at an area that is less

than 100x100 meters ($1/100^{th}$ of a square kilometer) at any one time. However, if you have done your IPB and determined that there are only certain locations where enemy mortars could be placed or that are most likely to be used for attack positions, you can now specify certain areas that you want to the INT asset to focus. These are named areas of interest (NAIs). NAIs are not only helpful in preparation for a mission but they are also useful for redirecting assets in the midst of an operation. Make them as small as possible and use them liberally. It helps to have INT specific NAIs to help you visualize what is actually covered. Ensure that your NAI overlay is sent to the collector along with the CONOP. NAIs can be mission specific.

Another way to focus your assets is to use "big picture" assets to "cue" a more focused and detailed asset. This can be done both within an INT (redundancy) and cross–INT (mixing). A chart that shows how this works is called an Intelligence Synchronization Matrix and should not be confused with the ISR Matrix which although related, only shows which assets are collecting on which NAIs when.

Specifying start and end times and dates is like developing an NAI overlay in the time dimension. The ability to specify times comes from good IPB and from tracking the results of previous ISR missions. While you might think, "I don't want to miss anything, so I will have the collection asset watch the NAI all the time," the reality is that collection assets are a very finite resource. By not recommending a time for the asset to observe your NAI, the folks running the asset will choose a time for you (if you are lucky and they choose to collect at all), and what you are looking for may or may not be there at that time.

One other important time element that needs to be addressed in an ISR Task is the latest time information is of value (LTIOV). This lets the collector know when your operation is over and you no longer care so they can focus their assets on more productive endeavors. For the purpose of your CP, properly using the LTIOV field will also enable you to purge (or archive) old and irrelevant entries from your CP.

The Air Force will require a justification for your RFC, and providing a justification for everyone is a good idea. This addresses the "Why" of the request and if well articulated, will enable the operator to give you the practical information you really need rather than just the information you requested. This is the purpose part of "Task and Purpose."

Finally, it is important that the collector knows who actually needs the information and how quickly. Is the information requested something that the Battle Captain needs to know immediately or is it something that can wait for the Company Intelligence Support Team to debrief from the platoon leader and then generate a report that you might read within 24 hours of the information being acquired? If you are requesting information from a higher echelon, what classification (including caveats) can you actually use (Who will you be sharing the information with?) What format do you want the information in (PowerPoint, Shapefile overlay, written report?) How do you want the information delivered (email, VoIP, FM, MiRC Chat, SharePoint?)

All of that information will go into a single row of the collection plan, and every row should be a separate ISR Task with only one NAI and set of times. Multiple collectors can be listed as capable. The S3 will "task" specific subordinate units to collect on these ISR Tasks based on his needs and the legitimate capabilities of the unit tasked. The Collection Manager will request assistance from higher echelon assets. Capable assets are not necessarily tasked, but if they happen to be passing through an NAI (even if it is not in their AO), they should know what would be helpful information so they can more effectively contribute to the fight. By utilizing a CP with discrete rows with only one NAI and start and end time per ISR Task, it can easily be filtered by column and can be quickly used to develop a prebrief to the unit. In addition, if you discover that higher level assets are flying through your AO on their way to support someone else's mission, you can quickly filter your CP and let them know what you are interested in and where they might find it.

## Targeting

While there are about 7 different acronyms to describe the targeting cycle (such as D3A, F3A, F3EAD, etc.), from an Intel perspective it is helpful to think of targeting as the focusing of the IPB–ISR cycle. The IPB process indicates a potential target which is then "nominated" to the target deck. The targeting meeting determines how much we should care and prioritizes resources to include ISR. ISR then collects on the chosen targets and feeds the new

information back into the IPB for that target. That additional information may raise or lower the priority of resources dedicated to the target. Eventually, enough information is known about the target to develop a CONOP to address the target either lethally or non-lethally. While this part of the targeting is usually handled by others, all of the IPB generated will be used, and ISR will be utilized in the execution of the mission. Information that is collected in the process is then added to the overall IPB and used to further develop other current or new targets.

## Conclusion

This was not meant to be a comprehensive explanation of everything related to MI. It is a framework within which you can place all of the information and skills you develop, and where your specialty fits into the big picture. In the end, pretty much everything in MI supports an aspect of either IPB or ISR, and as you have noticed, it is important to know how they are related because the two are very tied to each other. Now that you have the "hat rack," you can develop the "hats!"

**Endnotes**

1. For example, I include information from several FMs. FM 2-01.3 Intelligence Preparation of the Battlespace (IPB) (Defines the four steps of IPB) while FM 2.0 Intelligence describes IPB as six dimensions of the Operating Environment and eleven critical variables of the Contemporary Operating Environment.)

2. When the updated FM 3.0 is officially published in the fall of 2011, ISR will be replaced by "Intelligence Operations."

3. OAKOC—Observation and fields of approach, Key and decisive terrain, Obstacles, Cover and concealment.

PMESII-PT—Political, Military, Economic, Social, Infrastructure, Information, Physical Environment, Time

ASCOPE—Area, Structures, Capabilities, Organizations, People, Events

SWEAT-MS—Sewer, Water, Electricity, Academics, Trash, Medical, Security

4. ECOA development technically comes before the wargaming process that comes later in the Military Decision Making Process, but they are essentially one in the same. The first three steps of IPB that enable you to develop ECOAs should also enable you to dynamically modify the ECOAs during wargaming later.

5. The ISR Task is also known as a Request for Collection (RFC) when requesting assets from higher. The same principles can also be used to develop a Request for Information (RFI).

*Captain Perkins is assigned to 1/1 ID at Fort Riley, Kansas but is currently serving via a WIAS tasking in the J2 at U.S. Forces Iraq. He has served as an S2 in both combat and support battalions, as a SIGINT platoon leader in a Battlefield Surveillance Brigade, and an Assistant S2 in a Stryker Brigade. He was a DOMEX team OIC in support of Task Force 16 in Iraq.*
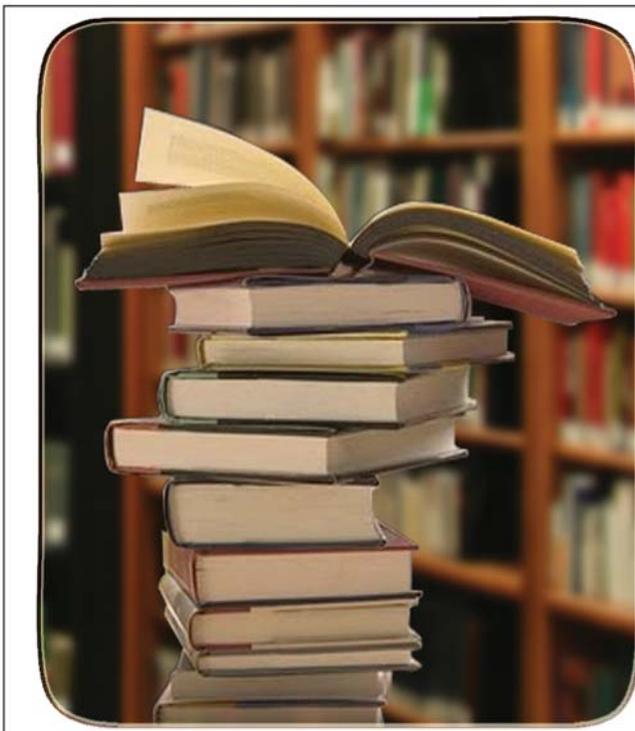
# Analyzing the Military Aspects of Human Terrain

## by Captain Jason A. Couture



*"In accurately defining the contextual and cultural population of the task force battlespace, it became rapidly apparent that we needed to develop a keen understanding of demographics as well as the cultural intricacies that drive the Iraqi population."*

*–Major General Peter W. Chiarelli, Commander, 1st Cavalry Division, Baghdad, 2004-2005*

## Introduction

From World War II to the invasion of Iraq in 2003, the U.S. Army demonstrated its prowess in maneuvering and dominating the physical terrain. However, it tends to lack a methodology for securing the peace once major combat operations are complete. Planners and leaders analyze the mission variable Terrain to achieve a decisive victory; however, irregular forces that dominate stability operations choose to operate in territory unfamiliar to the Army– the Human Terrain. Planners at all levels must be able analyze the military aspect of human terrain to deny the enemy observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, and cover and concealment (OAKOC) in the human terrain. *Active networks, social networks, key leaders, culture, and passive networks* (ASKCP) are human terrain corollaries to the military aspects of physical terrain.

The Army established Human Terrain Teams (HTTs) in 2006 in order to aid brigade combat team (BCT) Commanders in understanding the local populations of Iraq and aid in the counterinsurgency (COIN) fight. These teams are in high demand due
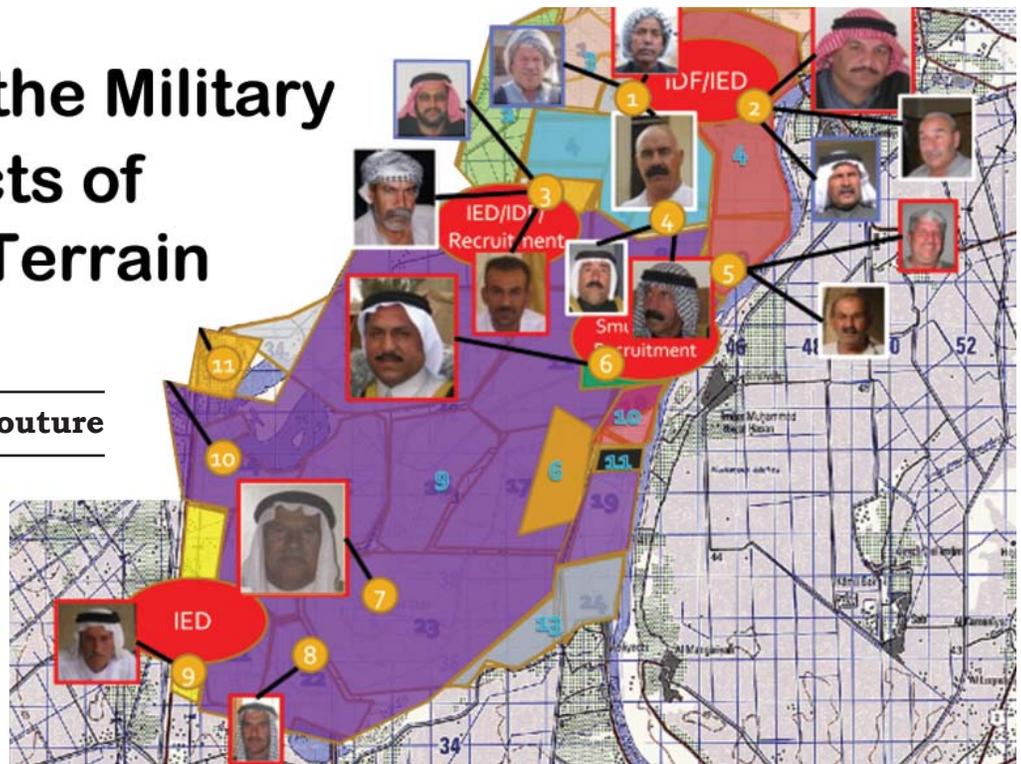
to their abilities to provide insight into cultural nuances of operations to the BCT Commander and his staff; however, the majority of the decisive operations in the COIN fight are at the battalion level and below. The HTT lacks the flexibility and resources to be able to advise platoon leaders and company commanders. The primary mechanism for problem solving at this level is the Military Decision Making Process (MDMP) and Troop Leading Procedure. Both of these include the analysis of mission variables: *mission, enemy, terrain, troops, time and civil considerations.*

## The Human Terrain

The Human Terrain System concept intends for Human Terrain to be included with civil considerations. These are summarized through the acronym ASCOPE (areas, structures, capabilities, organizations, people and events (civil considerations)). There is a problem with this categorization, namely that the term civil considerations immediately connotes that civilians are bystanders with no active role in the outcome of a given conflict. During Intelligence Preparation of the Battlefield (IPB) planners systematically scrutinize an area of operation and build a modified combined obstacle overlay (MCOO). Next they look at the enemy's capabilities and tactics, techniques, and procedures and create a doctrinal template. By analyzing both products, planners are

able to determine how and where the enemy will operate. The same can be done for human terrain.

FM 1-02 Operational Terms and Graphics defines terrain analysis as the collection, analysis, evaluation, and interpretation of geographic information on the natural and manmade features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. Logically it makes sense that human terrain can be analyzed in a similar fashion. With a substitution of a few words, the definition becomes: the collection, analysis, evaluation, and interpretation of *demographic* information on the *natural order* and *established organization* of the *human terrain*, combined with other relevant factors, to predict the effect of the terrain on military operations. This would capitalize on the current understanding of terrain analysis to ensure planners and leaders realize that human terrain is not a passive factor; rather it is a terrain on which forces can maneuver. The military aspects of physical and human terrain are compared below.

networks of people comprise early warning and human intelligence sources. They can provide insight into the nature of a conflict and provide clues on how to resolve issues.

*Social networks* are the established organization and patterns that determine the natural order and hierarchy enabling a force to achieve its objective. This includes tribal, political, or governmental networks. These groups serve as decision making authorities and can be used by irregular forces to recruit, propagandize, and support operations in order to meet their objectives. For example, in Iraq, a platoon leader conducts a key leader engagement with a sheik (tribal network) to reduce indirect fire (IDF) attacks, while the Company Commander influences the district mayor (political network) to refurbish a water treatment plant. Both are focused on the same objective, but take different paths.

*Key leaders* are personnel who have significant influence over the populace and whose assistance gives a marked advantage to either combatant. It

| Physical Terrain | | | | Human Terrain |
|---|---|---|---|---|
| Observation/Fields of Fire | Condition of weather and terrain that permits a force to see friendly, enemy, and neutral personnel, systems, and key aspects of the environment. | Networks that provide early warning and intelligence to enhance target detection, interdiction and destruction. | | Active Networks |
| Avenues of Approach | Route of an attacking force of a given size leading to its objective or to key terrain in its path. | Established organizations and patterns that determine the natural order and hierarchy that enable a force in achieving its objective. | | Social Networks |
| Key Terrain | Any area of which the seizure or retention affords a marked advantage to either combatant. | Personnel who have significant influence over the populace and whose assistance gives a marked advantage to either combatant. | | Key Leaders |
| Obstacles | Any obstruction, natural or manmade, which serves to disrupt, fix, turn, or block the movement of a force. | Factors unique to the terrain that prevent common understanding and cooperation: history, language, religion, perceptions, social rifts, modes of employment, etc. | | Culture |
| Cover and Concealment | Protection from the effects of fire/Protection from observation or surveillance. | Networks that are neutral or indifferent to the presence of either combatant. | | Passive Networks |

## Factors in Human Terrain Analysis

Army doctrine provides the necessary framework to analyze human terrain. By making slight adjustments to terrain analysis as outlined in FM 2-01.3 Intelligence Preparation of the Battlefield, planners can analyze the human terrain corollaries to OAKOC: *active networks, social networks, key leaders, culture, and passive networks.*

*Active networks* are the groups that permit a force to see friendly, enemy and neutral personnel, systems and key aspects of the environment. These

is necessary to secure the support of these individuals due to their placement in, and their ability to affect the society. In the Anbar province of Iraq, 23 tribal leaders succeeded in defeating the insurgency where five battalions of Marines failed.[1]

*Culture* comprises the factors unique to the terrain that prevent common understanding. These factors include language, religion, history, modes of employment, and perceptions. Just like obstacles, culture can be natural or manmade and can disrupt, turn, fix, or block an opposing force. Language

and history are natural to human terrain, but perceptions can be emplaced through Information Operations (IO).

*Passive networks* are the groups of individuals who are not actively supporting either side. They can be neutral, indifferent, or support by allowing an action. These groups tend to be categorized as "fence sitters," or those waiting to see which side will be the victors before aligning. It is these groups that will watch insurgents in Afghanistan emplace an improvised explosive device, and not warn a passing International Security Assistance Force patrol as it walks into the kill zone.

The outputs from Human Terrain Analysis are similar to those of Physical Terrain Analysis. With physical terrain analysis, planners produce the MCOO which enables them to see how to maneuver forces in order to achieve the desired end state. The MCOO visualizes all of the effects of terrain in relation to a map with respect to OAKOC. The same can be done with human terrain by creating a Human Terrain MCOO (HT-MCOO) which visualizes the effects of human terrain with respects to networks. The active networks show areas where both friendly and enemy have human informants or sources. It is in these areas that either force has the ability to detect and engage their adversary. The social networks show the extent of influence of each group. This includes tribal, military, police, political groups and religious groups. This shows where each group has the ability to impact the planners' desired outcome. These groups can be leveraged by either combatant against their adversary. Key leaders are shown in the vicinity of where they live or work. When the enemy situation template is overlaid, this will help planners know who must be engaged to counter the enemy's influence in that area.

Culture is the most difficult to depict graphically; however, it is possible to show how languages, religion, modes of employment, and perceptions are arrayed in the operational environment. Passive networks are shown as dead space. There are areas over which neither combatant has direct influence.

## An HT-MCOO

The HT-MCOO allows leaders to visualize the human terrain and see how to maneuver their forces. The forms of maneuver remain the same: infiltration, penetration, envelopment, turning movement,

and frontal attack. Take, for example, an IDF network in the vicinity of a U.S. air base in Iraq after the 2009 Security agreement requiring warrant based targeting. U.S. Forces (USF) has sources that identify the insurgent members but are unwilling to testify against them in the Iraqi court system. Likewise, the insurgents have a network of individuals who alert them when USF enter the area. The area is rural with generally heterogeneous tribal and religious distributions. To the north and south are generally Shia populations, while insurgents operate in the Sunni areas. There are two tribes in the area led by two tribal leaders.

These leaders are not the sheiks, but are clan leaders. The sheiks live in different areas. Both leaders are in support of the IDF network. The government does not provide support to the villages in the area and the Iraqi security forces (ISF) do not patrol the area. The network operates with the general support of the populations which are generally hostile to the USF. In the areas outside the villages, the people do not support either side. The insurgents' propaganda is generally focused on the USF disruption of the socialist system that provides for their livelihood and that by attacking the USF they could return to their previous economic system.

The USF desired end state is to leave a functioning government that is supported by the tribal system in order to deny the enemy the ability to operate. Given this situation and the fact that the end state cannot be achieved by military means, but through the will of the people, the USF must maneuver the human terrain.

Using the preceding simplified human terrain analysis, the USF can employ any of the five forms of maneuver within the human terrain. An *infiltration* entails bypassing the enemy strong points and attacking weaker objective. In the human terrain, combatants avoid the leaders supportive of the insurgents and build consensus amongst the populace. A *penetration*, which is applying mass to break the enemy's defenses, is conducted by multiple echelons of leaderships to engage the key leaders in the insurgent areas. Leadership will include USF, ISF, and governmental officials.

An *envelopment* involves fixing the enemy while maneuvering to an assailable flank. In the human terrain, envelopment consists of fixing the enemy while engaging those who provide support to the

enemy. A *turning movement* involves bypassing the enemy's strong points in order to force them to abandon their defenses. In the human terrain this is accomplished by engaging social networks around the enemy networks. A *frontal attack* is an attack across the breadth of the enemy's defenses. Similarly, in human terrain, a frontal attack is an engagement at multiple levels to defeat the enemy's influence.

In this scenario the USF took a multi-phased approach that focused on the eastern tribe in order to defeat the enemy network. In the first phase they conducted an infiltration and engaged the population with information engagements and humanitarian assistance. This resulted in securing support from the population. In the next phase, a turning movement, they conducted projects in the areas around the IDF networks and told the local leaders that if they wanted the same support that they would need to reduce IDF attacks from their area. In the next month IDF attacks decreased and the USF conducted a penetration. They rehabilitated an aging water treatment plant in conjunction with the local government. At the grand opening of the project, the USF chain of command all the way up to the Brigade Commander, the police chief, and mayor talked to the local tribal leader about supporting the local governance and security.

The USF immediately followed this project with a concerted IO which led to a majority of the population supporting the USF. In the last phase, the USF conducted a frontal attack by assembling the village, family, and tribal leaders and discussing their role in the future of the town and giving them an alternative to the insurgent solution. In this scenario, by the end of the USF deployment, attacks stopped from within the eastern tribe's area and the tribal and village leaders became actively involved in the local governance.

The above scenario is intended to serve as an example that human terrain is not a "consideration," but is maneuverable by both friendly and enemy forces. Moreover, by applying the time tested principles from existing doctrine, combatants can achieve a non-military end state through non-military or non-lethal means. Since the goal of operating in the human terrain is to gain support of the population, the primary weapon system is information. Regardless of the operations conducted, combatants always leave information. If USF build a

road in Afghanistan, they may intend to communicate their desire to help the local economy; however, when they leave, insurgents will say that Americans are making it easier to conduct raids. A thorough understanding of the human terrain will allow planners to employ all weapons systems while producing the desired effect on the population.

This does not negate the necessity of lethal operations. Lethal operations remain vital shaping operations to protect the population and prevent the enemy from employing coercion. However, the current MDMP model leads planners to the conclusion that the decisive operation is lethal or that by addressing civil considerations the enemy can be defeated. The analysis methodology does not take into consideration the various networks when determining enemy and friendly courses of action. ASCOPE generally looks at passive measures to gain support from the population. It aids in the targeting process to ensure that critical infrastructure is not damaged. What it fails to do is adequately address the effect of the people on operations.

Successful COIN operations require a detailed knowledge of the people in order to maneuver in the human terrain. An inadequate understanding will not only lead to mission failure, but can damage future operations. For example, in Afghanistan, U.S. Marines conducted a clearing operation of southern Helmand province. Echo Company established its combat outpost in the vicinity of a local market. The intent was to operate in close proximity to the people; however, the Taliban threatened to beat or kill anyone who used the market. The actual effect of the Marines was to deny the villagers use of the local market, forcing them to travel long distances to meet there needs.[2]

The Marines did the MDMP correctly; they saw the terrain, saw the enemy, and saw themselves. What they didn't see was the human terrain. The southern Helmand province had been "cleared" by USF several times in the past, but the area had never been held. The Marines' general IO theme was that the Americans were there, everything is now okay. They failed to account for the history of the area and that the people knew that the USF would eventually leave. The Marines did not deploy with Afghan replacements or develop a plan to leave an enduring presence. Moreover, they deployed with interpreters who did not speak the local dialect which exacer-

bated their problem. If the battalion staff had conducted human terrain analysis, they would likely have identified these issues.

The U.S. Special Operations Forces (USSOF) took a different approach the same problem. They are conducting Village Stability Operations (VSO) throughout Afghanistan. The goal is to establish Afghan Local Police in the towns to give the villagers local protection and a direct link to higher government officials. USSOF created this program after a detailed analysis of the human terrain. Their analysis revealed that tribal villages in Afghanistan are generally autonomous and see any outside influence, to include the government in Kabul as a threat to their independence. It also revealed that Afghans are very pragmatic and will accept outside help when it is in their best interests. Given this information, USSOF planners realized that VSO allows them to address both issues.[3]

Major General Michael T. Flynn, the former senior intelligence officer in Afghanistan, co-authored a report on the deficiencies of the intelligence effort in Operation Enduring Freedom. The report covered a number of organizational and functional inadequacies in the intelligence structure, and asserted that the Army is not properly focused on the human terrain. He highlighted several examples of units "getting it right" and the common theme is that those units "decided that understanding the people in their zone of influence was a top priority."[4] Some leaders naturally understand these concepts. For example, Lieutenant Colonel David Hodne, former commander of the 3rd Squadron, 4th Cavalry Regiment characterized the success of his organization in southern Salah Ah Din province, Iraq, as "a phased 'network-centric' strategy that required careful definition and understanding of both friendly and enemy networks as well as how these networks interacted with each other."[5]

He used an analogy of a societal "fabric" that is comprised of interwoven and interconnected groups to illustrate the need of analyzing the human terrain in order to achieve the unit's desired end state. Early in the deployment he noticed that the staff expertly defined enemy networks, but their training did not prepare them to analyze the effects of human terrain on both enemy and friendly operations. He noted that the unit learned over the course of the deployment to refocus its IPB to the decisive terrain.

This in turn caused them to refocus their collection efforts and target the human terrain with non-lethal effects (i.e., civil affairs projects, IO, public affairs). Unfortunately it took several months to develop their methodology, effectively limiting the impact of their deployment. This can be avoided in the future by standardizing the methodology and indoctrinating the force.

The Army envisions the future operational environment to pose a hybrid threat consisting of regular, irregular, terrorist, and criminal groups. Regular forces are generally easy to detect: tanks can be moved into urban areas, but they cannot blend with the local populace. Irregular, terrorist, and criminal elements have the ability to hide among civilians. In fact, they rely heavily on civilian assistance for logistics, and operations. In Iraq prior to 2007, insurgents and terrorists moved and lived among the populace with impunity. By June 2007, only nine months after the "Awakening," General Petraeus declared Ramadi a safe city. This is following a report at the end of the previous year by U.S. military intelligence in which the city had been declared "lost."[6] This begs the question, how did the full apparatus of U.S. military intelligence fail to grasp the problem, or more importantly, the solution?

U.S. military intelligence is extremely adept at defining and targeting enemy networks. However, as seen in Iraq, assistance from the local populace can deny irregular forces the ability to operate among the human terrain. The Army needs to implement a framework or methodology to analyze the military aspects terrain to apply non-lethal effects in order to remove the base of support and recruitment used by the irregulars. ASKCP and HT-MCOO provide the framework the Army needs. As the Army seeks to capitalize on the combined experiences of the past nine years of conflict, it is imperative that the art of human terrain analysis is not lost. ✴

### Endnotes

1. Kenneth Katzman, "Al Qaeda in Iraq: Assessment and Outside Links," CRS Report for Congress, updated 15 August 2008, 13.

2. Frontline, *Obama's War*, Public Broadcasting System, October 2009. Accessed at http://www.pbs.org/wgbh/pages/frontline/obamaswar/.

3. Sean D. Naylor, "Program Has Afghans in the Lead for Defense." *Army Times*, 20 July 2010 at http://www.armytimes.com/news/2010/07/army_specialforces_072010w/. See also Capt.

Neiman C. Young, "4th and Long: The Role of Civil Affairs in Village Stability Operations" at http://www.soc.mil/swcs/swmag/archive/SW2403/SW2403FourthAndLong_TheRoleOfCivilAffairsInVSO.html, originally published in Special Warfare, July-Septmenber 2011.

4. MG Michael Flynn, Captain Mark Pottinger (USMC), and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington D.C: Center for a New American Security, 2010), 13.

5. LTC David M. Hodne, "After the Surge: Task Force Raiders Experiance in Iraq," Best Practices in Counterinsurgency, Report 3 (Washington, D.C: Institute for the Study of War, 2010), 2.

6 Katzman, 14.

### Additional Reading

Center for the Army Profession and Ethic (CAPE). *An Army White Paper: The Profession of Arms.* Fort Leavenworth: Combined Arms Center, 2010.

Kipp, J., Grau, L. W., Prinslow, K., and Smith, D. "The Human Terrain System: A CORDS for the 21st Century." *Military Review*, September-October 2006.

Human Terrain Team Handbook. Fort Leavenworth: U.S. Army Training and Doctrine Command, September 2008).

*Captain Couture was commissioned in 2007. He graduated from Rensselaer Polytechnic Institute, Troy, New York. He served in a branch detail to the Infantry from 2007 to 2011. Assignments include: Platoon Leader, 1st Platoon, Charlie Troop, 3rd Squadron, 4th Cavalry Regiment, 3rd BCT, 25th Infantry Division. He was deployed to OIF 09-11 near Balad. He is a graduate of the MI Captains' Career Course.*

## Defining Moments in MI History

On the brink of the modern era of warfare, new technologies emerged. Signals Intelligence was born as telegraph lines were tapped and codes broken. The role of cavalry was redefined. Ulysses S. Grant was ably served in the western theater by Grenville Dodge who made effective use of Human Intelligence by organizing a Corps of Scouts specially trained in accurate intelligence gathering. When he moved to the eastern theater, Grant benefited from Sharpes Bureau of Military Information, the U.S. Army's first all-source intelligence organization.

1863

Maj. Gen. Grenville Dodge

Maj. Gen. George H. Sharpe

# Five Factors of an IED Attack

## by Major William Gettig

## Introduction

Without a doubt, the wars in Iraq and Afghanistan have shown us that Intelligence professionals play a critical role in operations. The contemporary operational environment of asymmetric warfare is highly fluid and often difficult for staffs to define and plan against. Today's enemy is also hard to identify in terms of personnel, let alone easily definable in theory. An asymmetric enemy typically uses anonymity as camouflage, fueling the perception that he is everywhere and can be anyone. It is important to emphasize that the role of an intelligence professional is not merely to report the enemy, but to understand the enemy as well. This understanding is vital to intelligence, allowing the focus of intelligence analysis methods and intelligence, surveil-lance, and reconnaissance (ISR) assets to place a spotlight on the enemy in the fog of the battlefield. Intelligence analysts should remember that they are not reporters; they are detectives in their own right, testing hypotheses and predicting results.

Despite the perceptions to the contrary, the enemy is not all-powerful, all-knowing, and invincible. The enemy can be detected and *can be beaten* and beaten often. The enemy is a human being, and enemy organizations are made of human beings. He must still plan in order to organize against a foe and expect success. The enemy also requires a method to ensure the survivability of the organization, however large or small. By examining past incidents, an intelligence analyst can discern (with varying degrees of success and accuracy) the battlefield geometry inherent in enemy planning.

Applying this philosophy of analysis will yield a better analysis overall, allowing Commanders and staff to focus operations and ISR assets. For exam-

ple, how does the enemy plan attacks? An attack does not "just happen." A successful attack requires some degree of planning, training, and execution. A perfect example of how an analyst can predict enemy attacks is in-depth analysis of improvised explosive device (IED) attacks.

## Five Factors of an IED Attack

There are five basic factors that are critical to a successful IED attack: bomb type; trigger type; the observer/triggerman; the target, and the bomb location. Any enemy planner addresses each one to some degree, and circumstances on the battlefield change the order of priority and importance. Indeed, the absence of any one of these will not yield the desired effects, negating enemy action. Lack of a bomb: no explosion. Lack of a trigger: no explosion. Lack of an observer/triggerman: no effects on target and possible compromise of the bomb. Lack of a target: no effect. Lack of location: no explosion.

*Bomb Type*. The capabilities of the bomb are important for an enemy planner. Potential effects upon a target will affect the design and composition of the bomb (based upon availability of materials), and in turn affect the location of its employment. In general, explosively formed projectiles (EFPs) are better than a lone artillery shell against an armored target. In contrast, an artillery shell is best suited against dismounted personnel or other targets requiring an area affect weapon. The bomb type also affects tactics the enemy will use to employ the bomb. A shape charge can bring down a tree or pole, causing a target to stop or separate from a group.

Analysis of the bomb type can tell an analyst, usually in broad terms, the level of sophistication or depth of logistics available to an enemy. An EFP requires a significant amount of resources and sophistication to produce compared to artillery shells and other similar explosives. An analyst with an enemy that employs EFPs on a daily basis is fighting a different fight than an analyst whose enemy employs only explosives in general. Harder-to-make EFPs that are used daily implies a much greater logistics structure and ability than easier-use munitions. In similar fashion, an enemy using explosives against hard targets with little success also indicates a level of training and ability to execute, allowing an analysis to provide relevant intelligence to the fight.

*Trigger type*. Trigger type is important in terms of bomb location and the observer (assuming for now that an observer also acts as a triggerman). As is the case of bomb type, the trigger will indicate the level of sophistication and depth of logistics. A wire-and-battery system is intuitively less sophisticated than a remote control trigger. As is the case in bomb types, neither trigger is better or superior to the other since both have their uses and are best employed in different scenarios. Even timers can be used, although they require a different degree of planning, employment, and logistical support. Analysts examining a situation should be cognizant of this, ask the relevant questions, and place thought into an analysis.

The purpose for the trigger is to not only produce effects upon a target, but to balance survivability of the observer/triggerman with the ability to execute an operation. Any trigger can go with any bomb. An enemy trend showing an association between a bomb type and trigger type enables an analyst to provide meaningful and relevant intelligence.

Trigger type will affect, and is sometimes affected by, the location of the bomb. In some ways, a target will also dictate which trigger type is most effective, depending upon the targets counter-IED capability. Each trigger type will also indicate a different logistical signature, leading to identification of an organization or to patterns of planning and execution.

*Observer/Triggerman*. The most important role in an attack is the observer/triggerman. Sometimes the observer is the triggerman, sometimes not. In any case, the observer should be disciplined enough to keep vigilant for a target and in some cases, a *specific* target. If an analyst can discern that a specific target was the goal of the operation, the analyst can then describe a whole level of planning remarkably different from a more general target of opportunity.

The observer/triggerman must also keep eyes on the bomb in order to prevent discovery and tampering of the bomb or compromise of the operation in general. Line-of-sight analysis may help an analyst to at least begin to discover where an observer was located, as well as offer the analyst the ability to predict future kill zones. In this light, the IED may be thought of as a fire support system for the enemy, allowing indirect contact and requiring observers to detect targets.

The survivability of the observer/triggerman is key to future enemy operations. A terrorist organization can be reasonably expected to conserve human resources for a variety reasons, such as training, operational security, and recruitment.

*Target*. The target is important to consider as well. Attacks upon logistics vehicles yield different results than attacks upon armor or infantry. A wise enemy planner will consider all the capabilities of a target. His analysis of available and/or desired targets will affect (or in logistical terms be affected by) bomb types and trigger types. The target is the point around which the web of enemy planning is woven, as the availability of bomb types, trigger types, observers, and bomb locations will affect and be affected by the target. An analyst fusing these inferences together at this point can also discern the enemy's ability to plan and execute operations based on logistical concerns.

*Bomb location*. There are two aspects to bomb location: macro and micro. They are often associated together, yet both must be considered separately and then fused into a comprehensive thesis later. Macro locations refer to terrain an analyst can see on a map in terms of terrain features, such as curves, straight-ways on roads, bridges, etc. Micro locations are best thought of in terms of what the target sees, such as left, right, above, and below. Macro and micro locations affect one another, yet require a shift of viewpoint from maps to lines-of-sight. When fused together in an analysis, both will provide a uniquely relevant and extremely useful insight into the mind of the enemy.

An enemy planner uses target capabilities to determine where to employ the bomb. A macro location will provide insight to the level of sophistication of the enemy's ISR capabilities as well as understanding of target capabilities. Features such as curves provide insight into an enemy that considers the importance of the ability to retain a higher speed (obvious for sure, yet important when compared to an attack on a straightaway). A macro location will also indicate where the enemy "knows" that a target will be available. Like minefields in conventional armies, an enemy employs a bomb in a specific place to cause an effect of some type.

Micro locations also indicate the enemy's ability to understand target capabilities. Lines-of-sight are all important in this regard, and their use or non-use will provide insight to an analyst. A bomb placed under asphalt is markedly different from one placed along the curb, *even if they are the same bomb and trigger type.* The difference comes not from a technical aspect, but more from a sophistication of planning. An enemy going to the trouble of hiding a bomb within a road is different in nature from an enemy merely placing one on the side. Micro locations also affect bomb types in as much as they dictate the camouflaging techniques necessary to hide the bomb from the target until detonation.

Macro and micro locations fused together in analysis provide tremendous insight to an analyst. Occasionally, and analyst can deduce the method and techniques used by a specific enemy group and create a useful (albeit mostly mental) enemy template. The understanding of bomb locations is crucial to an analyst, especially when predicting attack locations in a new area.

## Conclusion

Useful intelligence analysis always considers the art and science of warfare. Because of this, some exceptions do apply to any given scenario. Many different philosophies of thought go into the analysis, especially in Intelligence organizations. However, the analysis must start somewhere and then lead to some well-defined thesis or prediction. Analysis for the sake of analysis is never as important as analysis that paints a picture for a Commander. Applying critical thought to how an enemy may employ IEDs within an area leads to a better understanding of the enemy. Understanding an enemy leads to predictive analysis, which is far more actionable than simply reporting the activities of the enemy.

*Major William Gettig is the Brigade S2 for 1st Stryker Brigade Combat Team, 1st Armored Division at Fort Bliss, Texas. He has served four tours in Iraq, as a Battalion S2 for 1-17 FA BN, Brigade S2 for 75th FA BDE, and Military Transition Team Intelligence Advisor for 4th Battalion 1/6 Iraqi Army, and as an Executive Officer for USF-I J2 Strategic Intelligence Engagements.*

# The Joint Direct Support Airborne ISR Initial Capabilities Document

## by Lee F. Ilse, TCM Intelligence Sensors

Operations in Afghanistan and Iraq over the past ten years have made it apparent that traditional methods of employing airborne intelligence, surveillance and reconnaissance (AISR) assets in major combat operations are inadequate to support the current irregular warfare (IW) fight. This article describes a new concept of employment for those assets by placing them in direct support of tactical operations at the brigade combat team (BCT) level to support the full spectrum of future operations.

The Army Capstone Concept for Joint Operations describes several precepts that will underlie all successful future joint operations. Synergy at the BCT level and below is one of the most important competencies that will ensure future mission success. The Joint Direct-Support Airborne Intelligence, Surveillance, and Reconnaissance (JDSAISR) Initial Capabilities Document (ICD) was developed by a team led by the U.S. Army Training and Doctrine Command (TRADOC) Capability Manager for Intelligence Sensors and the Mission Command and Awareness Directorate from the Army Capabilities and Integration Center (ARCIC), Headquarters, TRADOC, and included representatives from all Services. The document was approved by the Joint Requirement Oversight Council (JROC) and published by the Army on 9 September 2010.

JDSAISR capabilities will promote synergy and enable tactical commanders to focus on their critical information requirements to drive operations. The JDSAISR concepts support not only major combat operations (MCO), but also operations dominated by stability tasks, and IW as seen in Iraq and Afghanistan. JDSAISR concepts are relevant in today's fight, and its construct allows for continued relevancy in the operations of the future. The JDSAISR concept is equally relevant to both Army BCTs and Marine Corps regimental combat teams (RCTs). Its desired outcome is operational synchro-nization of military actions to allow tactical commanders (defined as BCT and RCT commanders) to produce maximum relative combat power at a decisive place and time. The capabilities that JDSAISR delivers to tactical commanders are applicable to the current constellation of aerial platforms and sensors as well as the sensor systems envisioned for the future.

To fully appreciate the revolutionary nature of the JDSAISR concept, one must understand the type of assets and information flow that existed before. Prior to 2003, commanders envisioned fighting a conventional force-on-force war, and ISR support was funneled through hierarchical systems. These systems frequently delayed the development of a synergized, holistic, common operational picture derived from aerial and other collection assets. Timeliness of information flow tended to be tens of minutes and in some cases hours or days from assets that concentrated on division and corps needs. These assets' primary missions were to support division and corps commanders' priority intelligence requirements, with the majority of assets found in the aerial exploitation battalion located in the MI brigade at each corps.

The primary focus of those assets in conventional conflicts was for deep-look collection to find and identify second- and third-echelon forces. This deep look provided division and corps commanders with views geared toward shaping future operations rather than affecting the current, rapidly changing fight. Tactical commanders at lower echelons who were directly involved in the fight rarely had readily available aerial ISR assets to answer their more immediate commander's critical information requirements (CCIRs). The JDSAISR concept changes the old paradigm by placing assets in direct support of tactical maneuver forces that are most in need of this capability.

Lessons learned studies, after action reviews, and operational needs statements over the past eight years of combat operations have repeatedly shown that tactical forces suffer from significant ISR capability deficiencies that hinder completion of their missions. These shortages are in great part a direct result of insufficient organic/direct support aerial ISR coverage and/or capabilities. Adversaries' threat signatures continually grow more discrete, requiring additional ISR capabilities to discern indicators needed to develop the critical pieces of information/intelligence needed to answer CCIRs. The impact of these ISR gaps is that they considerably limit tactical commanders' overall situational awareness and understanding, and consequently their ability to make informed decisions and conduct synchronized operations in depth across their area of operations. The result is a significantly degraded ability to achieve mission success at the BCT echelon and below.

Through research of previous studies and interviews with subject matter experts from across the various TRADOC centers of excellence, the JDSAISR team identified eight broad capability gaps that significantly degraded the BCT's ability to achieve mission success across all four elements of full spectrum operations (offense, defense, stability, and civil support). These gaps are:

1. Situational awareness over wide geographic areas: The BCT lacks sufficient ability to gain and maintain situational awareness over the large areas of operations commonly assigned to it in current and future environments, particularly in complex terrain such as urban centers.

2. Sustained situational awareness: The BCT lacks sufficient ability to gain and maintain situational awareness over areas of operations or operational events for requisite periods of time.

3. Transform data into information and intelligence: The BCT lacks timely and responsive ability to transform available data into information and intelligence needed to answer CCIRs.

4. IW target detection and identification: The BCT lacks the ability to routinely detect, identify, and understand the intent of targets in an IW environment.

5. Target location accuracy: The BCT lacks the ability to locate targets in all operational environments with the requisite level of accuracy to support targeting operations.

6. Situational awareness and targeting timeliness: The BCT lacks a timely and responsive ability to acquire and transform data about the operational environment to provide adequate up-to-date situational awareness and to support targeting in all operational environments (particularly in IW).

7. Anticipate and respond to changing operational environments: The BCT lacks sufficient ability to achieve and maintain a requisite level of situational awareness and targeting support in response to a changing operational environment.

8. Synchronization: The BCT lacks the ability to fully synchronize intelligence and operations to enable the commander to make knowledge-empowered decisions in all operating environments.

The ICD makes recommendations to a variety of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities changes that can help to mitigate these gaps. Key recommendations include use of non-traditional ISR assets to increase available geographic and temporal coverage, shifting more analytic capability to the BCT, modifying training to include additional focus on the need for integration of intelligence and operations, and better tracking and assignment of personnel with key AISR skills. Additionally, it recommends further development and fielding of additional manned medium-altitude airborne systems and further development of new long-endurance and vertical takeoff and landing systems. The recommendations of this ICD have been incorporated in to the Army's Aerial Layer Platforms and Sensors (ALPS) investment strategy which will result in a sensor-centric federated system of sensors and platforms.

Before highlighting the different capabilities that will make up the pillars of the ALPS strategy, it is important to understand the future capabilities that tactical commanders will require. Timely, assured, persistent, and responsive AISR support is especially critical to the BCT and subordinate ground commanders' ability to execute their assigned missions in all operational environments–this is where the risk is the greatest. The future force must be able to persistently find, identify, and track vehicles,

personnel, and ambiguous/low-signature targets of interest over broad areas. In order to achieve this capability, the Army will employ a variety of AISR sensors, with interoperability, flexibility, multiple platform applications (manned and unmanned), greater sensor range and resolution, and increased target accuracy to support tactical commanders' expanding mission requirements.

The ability to perform camouflage, concealment, and deception detection operations in heavily cluttered and obscured terrain, such as vegetation (jungle/forest) and built-up urban areas, in day/night/adverse weather conditions at stand-off distance is necessary for IW and MCO. Counter-concealment sensor capability for AISR supports those needs, specifically by detecting concealed targets and lines of communications. Sensors must provide the ability to detect and positively identify targets of interest, (including, but not limited to, vehicle-size targets, individual dismounted personnel, and improvised explosive devices (IEDs) and their components). They must be able to detect the following types of targets: those located under foliage and camouflage; lines of communications and infrastructure under foliage or soil; roadside targets; buried targets, weapons caches, or other occurrences of disturbed earth; and targets inside structures.

To achieve this capability, additional investment must be made in new sensor technology. This technology falls in to four separate categories:

✦ Penetrating radars that can detect targets concealed under foliage or other buried in earth.

✦ Moving target indicator radars that can detect targets when acquisition via conventional electro-optical/infrared (EO/IR) sensors is not possible.

✦ Wide-area EO sensors that can be used for forensic backtracking.

✦ Precision location of Signals Intelligence (SIGINT) target signals.

Penetrating radars provide a tool for tactical commanders to detect man-made or natural objects concealed from the naked-eye. They provide a long/medium/short-range, wide-area, near real-time capability to detect these targets. Although the baseline technology is similar, individual penetrating radar systems provide different areas of coverage and levels of detection. Currently, there are at least

four variants of these radars at different stages of production or prototype:

✦ Foliage Penetration Radar (FOPEN).

✦ FOPEN Reconnaissance, Surveillance, Tracking and Engagement Radar (FORESTER).

✦ Tactical Reconnaissance and Counter-concealment Enabled Radar (TRACER).

✦ Vehicle and Dismount Exploitation Radar (VADER).

Collectively these fours radar sensors would provide tactical commanders an ability to track ground disturbances and movements, even when the activity is obscured by vegetation or an adversaries' use of varying methods of camouflage and concealment.

Ground moving target indicator (GMTI) and Dismount moving target indicator (DMTI) are two types of tracking systems that use advanced Doppler techniques to detect tactical vehicles and dismounted personnel, respectively. Vehicles and dismounted personnel appear as dots displayed on a digital map background. These systems track targets of interest in real time and can correlate with imagery and SIGINT data to provide tactical commanders a dynamic battlefield view.

In the past, EO/IR sensor operators and tactical commanders had to rely on narrow field of view (FOV) sensors for watching targets of interest. It was rarely possible to provide seamless coverage over wide areas, even when attempting to combine multiple video streams from different platforms on a single screen. New wide-area airborne sensor (WAAS) integration technology gives operators a capability to view a much broader area with high resolution over the entire field. The new technology automatically stitches together multiple narrow FOV video streams from the same platform in to a mosaic video stream which covers a wide area, and archives this video data over a period of hours. Playback of this video history can be used to backtrack individuals and vehicles from significant events (like the detonation of IEDs) to develop a better understanding of the IED network.

Finally, new technical capability to achieve high-confidence geolocation provides a critical new tool in the ability to find, identify, and prosecute individual SIGINT targets. The aerial application of this capability is known as Aerial Precision Geo-location

(APG), and it works in close cooperation with SIGINT Terminal Guidance (STG) conducted by ground teams.

In addition to this new sensor technology, the Army ALPS strategy invests in a variety of different multi-sensor platforms using a common Internet protocol-based sensor architecture. This sensor-centric federated solution has incremental options for future development and incorporation of new technology as it is developed. Under this strategy, four platform capabilities (pillars) will be developed; all of them will contain multiple sensors and use the JDSAISR ICD as their foundation. The figure below depicts the four-pillar strategy.

The first pillar is the Enhanced Medium Altitude Reconnaissance Surveillance Systems (EMARSS). The EMARSS platform focuses on supporting the current fight and irregular warfare by providing full motion video (FMV), Communications Intelligence (COMINT), and APG to the tactical commander.

While this system provides a necessary capability, it does not have the endurance and persistence necessary to operate for extended periods of time. To fill this niche, a Vertical Take-Off and Landing (VTOL) capable unmanned aerial system (UAS) and a Long Endurance (weeks) Multi-INT Vehicle (LEMV) provide unmanned solutions. The VTOL UAS is an unmanned rotary wing platform that will incorporate



**Sensor-centric Federated Solution w/ Incremental Options**

Irregular Warfare / Current Fight Focused

Minimize Infrastructure / Deployed Manpower Enhanced Long Term Persistence

Capability Growth

JROC-Directed Attributes

Limited SWaPC — Limited SWaPC — Not Agile — Agile and Niche

**EMARSS DR - CPD**
- FMV
- COMINT
- APG

Element 1

**VTOL UAS CDD**
- 2 x FMV
- COMINT / NVDF
- APG
- DMTI

Element 2

**PP (LEMV) CDD**
- 5 x FMV
- COMINT
- APG
- DMTI
- WAAS

Element 3

**ARL CDD**
- 2 x FMV
- SAR / GMTI
- HSI
- COMINT / APG
- LIDAR
- WAAS
- DMTI
- FOPEN

Element 4

**Each Element Requires Separate CDD or CPD to Define Diverse Requirements**

**Joint Direct-Support Airborne ISR ICD**

**Key:**

| | | | |
|---|---|---|---|
| SWaPC | Size, Weight and Power/Cooling | NVDF | Near-Vertical Direction Finding |
| CDD | Capability Development Document | SAR | Synthetic Aperture Radar |
| CPD | Capability Production Document | | |

two FMV cameras, a SIGINT system, and a radar capable of tracking DMTI. The LEMV is an un-tethered dirigible that contains five FMV feeds, COMINT sensors, a DMTI capability, and WAAS.

Finally, the Aerial Reconnaissance Low (ARL) will fill the fourth element of the JDSAISR strategy. The ARL baseline includes two FMV sensors, a COMINT package, an APG capability, and a radar sensor system. Additional sensors may include FOPEN, Laser Imaging Detection and Ranging (LIDAR) and hyperspectral intelligence (HSI) imaging sensors as niche capabilities.

The AISR layer capabilities must provide BCT and lower level commanders the ability to persistently monitor their area of interest and rapidly identify potential threats, such as individuals of interest who are attempting to blend into the civilian population, IEDs, and small teams of irregular forces. AISR must satisfy tactical commanders' requirements to rapidly achieve positive identification of high-value individuals (HVIs) and achieve the ability to track and target HVIs and other threat forces in urban and complex terrain. ASIR layer capabilities will provide once unachievable levels of situational awareness directly to the lowest levels where U.S. and multinational forces are in direct contact with threat forces and the civilian population. Even with capability overlaps and redundancies, there is insufficient overall capacity to meet validated requirements. The JDSAISR ICD is the driving force in advancement of technology in the form of new capabilities geared toward overcoming those gaps in support of tactical commanders.

In summary, the JDSAISR construct provides capabilities focused on the tactical environment at BCT and below echelons, and provides technical and operational flexibility and growth potential to cope with anticipated future threats. It is complemented by and fully interoperable with tactical, operational, theater and strategic ground and air capabilities and provides previously unachievable levels of situational awareness directly to the lowest level where U.S. and coalition forces are in direct contact with threat forces. ✳

## Defining Moments in MI History

World War II was an "intelligence war." In the U.S. Army alone, thousands of men and women became engaged in intelligence-related work over a wide spectrum of disciplines in seperate theaters around the globe, and at levels from strategic headquarters down to tactical companies. As a result, the war gave rise to many stories of individual achievement and innovation that would have a lasting effect on how intelligence would be thought about and conducted in future American wars.

*1944*

Detail from "Sherman Tanks Passing Streams of German Prisoners," Odgen Pleissner, 1944, Oil, U.S. Army Art Collection.

# Culture Corner

# Strategies For Integrating Language Capabilities into the MI Officer Corps

### by First Lieutenant Alec Augustine-Marceil

## Introduction

There is never going to be a point in your career as a Military Intelligence (MI) officer when language capabilities aren't important. Every deployment is to a foreign land with foreign cultures, customs, and languages. Thus, language capabilities must be understood as an integral component of intelligence work. Yet this is not an asset we have cultivated in our officer corps, and as a result we've become over reliant on contract linguists and automated translation, options that have severe limitations and drawbacks beyond the scope of this article.[1]

Acquiring a foreign language is especially important for the field of intelligence, because language is a gateway to understanding how someone else thinks. Language competency is central to our mission of understanding the enemy, a lack of capability in this area leads to a gap in intelligence capabilities. This is particularly true in counterinsurgency with an enemy that hides within a civilian population. Arie Amit, a retired Israeli General and a seasoned counterinsurgent, told an audience in Washington, D.C., that the U.S. would not prevail against the terrorists unless we understand "their language, their literature, and their poetry."[2] Language competency can increase our ability to read the civilian population, isolate them from the enemy, and operate within alliances–thus these competences should be a priority for training at the U.S. Army Intelligence Center of Excellence.

## Emphasis on Language Competency

Other services and other nations have made a concerted effort to develop language skills in their officer corps and we should follow suit. If we don't, we risk finding ourselves on the sidelines when important decisions are to be made, or worse, not fully equipped when we do have to make a judgment. According to the Defense Language Institute's Foreign Language Center's (DLIFLC) Command Historian, Clifford F. Porter, "Historically, U.S. forces have never had enough foreign language capability and had to adapt the best that they could, sometimes with terrible results, including the events of 11 September 2001."[3]

Within the militaries of other nations, most officers have at least a minimal capability to speak a second language. For example, in the Canadian Forces, all soldiers are required to become at least nominally bilingual, and every officer, fluent. In the Australian system, every Army officer is tested before commissioning, and officers are expected to become proficient in regional languages.[4]

Language capabilities have not always been pushed to the sidelines as they are now. In 1960, General Maxwell D. Taylor, Chairman of the Joint Chiefs of Staff, was so convinced of the necessity of language and cultural training that he wanted all officers to have foreign language as an integral part of their education.[5] This tradition has found renewed emphasis in some commands, in the form of requirements at service academies and bonus points in accessions, but the Army has yet to make foreign language acquisition a priority to train officers within the force, except within the limited Foreign Area Officer (FAO) program.

Other services, such as the U.S. Air Force, have placed a greater emphasis on foreign language training in their accessions process, at the point of accessions, and throughout each officer's career. They have even added language training given by DLI's mobile training teams to resident training at the Air War College and Air Command and Staff

College.[6] Additionally, the newly activated Language Enabled Airman Program is designed to sustain a corps of 3,300 officer-linguists across 26 languages. Almost 400 officers each year are recruited into the program, trained by immersion, and receive biannual language immersion training as "upkeep" of their language skill every year thereafter.



## Suggested Options for Language Training

The chief reason the Army MI Corps has not decided to make language training integral to officer education is not the lack of justification, but the lack of time. This, however, is a fallacy of time management. Sufficient time exists in every officer's career, the available time just needs to be better allocated. In the case of MI Basic Officer Leadership Course (MI BOLC) held at Fort Huachuca, Arizona, the average wait time from commissioning to course start is a minimum of 3 months, with some students waiting as long as a year.[7] Many of these students find themselves on "holdover status." They can do little of substance, because they haven't an Area of Concentration. Some will wait on leave, others at home (Reserve Component), some will spend several months at Fort Huachuca, Arizona, but all will wait. At Charlie Company, 304th MI Battalion, the unit responsible for MI BOLC, there are at the time of writing, forty second lieutenants (2LTs) on "holdover," (waiting for the next training cycle) and nearly double that number when the influx of graduates from the Reserve Officer Training Corps and the U.S. Army Military Academy report in the spring. This costs the Army valuable time on that Soldier's

contract, and there is also a cost paid in terms of the continuing enthusiasm of those young officers.

Instead of making compromises in course content or instructor time in order to decrease the backlog, let us take advantage of this time to develop some of those lieutenants' skills that will serve them (and the Army) for the rest of their career. This process starts with a skills assessment. Upon being selected for the MI Branch, all new 2LTs, regardless of commissioning source or destination (Active, Reserve, or National Guard) should be assessed as to how they can best contribute to the MI Branch. By the time these Soldiers receive their commission, they are no longer a "tabula rasa" (blank slate). They have developed skills, harnessed talents, and gained experiences which will have already shaped and defined them–hopefully as someone who will make a good intelligence officer. We need to make a better effort to identify those skills, for example, in languages. This may be someone who is a native speaker of Mandarin Chinese, or who has a little high school Spanish; however, in the age of cyber warfare, knowing C++ or Python may be just as critical. The many different sources of intelligence require many different skills to grapple with them. Taking an inventory of these skills within the force allows us to make better use of them in assignments.



One option on the initial skills assessment or survey should be an option to volunteer for immediate deployment. This option would include intensive language training for their target country during the time they are waiting to report for MI BOLC. Candidates would be chosen based on one criterion

alone: a Defense Language Proficiency Test (DLPT) score. This option would draw people who are highly motivated to learn that language, because they enter the course knowing they are going to use that skill, and how well they learn that language has a direct correlation with how they do in theatre. The course would be abbreviated, but intensive; ideally at least 16 weeks, but certainly shorter than the normal Initial Acquisition Course at DLI. It could be either held at DLI or one of the regional language centers as at Fort Lewis, Washington or at Fort Huachuca.

Target languages would be primarily Arabic, Dari, and Pashto, as well as other languages such as Korean or languages spoken in the Horn of Africa, which would be ideal for this type of program. This not only enhances the receiving unit's capabilities as they deploy, but sharpens that soldier's skill by following up their initial acquisition with a chance to put their skills into practice within an immersion environment. This program should be open to all commissioning 2LTs, active and reserve. If a reserve component Soldier chose and was selected for this option, he would join his home unit after the initial tour of duty. This program would offer an option for all MI lieutenants to study a language, where previously none exists, even for the most highly motivated.

Perhaps more valuable than initial acquisition is developing existing language skills within the MI Officer Corps. Many officers have acquired language skills outside of the Army, either in an academic setting, as an enlisted soldier, or perhaps as native speakers; yet the Army is often unaware of these talents because that soldier hasn't taken a DLPT. Identified by a skills assessment examination, lieutenants with a language would receive refresher training until they report to MI BOLC, with a mandatory DLPT at the end of their language training. Training soldiers who are already grounded in a language offers a better return on investment than training someone from a 0/0 level of proficiency.[8] Additionally, according to Army Regulation 11-6, The Army Foreign Language Program, soldiers trained at government expense (such as the afore-

mentioned refresher course) are required to retest each year for as long as they remain in the Army.[9] Following MI BOLC, students with a 2/2 or better would be posted to a unit which utilizes that language within their area of operations, either one of the regional commands, or to a deploying unit.

Another course of action, perhaps the simplest, is to use a DLIFLC MTT to train the Command Language Program Manager's (CLPM) Course onsite at Fort Huachuca. The CLPM course is a one week overview of the capabilities the Army has for language training. The course provides valuable training in how to develop soldiers, regardless of whether they are trained as linguists or not. The team teaching the course is funded with Total Army Language Program monies, and would not become a burden on the command's budget. Any unit with linguists on its Modified Table of Organization and Equipment is required by regulation to have a CLP,



a duty often tasked to a new lieutenant. It could be argued that that one reason military human intelligence collectors have lost their language capabilities is not just the high pace of deployment, but also lack of proper management. Putting students on hold-under status through the CLPM course provides them with a tangible skill with which to make real contributions at their first unit of deployment, because all members of the MI community can benefit from language training.

## Conclusion

By implementing one or all three of the above options, the MI Officer Corps can build junior officers' language capabilities without significantly disturbing their career path. It offers junior officers a chance to study a language, something even the

most highly motivated officer is currently precluded from. In addition, the Army's backlog of 2LTs waiting for MI BOLC is alleviated without shortening the course or compromising on content or instructor time. It brings us up to the standards being set by other branches and other nations, in a time of war when the skills we build can be put directly into the fight. ✵

## Endnotes

1. Clifford F. Porter, *Asymmetrical Warfare, Transformation, and Foreign Language Capability* (Fort Leavenworth: Combat Studies Institute Press, 2003). An excellent discussion of this issue may be found in this report.

2. Porter, 4.

3. Ibid., 1.

4. David Kilcullen, *Counterinsurgency* (New York: Oxford University Press USA, 2010).

5. Porter, 2.

6. Captain William T. Cambardella, "The Air Force Culture and language Center," *Military Intelligence Professional Bulletin*, January-March 2010, 26-32.

7. 2LT Kenneth Tarpley, Executive Officer, Charlie Company, 304th MI Battalion, August, 2010.

8. A 0/0 refers to a DLPT score showing no proficiency in reading/listening comprehension. A 2/2 is the standard score expected of DLI trained linguists, though the scale goes as high as 5/5. A third score (Speaking) is based on an Oral Proficiency Interview and is not included on all DLPTs for all languages.

9. AR 11-6, Army Foreign Language Program, 30 September 2009, 14.

*1LT Augustine-Marceil is a recent graduate of both the MI BOLC and the Civil Affairs Officer Qualification Course, and has deployed to a Provincial Reconstruction Team in Afghanistan as the team's Civil Information Manager. One of his duties will be to manage the team's linguists. He studied French at the Université du Québec à Chicoutimi .*

# Promoting Reconciliation in Afghanistan

by Colonel Donald R. Dunne, U.S. Army Reserve

*The challenge in Afghanistan...is to figure out how to (create) the conditions in which one can have successful reconciliation with some of the elements fighting us.[1]*

*—General David Petraeus*

## Introduction

This article presents a framework with which to create the conditions to reconcile some of the elements fighting the U.S. and its allies in Afghanistan. The first section contains five proposals to facilitate that reconciliation. Next, an education plan and media plan to counter the Taliban is presented. Third, ten themes around which arguments and lines of reasoning can be developed to cause doubt in the minds of Taliban members and potential recruits are outlined. I conclude with a brief discussion of how free market capitalism and republicanism might be established in the country.

## Proposals to Facilitate Reconciliation

✦ Determine if there is evidence, real or imagined, that the reputed founding father of Pashtun genealogy and culture, Qais Abdu Rashid, a Companion of Muhammed, is alleged to have said and done things which have been interpreted as eschewing tribal antagonisms and discrimination. Such evidence can be used as examples for the tribes to follow today to begin reducing their internecine conflicts.

✦ Ensure that educational, judicial, tax, and social reforms are seen as compatible with Islam and enhance the position of the religious leadership, including the mullahs at the tribal and village level. The imams/mullahs not only have ritual, juridical, medical, and educational roles at the village and tribal level, but also exercise spiritual leadership, especially when confronted

with threats from the Taliban to their culture or their faith. Focus on these religious leaders because their power and influence over their mostly illiterate and ignorant (in the ways of the modern world) countrymen is enormous.

✦ Develop an ongoing series of debates between moderate Afghan Muslims and the Taliban. Debate is a time honored tradition in Islam. Debates even occurred between Ali, the fourth Caliph, and the Kharijites, the most heretical sect in Islamic history. There is no better way for those Afghan Muslims to generate credibility than to participate in public debates. The most potent weapons in the war of ideas are those Muslims who are able to counter the Taliban's arguments.

**An interpreter, Kunar provincial Gov. Fazlullah Wahidi and Kunar chief of police Brig. Gen. Hussain Khallullah listen to Afghan elders from Chapa Dara district during a shura in Kunar province, Afghanistan.**

✦ The Gamaat Islamiyya has written a four-volume work wherein they renounce violence and theologically justify non-violence to accomplish their revolutionary goals. Translate it into Pashto and collaborate with Hanafi clerics to use some of its arguments to delegitimize the Taliban's reliance on violence. A reduction in violence could presage the creation of the conditions necessary to begin reconciliation efforts.

✦ Establish a version of South Africa's Truth and Reconciliation Commission in order to use religion to separate people from the problem. The South African Commission was partly established by wedding the notions of Christian forgiveness with the pan-African notion of forgiveness, known as *Ubuntu*. That commission was implemented without a shot being fired in anger. One method of applying the concept of the commission in an Afghanistan context is to link the Islamic concepts of forgiveness with the Pashtunwali concept of reconciliation known as *Roogha* (settlement of a dispute between warring factions). Then structure a Truth and Reconciliation Commission so that it incorporates the processes and mechanisms of the *Qawmi Jirga*. Thus structured, such a commission could be a basis upon which members of the Taliban could be reconverted to non-violence. The reconverted might then be induced to discourage fellow Muslims from joining the Taliban in the first place. In that way, the Taliban's recruiting pools might begin to dry up.

## Education and Media Plans to Counter the Taliban

*The Education Plan*. The Afghan government should invest in an educational system–from kindergarten through the university level–which incorporates the moral norms and social principles of the Hanafi Islamic legal tradition and the Pashtunwali Code of Behavior. Central Asian and Turkish Islamic educators have already devised very thorough educational training programs which promote Hanafi principles. These programs can serve as a useful baseline for developing similar educational programs in Afghanistan, using local Hanafi scholars to write the textbooks and curricula for lessons on ethics and faith. This approach will serve as an engine to delegitimize and dismantle the Taliban ideology, thereby limiting their influence on all Afghans, again drying up the recruiting pools.

*The Media Plan*. Promote reconciliation and political liberalization in Afghanistan by supporting, coordinating, and hosting discussions on Taliban ideology by anti-Islamist and non-Islamist dissident groups in public places and on radio. In order to accomplish this, coordinate the creation and funding for radio stations that broadcast live in Dari, Pashto, Tajik, Uzbek, and Turkmen from multiple locations, and have bureaus across Afghanistan and Pakistan. Guests on these shows should include Hanafi jurists, clerics, and other ulema, and proponents of those principles from both Afghanistan and Pakistan.

The focus of the discussions and debate will be to convince tribal elders and religious leaders who are the real powerbrokers in Afghan tribal society to undertake certain reconciliation activities. They are the decision makers and have a decisive impact on the values and behaviors of the youth that will listen to this radio station. They also have a lot of discretionary time for listening to radio programs in order to learn about a topic.



**A Humanitarian Assistance projects specialist negotiates with Afghans in the town of Mondi in Paruns Valley, Afghanistan.**

With this radio station we will improve our ability to conduct a war of ideas against the Taliban in two ways. First, it will provide a podium for respected religious and secular leaders who will urge their communities to fight against violence, cruelty, and terror. Five topics for such broadcasting are:

✦ A critique of the Taliban's definition of who is an apostate and who is a true Muslim.

✦ An examination of who benefits from Taliban ideas–groups interested in creating instability in Afghanistan and those who wish to make a fortune from inter-tribal/inter-ethnic conflicts and from spreading hatred.

✦ Mutual understanding and respect are *the* key issues in the Hanafi legal tradition.

✦ No coexistence between Islam and terror. The moral commandments of Islam are against all forms of violence, cruelty, and suicide, and the Qur'an forbids murder.

✦ The immorality of using religion for political or national aims. The only aim of religion is to satisfy a person's spiritual needs.

Incorporating both religious and lay leaders in this radio station programming can begin to win over important tribal elders and religious leaders, and thereby, begin to gain the information advantage in Afghanistan. The station must broadcast to all the rural regions of Afghanistan. Funding could be obtained by providing certain media moguls, not tied to the U.S. Government, with incentives to establish these radio stations and bureaus.

## 10 Themes to Cause Doubt

Using the 10 themes listed below, arguments and lines of reasoning can be developed to: cause doubt in the minds of the members and potential recruits of the Taliban; demonstrate the premises of the Taliban to be false; delegitimize Taliban belief systems, and dry up their recruiting pools.

1. In order to cause Afghans to doubt the Taliban, simply ask them: "Why are you entrusting your soul and salvation to a man and a group who have no formal religious training at all?" Do you really think our people were mistaken in their understanding and practice of Islam and only discovered the truth from Mullah Omar and the Taliban?

2. Use Imam al-Tahawi's, "Statement of Islamic Doctrine" to discredit and delegitimize Taliban statements and beliefs. A-Tahawi lived from 843/853-935 AD and is regarded as one of the greatest authorities on Hadith and Islamic law. I think his text could more aptly be titled, "What All Muslims Believe." This seminal work has been referenced and quoted through the centuries by so many important Islamic authorities, to include Salafi scholars, that it can be inferred they accept his exposition.

3. Divide the Taliban from the Pashtun by:

✦ Emphasizing that the Taliban's puritanical reactionary interpretations and expositions are inimical to the tenets of Hanafi Islam.

✦ Arguing that the Taliban completely change the Islamic and Pashtunwali values of those who join them. Thus, the Taliban are a threat to Pashtunwali culture and the Pashtun way of life.

✦ The Taliban attack and kill fellow Muslims on purpose.

4. Each family must teach their children to read, write, and study the Qur'an, as well as teach those adults in their households who lack these abilities. Improved literacy is the only way to alleviate the ha-

tred of fellow Muslims preached by the Taliban. In addition, the literate must seek out important leadership positions, at all levels, and encourage their family members to follow in their footsteps.

5. The Taliban's use of terrorist attacks can be countered by focusing on the immorality of their actions. Several messages and activities to do this include:

✦ Family members convince each other to tell the authorities who are the bomb makers, and where they can be found, and who are training the suicide bombers. By doing so they are defending Islam, their young men seeking employment, their women and their children, and their culture.

✦ Arguing that one man's terrorist is not another man's freedom fighter. That is because unjust means produce unjust ends. Individuals do have a right to overthrow an un-Islamic or corrupt repressive government. But using terrorism to do so cannot contribute to establishing a just government, for terrorism itself is unjust. Since the Taliban use terrorism and other unjust means to achieve their ends, their intent is unjust and therefore they will produce an unjust government.

✦ Who do you want to ensure your salvation? A credentialed Hanafi jurist who has read and studied the enduring works of Islamic theology, philosophy, and history? Or are you entrusting your salvation to one whose religious qualifications are just a matter of reputation?

✦ The Taliban insist on committing suicide operations because they are outnumbered and facing an overwhelming enemy military force. But Saladin did not resort to conducting suicide operations when he was outnumbered. So those operations are unnecessary. The Taliban therefore ignore both the Pashtun cultural traditions and Hanafi juridical positions on jihad.

6. Our poverty is not the product of Allah's will. It is due to the practices of the heretical Taliban.

7. Create the conditions that cause the Durrani mullahs and ulema to refuse to arbitrate between their tribes and the Taliban.

8. Discredit the Taliban's total refusal to compromise as being completely at odds with Islam and Pashtun culture.

9. Depict the Taliban as imposing on Pashtuns a profoundly alien way of life, in order to push them outside the sphere of Pashtun tribal culture.

10. The Islamic education in the Taliban's madrassas does not prepare students for jobs once they graduate. And when they do not get jobs, they become angry and take up weapons to vent their anger at society. What honor is there in doing that?

## Promotion of Free Market Capitalism and Republicanism in Afghanistan

Since Christianity and Judaism are subsumed within Islam, an argument can be made that the economic and political engines of those religions are also subsumed within Islam. Consequently, those economic and political engines, it can be further argued are Islamically legitimate. Afghans have demonstrated they want democracy, economic success, the rule of law, and industrial and political modernization. Therefore, in order to promote those developments, convene a Loya Jirga to accomplish the following:

1. Demonstrate that a secular constitution is compatible with Islamic law. For example, "…Islamic concepts that legitimate Muslim versions of democracy…include…consultation (shura) between the government and the people in the selection or election of rulers. This idea, coupled with a community consensus (ijma), a source of Islamic law, is now used to support modern parliaments and national assemblies as a way to reflect the collective judgment of the community."[2]

2. Establish that constitution based on Natural Law. In order for several religions to coexist, one law must transcend the different laws among the religions. Make it the Natural Law. That way, Pashtun tribal virtues such as honesty, loyalty, obedience, decency, and bravery will not be defined by Mullah Omar and the Taliban.[3]

3. Forbid clerics from holding office in order to prevent the creation of a theocracy. Theocrats can hijack a democracy because they will decide who will be allowed to run for political office.

4. Form a group composed of military and civilian Afghan experts, economic and Islamic historians, political scientists, sociologists, and economists to:

✦ Transmute the concepts contained in Milton Friedman's book, "Capitalism and Freedom,"

through the prism of the writings of prominent Muslim economists. In this way capitalism and republicanism might take root in Afghanistan.

✦ Apply the ideas contained in, "*The Road to Serfdom*" written by Friedrich Hayek in 1944. His purpose in writing the book was to outline a plan to ideologically combat the Nazis and the Soviets. After publishing the book, Hayek enlisted some of the most promising graduate students in the social sciences in the U.S. to help operationalize his ideas. Milton Friedman was one of them. Many of the ideas contained in this book can be applied against the Taliban for they too have a totalitarian ideology.



Photo by USMC Lance Cpl. Tommy Bellegarde

**The deputy governor of Helmand province, Afghanistan, during a reintegration shura at FOB Sher Wali, Marjah, Helmand province, Afghanistan.**

There may be dozens of students in the U.S. and in the West enrolled in graduate National Security Studies and social science programs who are first- and second-generation Afghan Muslims and who speak Dari and/or Pashto as a second language. The best and brightest of this group could assist with developing plans to apply Hayek's ideas against the Taliban as well as developing reconciliation plans. These students can also serve as a cadre of counter-ideology specialists to assist, for example, the National Counterterrorism Center's Global Engagement Group's efforts to counter violent extremism.

There are downsides to implementing these approaches. But the Taliban will eventually be defeated or eclipsed because they have no capability to correct the systemic problems in Afghanistan.

## Conclusion

Outlined in this article is a framework with which to create conditions to reconcile some of the elements fighting the U.S. and its allies in Afghanistan. First, five proposals to facilitate that reconciliation, then education and media plans were sketched out as ways to counter the Taliban. Ten themes were then outlined as a baseline upon which arguments and lines of reasoning can be developed to cause doubt in the minds of the members and potential recruits of the Taliban. These arguments and lines of reasoning can also be used to demonstrate the premises of those groups to be false, so that their belief systems will be delegitimized, thus bringing a halt to their movements. Finally, methods were briefly discussed to establish free market capitalism and republicanism in the country ensued. ✳

### Endnotes

1. Nathaniel C. Fick and John A. Nagl, "Counterinsurgency Field Manual: Afghanistan Edition," *Foreign Policy*, 5 January 2009. Accessed at http://www.foreignpolicy.com/articles/2009/01/05/counterinsurgency_field_manual_afghanistan_edition?page=0,1.

2. John L. Esposito and Dalia Mogahed, *Who Speaks for Islam? What a Billion Muslims Really Think* (New York: Gallup Press, 2007), 57.

3. Noah Feldman, *After Jihad: America and the Struggle for Islamic Democracy* (New York: Farrar, Straus, and Giroux, 2003), 189-234.

*Colonel Dunne currently commands an operational HUMINT unit in the Army Reserve. He assisted the Joint Information Operations Warfare Center J-34 in the development of an Influence Net Model for use against violent political Islamists and groups around the world and participated in a nomination-only seminar commissioned to answer a terrorism-related policy question for OSD(P). He has authored five articles on terrorism published by ABC-CLIO.*

# Enabling MI Analysts to Succeed in COIN Operations

by Major Edd Harrison

## Introduction

Are U.S. Army Military Intelligence (MI) analysts capable of providing a comprehensive assessment of the operational environment for decision makers during counterinsurgency (COIN) operations? If you use the paper, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, as a guide, the answer would be "no." The authors of the paper stated that the "vast intelligence apparatus is unable to answer fundamental questions about the environment in which U.S. and Allied forces operate and the people they seek to persuade."[1]

Being a large part of that intelligence apparatus, the Army MI Corps must be fixed to make it relevant in the COIN fight. Previous efforts to address these shortfalls have primarily centered at pushing additional intelligence, surveillance, and reconnaissance assets to the brigade combat team (BCT) and division levels.[2] While these efforts have greatly added to the capability of the modular force to collect critical information in a theater of operations, it has failed to teach analysts the necessary skills to process an ever increasing amount of information into accurate, precise, and comprehensive assessments of the operational environment (OE). The MI Corps needs to enable its analysts to produce quality assessments in COIN operations by updating doctrine with the introduction of a COIN intelligence summary (INTSUM), create a cadre of Master Analysts to oversee the analytical process at the BCT and division level, and to increase the collaboration of BCT and division analysts with the Intelligence Community (IC) at large.

## COIN INTSUM

If one looks up the doctrinal format of an INTSUM in FM 6-99.2, U.S. Army Report and Message Format, one will find that it caters strictly a high intensity force on force engagement.[3] Without a doctrinal template of an INTSUM for COIN operations, analysts are left to determine how to shape the current INTSUM to meet the demands of a COIN environment. This leaves analysts to fall back on what they are taught–enemy centric assessments, which does not describe all aspects of the OE in a COIN operation. This can be remedied by creating a doctrinal COIN INTSUM based on the six operational variables (political, military, economic, social, infrastructure and information–PMESII).[4] A PMESII based COIN INTSUM forces analysts to use all available information from open source to TOP SECRET to produce an accurate assessment. Its use will facilitate knowledge management by establishing an Army wide standard.

A criticism against analysts is that they use only classified reporting in their assessments, which mainly focuses solely on the enemy, thereby missing critical information about the OE. This tendency would be eliminated with a COIN INTSUM. The COIN INTSUM would be a forcing mechanism that compels analysts to look at all available information for their assessments. For instance, to provide a thorough political assessment, an analyst would be forced to look at reports like the State Department cables, provincial reconstruction team reporting, key leader engagements, and media reports, just to name a few. Another example would be economic assessments, which would force analysts to review reporting such as U.S. Agency for International Development reports, Civil Affairs assessments, and multinational media reporting (e.g., Chinese or Indian reporting on their investments in Afghanistan). A doctrinally based COIN INTSUM format would force analysts to review all available reporting to produce an accurate assessment of the OE that would influence a commander's decisions.

**INTSUM Format IAW FM 6-99.2**

**Proposed COIN INTSUM Format**

Another reason to create a doctrinal COIN INTSUM is to ensure reports can be easily retrieved from intelligence databases. A uniform COIN INTSUM would ensure that the information can be searched by metadata fields rather than by relying solely on word searches.[5] The use of metadata would facilitate analysts in quickly retrieving relevant information rather than going through extraneous links. Rather than playing with various word searches to find the information, metadata searches would allow pin-point searching, even if the information has to be in a set format. Metadata searches can only be maximized if the Army establishes and enforces a doctrinal COIN INTSUM. A doctrinal COIN INTSUM could be found using descriptive metadata (keywords, author, title, etc.), structural metadata (how the report is put together), or by administrative metadata (date of creation, file type, etc.). Until a doctrinal COIN INTSUM is established, analysts will continue to have to rely on word searches thereby wasting analyst's time and possibly leading to missed information, since no one can guarantee that a word search got all the information.

## Master Analyst Cadre

With a doctrinal COIN INTSUM established, the MI Corps needs to create a cadre of Master Analysts who will lead the analytical process at the division and BCT levels. The cadre would be responsible for enforcing intellectual standards (clarity, accuracy, precision, relevance, depth, breadth, logic, significance, and fairness) in all products, ensuring all writing is substantive in nature and enforcing critical thinking in all analytical products.[6] These personnel would be the analytical experts at the tactical level. This cadre could be established through a revamped Master Analyst course, attended by all military occupational specialty (MOS) 350F (All-Source Intelligence Technician) and selected senior Intelligence Analysts. [7]

Right now, there is no Department of Army course designed to provide advanced analytical skills training.[8] If a unit wants to train an analyst on topics such as critical thinking, mind mapping,[9] argument mapping,[10] or analysis of competing hypotheses,[11] then they are forced to send someone to courses held at the various national intelligence agencies in the Washington D.C. area.[12] To fix this shortfall and maximize training opportunities since the Army receives a selected numbers of slots in those courses, I recommend the Army create a two-week Master Analyst Course training all MOS 350F and at least one E6 or above from each battalion and MI company on advanced analytical techniques. This would create a cadre of Master Analysts. The Army could use critical thinking courses from the Defense Intelligence and Central Intelligence Agencies to jumpstart this course. With a cadre of trained analysts, intelligence assessments will improve in quality and depth; providing a clearer picture of the environment for decision makers at all levels.

## Improving Collaboration Tools

Training a cadre of Master Analysts in the same techniques as the majority of the IC analysts would facilitate collaboration. The training would provide a common language and structure between the Army and national level analysts. The only thing standing in the way is access to the IC's collaboration tools. BCTs need access to the IC's collaborative analytic workspace, Analytic Space (A-Space.)[13] Access to A-Space will allow analysts down to the BCT level to collaborate with multiple analysts in producing a collaborative assessment of the unit's area of operations. Further, BCTs can provide the IC a view of the respective AO to which analysts

in D.C. usually don't have access. For example, with proper access, analysts operating in Helmand Province, Afghanistan can collaborate with IC analysts in Washington, D.C. on poppy production, thus providing a more accurate picture of the issues to decision makers at all levels. Due to security restrictions, specific analysts (Master Analysts) must be given access to Joint Worldwide Intelligence Communications System (JWICS) terminals and granted access to A-Space. This might force additional facilities to be authorized to handle JWICS, which will produce budgetary requirements, but in the long run will allow greater collaboration of Army analysts into the greater IC.

## Conclusion

The job of MI analysts is to provide an accurate assessment of the OE to the commander that will influence his/her decisions. In a complex OE, this is made more difficult by the immense amount of data that an analyst has to sift through, ranging from TOP SECRET to UNCLASSIFIED reporting. To accomplish their mission, analysts must be enabled by changes to doctrine and training, as well as be allowed access to collaboration tools. For an analyst to effectively organize the analysis, he/she must be provided a doctrinally based COIN INTSUM as a guide to focus their analysis rather than relying on the current format. Further, analysts require a trained cadre of Master Analysts to guide their work and to ensure their products meet all the intellectual standards. As the reviewers of the COIN INTSUMs, the Master Analyst cadre must have access to the larger IC to collaborate with IC analysts ensuring analysts at all levels have the same information and access the tactical point of view. These three steps will greatly enhance the ability of the analysts to provide accurate holistic assessments of the OE in complex environments like Afghanistan. Until these changes are enacted, every BCT will continue to conduct analysis according to different formats and standards resulting in assessments that do not address all pertinent requirements for the commander. ✦

### Endnotes

1. MG Michael T. Flynn, Captain Matt Pottinger, and Paul Batchelor, Fixing Intel: *A Blueprint for Making Intelligence Relevant in Afghanistan*, Center for a New American Security, January 2010, 7, retrieved at www.cnas.org.

2. LTG Richard P. Zahner, "Rebalancing the Army Military Intelligence Force," *Army Magazine*, October, 2009. Focuses on how the MI Corps need to rebalance ISR assets to meet modular force. LTG Zahner states, "The Army MI end state should be an optimized force structure that provides core capabilities in support of the brigade combat team and division/corps full spectrum operations on a sustained ARFORGEN cycle–readily available to our readiness enterprise."

3. FM 6-99.2, U.S. Army Report and Message Format, April 2007, 127.

4. For description on each variable see FM 3.0, Operations, 27 February 2008, 1-5.

5. National Information Standards Organization, *Understanding Metadata*, 2004, retrieved at www.niso.org.

6. Linda Elder, PhD and Richard Paul, PhD, *The Thinker's Guide to Intellectual Standards: The Words That Name Them And the Criteria That Define Them*, Foundation for Critical Thinking Press, 2008, 7-11. Pamphlet outlines how to write for a purpose, provides exercises to train and test analysts, and outlines basic tenets of Critical Thinking.

7. The previous ASAS Master Analyst course taught analysts how to use the old ASAS system. The course did not address teaching an analyst Critical Thinking nor advanced writing techniques. For a full description of the old course see the ATRRS Catalog at https://atrrs.army.mil/atrrscc/courseInfo.aspx?fy=2007&sch=301&crs=3A-F71/232-ASI1F&crstitle=ASAS+MASTER+ANALYST&phase=.

8. David T. Moore, *Critical Thinking and Intelligence Analysis*, National Defense Intelligence College Press, 2007, 64.

9. For an explanation on mind mapping, see http://en.wikipedia.org/wiki/Mind_map.

10. For an explanation on argument mapping, see http://en.wikipedia.org/wiki/Argument_map.

11. For an explanation on analysis of competing hypotheses see Richards J. Heuer, Jr., *Psychology of Intelligence Analysis,* (Center for the Study of Intelligence, Central Intelligence Agency, 1999) at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/index.html.

12. Moore, 64. Critical thinking is currently only taught at the CIA, DIA, and NSA.

13. Ben Bain, "A-Space set to launch this month," *Federal Computer Week*, 3 September, 2008, retrieved at http://fcw.com/articles/2008/09/03/aspace-set-to-launch-this-month.aspx.

*Major Edd Harrison currently serves as a Joint Intelligence Planner at Allied Forces Command Heidelberg (NATO). His previous assignments have been as an S2X during OIF7, an MI company Commander in an SBCT, and an infantry battalion S2 during OIF 3. Major Harrison holds a BA in History from the University of Florida and a MA in History from Clemson University. He can be reached at edd.harrison@us.army.mil.*
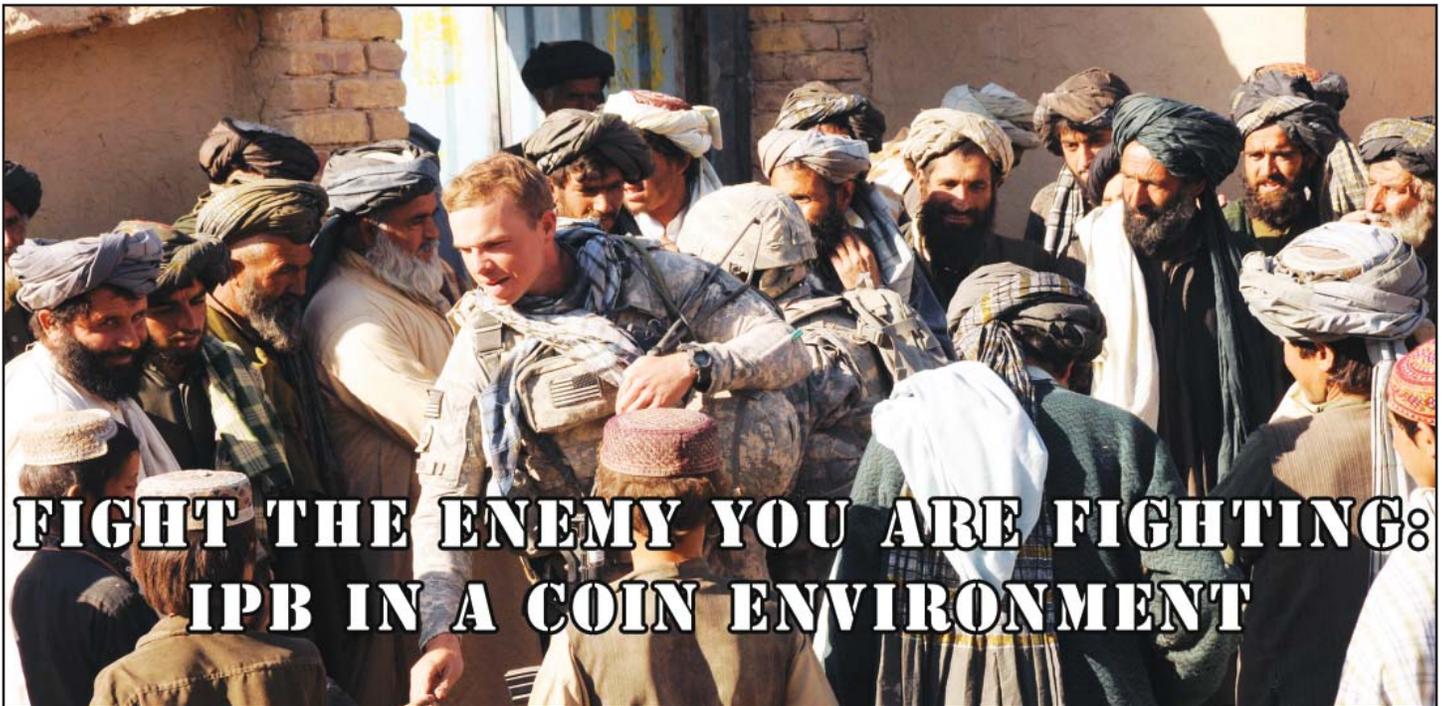
# FIGHT THE ENEMY YOU ARE FIGHTING: IPB IN A COIN ENVIRONMENT

by Major Eric H. Haas

*"The intelligence is the most important part of this whole damn thing. And if that's good, we can handle anything."*

—*General Creighton Abrams*[1]

## Introduction

With the release of the new edition of FM 2-0 Intelligence, the Military Intelligence Corps has the chance to reassess the fundamental core competency expected of the intelligence field: understanding the enemy and/or threats that affect our forces. Over the last nine years of conflict in Afghanistan and seven years of Iraq conflict, the U.S. Army has faced a myriad of enemy formations arrayed against it and has encountered difficulty as to how analysts visualize that enemy for their commanders to conceptualize. There has also been a reluctance to put form or structure to what appear as irregular forces.

Intelligence analysts have been unwilling to think of the enemy or threat in terms of how the enemy or threat actually fights. By inaccurately visualizing how the enemy arrays itself across the battle space, intelligence analysts create conditions that cause unit commanders to misdirect assets, fail to engage the right population to influence threat forces, and fail to create conditions having cascading and overwhelming effects to separate the enemy from the populace.

In order to create the conditions for success, it is imperative that intelligence professionals work to understand the structure of the enemy they face, how that enemy interacts with the population, and how the civilian populace resources and funds the enemy. If one does not perceive how the enemy arrays, it will be impossible to comprehend how the enemy interacts with the population–the source of the insurgents' sustainment and survival. Intelligence analysts cannot boilerplate formations, assuming that insurgents in one country or environment will fight in the same organizational modes as another, but the threat does have a structure as to how it conducts operations. Deducing an enemy's order of battle is becoming a lost art with too much focus by analysts on tracking individual leaders, but not enough focus on how that enemy or threat organization interacts in the battle space. This comprehension can only be developed by learning all you can about the enemy, as well as all of the civil, host nation security apparatus, and non-governmental organizations. An analyst must work to combine all the "red" (enemy), "white" (civilian population), and "green" (host nation security forces) data into a consolidated picture.

The failure to combine all these types of information into a single picture denies units true knowl-

edge of enemy intentions and interactions, an understanding of which is what intelligence analysts are supposed to provide a commander. Along with threat data, it is critical to realize the civil-military picture so the analyst can determine how the threat operates in its environment to sustain and grow the insurgency. A potential pitfall is in looking only at the civil-military data, and not relating it back to the enemy and threats operating within a unit's battle space. By not grasping how the enemy is structured, units are unable to appropriately apply resources to gain access and secure the civilian populace–a cornerstone of effective counterinsurgency (COIN) operations.



Task Force Stryker Conducts a Partnered Patrol in Kandahar Province, Afghanistan (2010.)

## Southern Afghanistan 2009
*Commanders must understand how current and potential enemies organize, equip, train, employ and control their forces"*

*—FM 2-0[2]*

In July 2009, 5th Brigade, 2nd Infantry Division (Task Force (TF) Stryker) arrived at Kandahar Airfield, Afghanistan as part of the initial surge of Coalition and U.S. Forces into the southern, Pashtun-dominated areas of the fractured country. As the Brigade moved into its assigned sectors, there was little knowledge of how the threat forces were structured, resourced, or funded to fight U.S., Coalition, and Afghan Forces. When the Brigade's intelligence officers worked with higher and adjacent units to comprehend the nature of the enemy, they received vague and incomplete answers. The higher and adjacent units provided intelligence updates that displayed line-and-block charts of the enemy leadership and vague circles or colored boxes drawn on PowerPoint slides depicting areas under threat control. The updates did not display what the actual strength of the enemy was in those areas, and in some cases completely misstated the hostile areas.

This lack of data led the TF Stryker's intelligence officers to significantly underestimate the strength, composition, and disposition of the threat forces arrayed against the Brigade. It did not have an understanding as to which areas were permissive, uncertain, and/or hostile during initial operations. Intelligence briefings and reports from adjacent and non-American units to TF Stryker tended to highlight which areas contact was expected, but never articulated the strength of enemy forces in those areas. Many analysts were very hesitant to assign strengths and organization to irregular enemy and threat formations within Southern Afghanistan. Part of this hesitation stemmed from a fear of being wrong. Another aspect related to poorly developed priority intelligence requirements (PIRs) that did not address what the threat's disposition and strength were in a specific area.

## PIR Refinement
When TF Stryker moved into its assigned area of operation (AO), the Brigade Commander developed initial PIRs that addressed the strength and composition of the threat forces, as well as identifying who the formal and informal powerbrokers were within the AO. This information was critical for the Commander and Operations Officer in order to de-

velop a plan to gain a foothold in contested territory and apply the assets appropriate to separate the insurgent forces from the population.

The refinement of these PIRs was critical to the process of determining the enemy disposition and strength as all the intelligence disciplines together are required to develop this information. Signals Intelligence was vital for determining the enemy's leadership structure and command and control mechanism. Human Intelligence developed the strength the enemy leaders had in their respective fighting formations as well as determine the enemy's intentions for holding specific areas. The critical piece for the analysts was fusing this data together. Despite what single source advocates will state, understanding the enemy requires an all-source, holistic approach. No single intelligence discipline can accomplish this.

## Hostile, Uncertain, and Permissive Operating Environments

The first step when entering a new operational environment (OE) is to determine if the area is hostile, uncertain, or permissive. A hostile environment is one in which hostile forces have control and the intent and capability to effectively oppose or react to the operations a unit intends to conduct. An uncertain environment is an environment in which neither host nation forces nor U.S. Forces have total effective control of the territory and population in the intended operational area. A permissive environment is one in which host country security forces have control as well as the intent and capability to assist operations that a unit intends to conduct.[3]

Enemy forces will present different signatures depending on the OE. A hostile environment allows enemy forces to conduct prepared defensive operations. In addition, in a hostile environment the enemy has complete freedom of movement to conduct offensive and defensive operations, logistical resupply and recruitment operations. In a hostile environment, the civilian population is inaccessible to Coalition Forces, by way of enemy forces creating physical and psychological barriers between Coalition Forces and the population. *Examples of historic hostile environments for COIN forces include Richmond 1865, Palan, Philippines 1901, Quang Tri, Vietnam 1972, Fallujah 2004, and Arghandab River Valley, Afghanistan 2009.*

The uncertain environment is the battleground within a COIN environment. Neither side completely controls an uncertain environment; hence, this category is the hardest to comprehend. Indicators of an uncertain environment encompass attacks targeting both military forces and civilians, assassination and murder campaigns, and large-scale and sustained attacks, as insurgents work to expand their control over the population. Due to the contested nature of this environment, it is very easy to focus on attack levels and overt enemy data, but miss the intentions of what insurgent forces are trying to accomplish. It is also easy to overstate successes in uncertain areas, when in actuality the insurgents are consolidating during a natural lull period. Analysts can at times label an uncertain environment as permissive without understanding how insurgents are targeting that area (whether through direct action, intimidation, information operations, etc). *Examples of uncertain environments are Kansas 1854, Manila 1901, Belfast 1978-1998, Baghdad 2006, and Kandahar 2010.*

Permissive environments analysts can also easily misunderstand, since permissive does not mean "friendly." Host nation security forces and Coalition Forces have a high level of freedom to engage with the population, but permissive does not mean safe. Insurgents will have reduced freedom of movement and generally focus their efforts on intimidation and information operations. The insurgent's goal in a permissive environment is to move it into an uncertain one using intimidation, spectacular, high-casualty attacks and assassinations to undermine security efforts. *Examples of permissive environments are Maryland 1861, Nashville 1864, Saigon 1970, Kosovo 2000, and Baghdad 2010.*

## Framing and Resourcing the AO

Once a unit determines what type of OE they are in the focus needs to shift to discerning the enemy strength and composition within the AO. It is not until a unit frames the OE and enemy's composition, disposition, and strength that the unit can apply resources (especially enablers) to their AO. The resources applied will vary significantly depending if the target area is hostile, uncertain or permissive. A hostile area will require focused, fully resourced clearing operations in order to establish a foothold to the population. An uncertain environment will require saturation patrolling with the ca-

pability to mass in critical areas quickly, complete quick impact civil projects, hold strong key leader engagements, and conduct intensive Information Operations (IO) to build trust for Coalition Forces. A permissive environment will require partnered security operations and a focus on more long-term projects to continue to bind the population to the host nation government and Coalition Forces.

If the Brigade did not perceive how the insurgents worked to control the population, it would be nearly impossible for it to apply the correct resources at the right time, place, and group. A brigade-level clearing operation into an area with few insurgent forces could potentially have negative effects upon the population, just as a focus on only civil-military projects in an area where there is no persistent security could also undermine efforts by not demonstrating success with the projects.

With the understanding of the strength and composition of enemy forces, it is now possible to see areas the enemy considers important to their operations, and the enemy's techniques to influence the civilian population in those areas. The danger is to look at one's AO as a unified whole, when one should break the area down into what the competing factions and enemy formations and intents are. Doing this ensures intelligence professionals are presenting their commanders a true view of what the enemy is achieving, and how the insurgency embeds in the population.

TF Stryker's AO from 2009 to 2010 included areas that ran the gamut of hostile, uncertain, and permissive. This required the Brigade staff to employ a wide range of different toolsets to work against the insurgents in the AO. The hostile environments required focused, offensive operations in order to gain a foothold into the population. Once a foothold was gained, TF Stryker had to expand that foothold and develop the perception of permanent, persistent presence to begin the separation of the insurgents from the population.

Uncertain and permissive environments allow for an expanded toolset for units to employ. As the environment becomes more permissive, it is possible to execute more projects, meetings and engagements. The focus can also shift to greater economic development and focus on issues outside of basic security concerns.



Photo by TSgt Francisco V. Govea II

**Biometrics Collection is invaluable to the COIN environment to conduct populace and resource control. Afghanistan (2010.)**

Within a permissive environment, one tool that greatly assisted the Brigade staff in understanding how the enemy interacted with the civilian population was the Tactical Conflict Assessment Planning Framework (TCAPF) developed by the U.S. Agency for International Development (USAID). The TCAPF is a questioning strategy that has four basic questions:

*1. Has the population in the area changed recently? If so, Why?*

*2. What is the biggest issue facing your village? Why?*

*3. Who can solve that issue? Why?*

*4. What should be done first? Why?*

*—FM 3-07*[4]

All of the maneuver battalions within the TF received training on these questions and incorporated them into their patrol focus. These questions allowed the commanders and staffs to comprehend what the major issues were facing villages in south-

ern Afghanistan and work to fix those problems. If an area had a large concentration of security related concerns, it helped to refine the enemy situational template; likewise if the concentration of issues focused more on civil-military issues (water tables, transportation to markets, infrastructure) it allowed the Civil Affairs detachments to focus specifically on issues in an area. This worked in the permissive areas, the enemy control and interactions in hostile and uncertain environments prevented this questioning technique from providing much insight into the environment.

By understanding the composition of the threat in specific areas, the Brigade staff could make informed recommendations to the Brigade Commander regarding resources to apply to specific problem sets. Areas that had a lower enemy threat were an immediate focus for civil-military and focused partnering operations to increase the legitimacy of the Government of the Islamic Republic of Afghanistan. Areas where the threat forces had control of the local population had more military assets dedicated to them including focused Clear, Build, Hold Operations, Special Operations missions, specific key leader engagements and IO messaging to separate the insurgents from the local population. The allocation of resources and efforts must be tied to the enemy control in an area.

## Conclusion

*Intelligence personnel provide mission-oriented intelligence about enemy forces within the AO, area of influence and area of interest as well as about other relevant aspects of the AO.*

*—FM 2-0[5]*

Understanding how enemy forces are operating within an assigned battle space is the critical function of intelligence professionals. To gain this knowledge in a COIN environment, analysts must pull data from all available sources to create a picture for their commanders. The data must include tradi-

tional and nontraditional sources of data, whether a single-discipline report, open source media, and the wide range in between. The intelligence professional then must be able to present the data in a way that decision makers can rapidly grasp the information, leading to informed decisions.
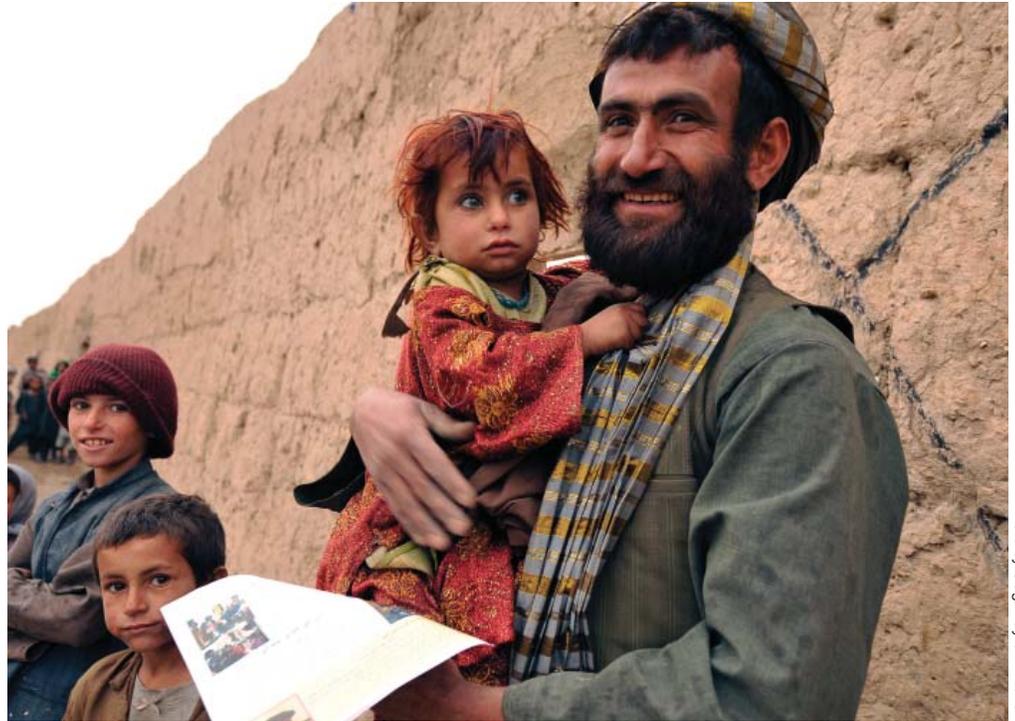


Photo by SSgt Dayton Mitchell

**TCAPF and other population engagement tools ensure patrols are learning about the human terrain. Afghanistan (2010.)**

In a COIN framework, all forms of data are critical to providing knowledge about the enemy operations within civilian the population. One must take in the social structure of an area to realize how the enemy is manipulating those interactions. Is the enemy purposefully manipulating tribal tensions to sustain or increase their hold over a population? How best should Coalition Forces distribute information products to have a specific and positive impact on the population? An analyst or staff member cannot accurately answer these questions without knowledge of the social structure. The critical part is to relate the social structure back to influencing the battlefield.

Another example is how the local economy and commerce data is critical information to knowing how friendly and enemy activity can influence the microeconomics of an area. In Afghanistan, many different agencies track the opium growing and harvesting season, but very few were tracking the harvest of legitimate crops. What is the underlying

message that commanders send to the population with operations that occur during the pomegranate and wheat-harvesting season, while during the opium season there are no significant operations? Within the AO, is the populace dependent on market commerce for significant portions of their income? This could mean that enemy attacks against markets and routes leading to markets could have an overwhelming detrimental effect on the population. These are critical questions and require many



Threat and force protection measures are dependent upon knowing the enemy threat in a specific area. Spin Boldak, Afghanistan (2010.)

different forms of data to answer–enemy composition, economic data, and host nation security forces information.

In order to conceptualize the COIN battlefield, intelligence analysts must breakdown their AOs into hostile, uncertain, or permissive environments. Then they must prioritize their effort to develop the

strength, disposition, and composition of the enemy threat within those zones. To assist in the comprehension of this threat, the analysts must pull in all forms of data that affects these operating zones. The social, economic, political, religious, and security data combined with the physical terrain ensures a comprehensive picture of how the enemy interacts with the environment. By realizing these interactions, Coalition and partnered forces can apply the correct resources to defeat the enemy forces. Without this understanding, the enemy will always be able to dominate the population and not allow that wedge to form.

### Endnotes

1. Lewis Sorley, *A Better War: The Unexamined Victories and Final Tragedy of America's Last Years in Vietnam* (New York, Harcourt, Inc, 1999).

2. FM 2-0, Intelligence, March 2010, 1-19.

3. FM 1-02, Operational Terms and Graphics, September 2004, "Operational Environment" 1-138.

4. Stability Operations, 6 October 2008, para D-49.

5. FM 2-0, Intelligence, March 2010, 1-20.

*Major Eric H. Haas earned his commission from the College of William and Mary with a BA in History and Anthropology. He has completed combat tours in southern Afghanistan with 5/2 ID (SBCT) as the Brigade S2X in support of OEF 09-11; southern Baghdad, Iraq as a Battalion S2 for 2-6 IN, 2/1AD in support of OIF 05-07; and a Battalion S1 in Baghdad, Iraq in support of OIF I. He previously served as a Rifle Platoon Leader in C/ 1-9 IN (MANCHU), commanded the 572nd MI Company, 5/2 ID (SBCT), and most recently served as the Brigade S2, 2-2 ID (SBCT) at Joint Base Lewis-McChord. MAJ Haas is currently attending the Command and General Staff Colleges ILE class 2011-02.*

# Pre-Deployment Source Operations Training for Maneuver Commanders

## by First Lieutenant Sean Gahagan

In the modern counterinsurgency (COIN) fight, commanders rely more heavily on Human Intelligence (HUMINT) to achieve the situational awareness and actionable intelligence they need to be successful in their areas of operation (AOs). Much of HUMINT's value in COIN is provided by military source operations (MSO), which can only be conducted by trained and certified personnel. However, a lack of understanding may lead some commanders to unwittingly conduct unauthorized source operations or to underutilize their MSO assets. The consequences of both of these mistakes can be detrimental to a commander's success within their AO, and unauthorized source operations can ruin careers. To provide deploying commanders with the training they need to avoid the pitfalls of MSO, the Army must make better use of resources and training programs already in place at the National Training Center (NTC) and Joint Readiness Training Center (JRTC), by providing a new class specifically on MSO to deploying maneuver commanders.

In the ongoing counterinsurgencies in Iraq and Afghanistan, the population is the center of gravity. Both operations and intelligence must shift more focus towards the population in order to be successful. In his classic work on COIN warfare, Lieutenant Colonel David Galula describes the population as the "new ground."[1] His description challenges the conventional perception of what constitutes key terrain. He goes on to state, "Politics becomes an active instrument of operations [in counterinsurgency.]" [2]

Colonel Ralph Baker recounts holding bi-weekly meetings with local leaders within his AO as a brigade combat team (BCT) Commander.[3] Using this political instrument to gain counterinsurgency's key terrain, commanders often meet with local leaders and liaisons on a regular basis. Concurrently, the population is also a critical source of intelligence in COIN. In a previous article on the subject, Captain Raven Bukowski described HUMINT and Counterintelligence (CI) as "two of the most im-portant capabilities a maneuver commander can leverage when conducting counterterrorism and counterinsurgency operations."[4] Maneuver commanders can often rely on HUMINT source operations for some of the most valuable information on insurgent networks and intentions, capable of leading to valuable actionable intelligence. Without sufficient understanding of MSO, maneuver commanders may unwittingly undermine the capabilities of their MSO assets. To mitigate this possibility and improve leverage of MSO, it is highly desirable that maneuver commanders be given sufficient training on MSO prior to deployment.

The need for this training is expressed in the observations of many people with HUMINT experience. Ryan Bareilles, a former CI Special Agent, deployed with a Tactical HUMINT Team of the 173rd ABCT to Afghanistan in 2005, observed that "people who were not qualified to conduct source operations were conducting source operations" and "commanders tried to run locally employed persons as sources without coordination or approval."[5] He stated that if maneuver commanders do not understand the MSO assets they have at their disposal, "they're shooting themselves in the foot!" This former MSO manager's frustration is evident in his observations. Regarding source operations, it is the opinion of Pete Swolak, a 2X Contract Instructor with MSO experience, that "there is a critical need for basic understanding by maneuver commanders. Without it, true synchronization of operations is impossible."[6] In order to avoid these issues and achieve better synchronization with MSO, better educational training must be provided to maneuver commanders.

A poor understanding of MSO may lead to legal consequences, disrupt or complicate such operations, and may deprive HUMINT collectors of valuable new sources. According to HUMINT collection doctrine, authority to conduct MSO is limited to HUMINT collectors, CI, and other select personnel who are trained and certified.[7] Strong emphasis on the "Every Soldier is a Sensor" (ES2) concept in recent years may have inadvertently encouraged

unwitting soldiers to attempt their own source operations. Considering this potential confusion, a U.S. Army Intelligence Center of Excellence training packet on tactical questioning clarifies, "A key difference between MSO and ES2 is that MSO involves intent to elicit information from a source by a specific collection plan or methodology" and "an authority to task the source."[8]

The manual goes on to describe the difference between sensitizing and tasking, and then lays out the "Golden Rule" of "Ask, Don't Task." In this manual, and others like it, leaders can find a basic description of their authorities with respect to liaisons and local contacts, as well as their limitations with respect to MSO. Nevertheless, this information will likely go untouched by many leaders, opening the door to continued unauthorized source operations.

A poor understanding of the MSO system can also lead to the disruption of ongoing military source operations. Within this system, sources are de-conflicted, synchronized, and vetted. Unauthorized source operations outside of this system are not de-conflicted, and according to FM 2-22.3 Human Intelligence Collection Operations, "may result in compromise of assets and interruption of collection operations and potentially unintended casualties."[9] To avoid these consequences, including potentially career-ending legal ramifications, maneuver commanders should receive better training on source operations as part of their pre-deployment training.

To achieve this training, maneuver commanders should receive stand-alone MSO training, which could be condensed to less than half of a day's training. The training should include the authorizations and limitations regarding MSO, the appropriate time and manner by which to hand-off sources to HUMINT collection assets, the MSO process (to include vetting sources), and it's capabilities as a force multiplier. The training programs in place for leaders rotating through the NTC and JRTC already include instruction on intelligence capabilities; however, instruction on MSO needs to be emphasized by adding a new stand-alone abbreviated course. Because these training centers already employ MSO personnel, they are the ideal location for an abbreviated MSO class. By drawing upon the existing resources of NTC and JRTC, the Army can better equip its maneuver commanders by providing them with this additional stand-alone MSO class.

The establishment of a short pre-deployment MSO class at NTC and JRTC will provide maneuver commanders with the legal awareness necessary to avoid accidentally conducting unauthorized source operations. The resources, knowledge, and personnel are already in place for this class. This small change to pre-deployment training will allow deploying maneuver commanders to better utilize their MSO assets and appropriately bring interactions with local contacts into the fold of HUMINT collection. With this training, maneuver commanders can better leverage the instruments of both operations and intelligence on counterinsurgency's "new ground."

### Endnotes

1. David Galula, Counterinsurgency Warfare Theory and Practice (PSI Classics of the Counterinsurgency Era) (New York: Praeger Security International Academic Cloth, 2006), 4.

2. Ibid., 5.

3. Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations." Military Review, May-June, 2006, 23.

4. Raven Bukowski, "Bridging the Doctrine Gap: A CI and HUMINT Focused Look at the Transformation of MI Doctrine" Military Intelligence Professional Bulletin, April-June, 2008, 5-14.

5. Ryan Bareilles, Telephone Interview, 5 January, 2010.

6. Peter C. Swolak, E-mail Interview, 11 December, 2009.

7. FM 2-22.3 Human Intelligence Collection Operations, September, 2006, 28.

8. MI Basic Officer Leadership (BOLC) 2X Course Tactical Questioning: Training Packet (USAICoE, 2009).

9. FM 2-22.3, 73.

*First Lieutenant Sean Gahagan was born and raised in Baton Rouge, Louisiana. He graduated from the U.S. Military Academy in 2009 with a B.S. in Physics Honors and a Minor in Terrorism Studies. As a cadet, he studied in Monterrey, Mexico for a semester and competed in the annual Sandhurst Competition with Company H-3. He is currently assigned to 8th STB, 8th TSC, Fort Shafter, Hawaii.*

# Applying the Theory and Techniques of Situational Criminology to COIN:

## REDUCING INSURGENCY THROUGH SITUATIONAL PREVENTION

by Major Stephen R. Gibbs
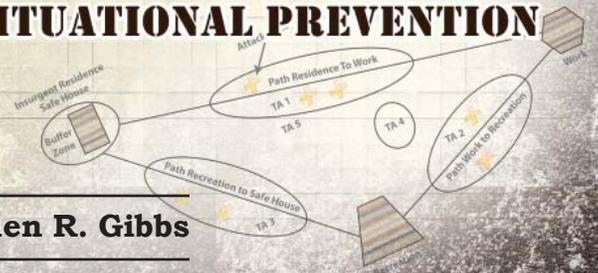
## Introduction

This article introduces the 25 techniques of Situational Crime Prevention (SCP). These techniques are based on a set of powerful theories within the fields of Environmental and Situational Criminology and offer a practical means to apply these theories to the reality of the asymmetric battlefield. Use of the 25 techniques would expand our repertoire of interventions, and enable a security force to intervene in the causal chain events to prevent or reduce the occurrence of insurgent violence and crime.

## Relevance of Situational Prevention in COIN

Counterinsurgency (COIN) techniques should be the practical application of good theory. Regrettably, theory is often considered irrelevant to security forces when conducting COIN operations. Criminologists Marcus Felson and Ronald Clarke argue this irrelevance likely comes from attributing insurgency solely to political, religious, or socioeconomic factors. Unfortunately, these factors are often beyond the purview of counterinsurgency, and therefore, often have little practical application.[1]

Opportunity theories within criminology could bring theoretical relevance to COIN operations by emphasizing principles and techniques that can be implemented at all levels of conflict to reduce insurgent violence and crime. These techniques are derived from the following three theoretical approaches: routine activity theory, crime pattern theory, and the rational choice perspective. Felson and Clarke say these theories build on the old adage that "opportunity makes the thief." In COIN op-

erations these theories build on David Kilcullen's concept of the "accidental guerilla." These theories, principles, and techniques are described here as are techniques that can be used to reduce insurgent opportunities, and thereby also reduce insurgent violence, crime, and the number of accidental guerillas.[2]

## Behavior is a Function of Both the Person and the Environment

Individual behavior is a function of both the person and the environment. This is one of the most well known principles in Social Psychology, and is referred to as Lewin's Equation, often expressed in the symbolic terms of B = f (P, E). Most COIN theories focus primarily on the person and discount the situational factors within the environment that turn an insurgent's motivation into action.[3]

Insurgency is a form of behavior, and as such is also governed by the Lewin's Equation. Insurgent behavior depends upon the conjunction of motivation (of whatever nature and whatever source) with opportunity (whether defined in terms of risks, efforts or rewards of the act).[4] Lewin's Equation shows the importance of the immediate situation in understanding an insurgent's behavior, rather than relying solely upon their past experiences. The causal effect that the environment has on insurgent behavior is evidenced by the fact that no attack can take place without overcoming the physical requirements to carry it out.

Conversely, the majority of people with strong political or religious grievances do not take up arms against the state, and many of the people that do participate in a rebellion belong to the upper or

middle class.[5] At this time there is no theory based upon the person that will always lead to an insurgency, but situational opportunities within the environment are always necessary for insurgent activity to occur.

Insurgent violence and crime are, in part, a result of situational opportunities within the environment. If we approach insurgent acts of violence as politically motivated crimes, they can be prevented or reduced through the application of the 25 techniques of SCP. These techniques originate from five core principles: increasing effort, increasing risk, reducing rewards, removing excuses, and reducing provocations.

## Theoretical Perspectives

SCP is a strategy that addresses specific crimes, or insurgent activity by managing, designing, and manipulating the environment in a manner that seeks to increase the risk to the offender, while reducing the offender's potential reward for committing the act.[6] It is informed by theory, and as stated earlier has Lewin's Equation as one of its foundations. Situational prevention also draws from three approaches within Criminology: Routine Activity Theory, Crime Pattern Theory, and the Rational Choice Perspective.

These three theories are often referred to collectively and individually as opportunity theories. Each of the theories is unique, but they all share three common assumptions. The first assumption is that crime, in this case insurgent activity, is a result of an interaction between disposition and situation. The second and third commonalties are that all three theories seek to explain criminal acts, not criminals, and stress the importance of situational opportunities.

***Routine Activity Theory.*** Routine Activity Theory was developed by criminologists Lawrence Cohen and Marcus Felson and states that in order for a crime to occur three things must come together at the same time and place: a likely offender, a suitable target, and the absence of a capable guardian to prevent the crime. This theory assumes there is always a likely offender, and focuses on targets, guardianship, and place.[7] Because all three elements must be present for a crime to occur, if you can control one element you can prevent or reduce crime. This is often modeled as the "Basic Crime Triangle", but

could also be viewed as a "Basic Attack Triangle" as shown below.



Routine Activity Theory and the Basic Crime and Attack Triangles
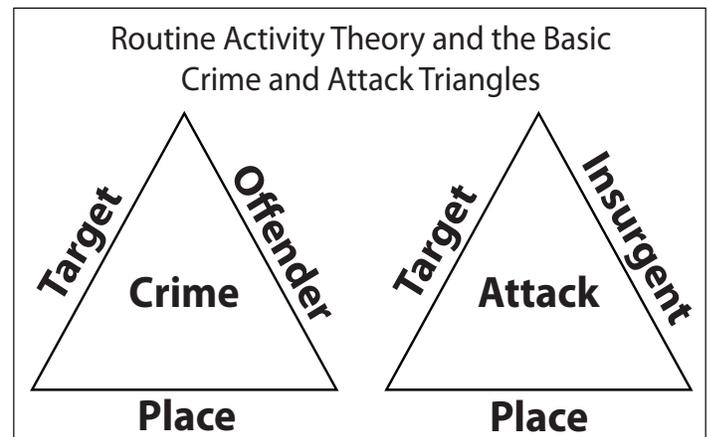
The guardian is not always a member of a security force, but could be anyone whose presence or proximity would deter a crime from happening. A target can be a person, place, or an object whose location in time and space puts it at more or less risk of criminal attack.[8]

Routine Activity Theory considers targets from the criminal's point of view. Evaluating targets from an insurgent's point of view is important because insurgents, like criminals, will only be interested in targets they value. This provides some explanation as to why every potential criminal opportunity is not exploited, and why every potential insurgent target is not attacked.

Felson and Clarke state that, "although the routine activity theory begins with the basic elements of crime and activity patterns, it ends up emphasizing changes in technology and organization on a societal scale."[9] A societal scale example would be the increased use of global communications technology by everyday people. This technology is exploited to increase the political value of insurgent violence and acts of terrorism, and allows the movement of information and money across regional and international boundaries. These are structural changes in the situational opportunities for insurgency and terrorism that have societal implications.[10]

***Crime Pattern Theory***. Crime Pattern Theory was developed by environmental criminologists Patricia and Paul Brantingham. It seeks to discover how offenders look for and find criminal opportunities in the course of their everyday lives. Because insurgent violence is mechanically and operationally the

same as ordinary crime, it can be used to understand how insurgents identify and select targets while going about their activities of daily living.

***Crime Pattern Theory.*** This argues that opportunities for insurgent violence do not always occur randomly, insurgents often search for and create these opportunities. Crime Pattern Theory also provides insight into how an insurgent evaluates these opportunities and chooses to act upon them.

There are three main elements of Crime Pattern Theory: nodes, paths, and edges. Nodes are the places that a person goes such as home, work, and places of recreation. The space around these nodes is considered activity space which is a sub component of a person's overall awareness space. Activity space is where people do the things that they do: live, work, socialize, commit crime, or engage in insurgent activities.

Paths are the routes that people take to and from these nodes. Offenders and insurgents look for opportunities and targets around their activity nodes and along the paths between them. Edges refer to the boundaries of the areas where an insurgent lives and works. Certain types of attacks are more likely to occur at the edges, such as sectarian violence between ethnic groups. More violent events occur along the edges because people from different activity spaces come together at the edges. Clarke and Felson state that the edges become important because there is a distinction between insiders and outsiders. Insiders will more often attack within their activity spaces, while outsiders will find it safer to attack at the edges and then retreat into their own areas.[11]

Brantingham and Brantingham would argue that target selection is largely dependent on routine pathways used by insurgents to move between their normal, daily activity nodes. Attacks are most likely to occur where the awareness space of the insurgent transects with suitable targets.[12]

Crime Pattern Theory is also modeled with a triangle. The diagram (right) shows how an insurgent

would go from his residence to work to recreation. Around these nodes of activity, and along the paths and edges he would look for situational opportunities to conduct attacks. Crime pattern theory posits that insurgents may find these opportunities a little ways off their paths, but they prefer to conduct operations in the areas that they know. This is because the effort and risk required to commit an attack increases the further an insurgent moves outside of his activity space. The diagram also shows a buffer zone around the insurgent's residence. There will be little insurgent activity within the buffer zone because of the risk of being identified and renounced to the authorities. There are five target areas within the diagram. Attacks are more likely to take place in target areas 1, 2, and 3 because they transect the insurgent's activity space. Target areas 4 and 5 are less likely to be attacked because they do not intersect with the insurgent's activity space. The insurgent may in fact be unaware of target areas 4 and 5 if they are also located outside of his awareness space.

Crime pattern theory also provides insight on how an insurgent evaluates opportunities and chooses



**Brantingham Crime Pattern Theory**
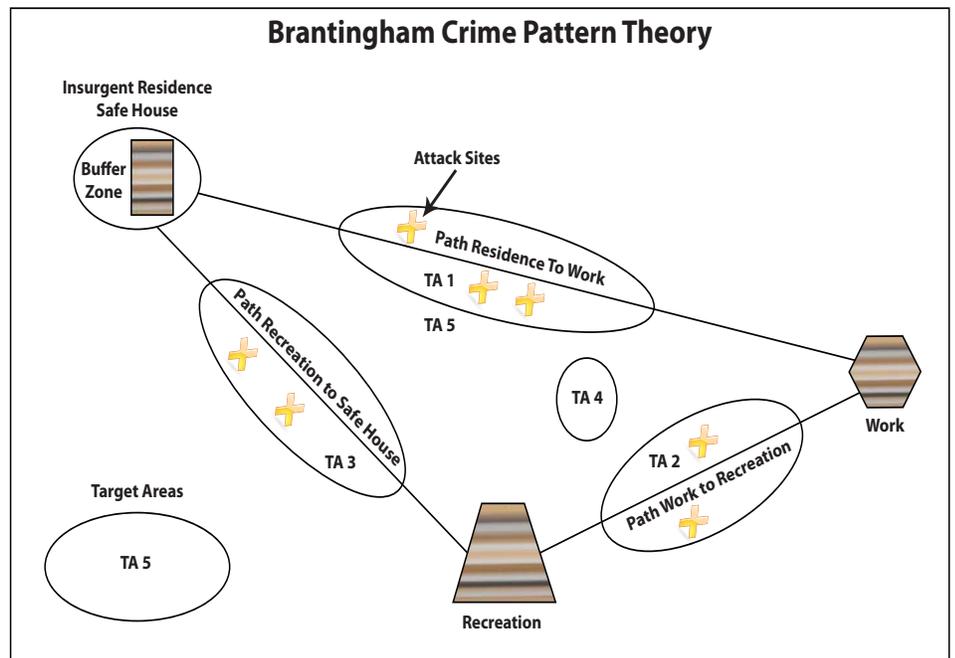
Adapted: Kim Rossmo, *Geographic Profiling* (Boca Raton: CRC Press, 2000).

to act upon them. The following is an adaptation of some of the principles of crime pattern theory taken from the institute of Canadian Urban Research Studies. As insurgents move through a series of activities they make decisions. When these activi-

ties, such as planting improvised explosive devices (IEDs) are repeated frequently, the decision process becomes routine. This routine creates an abstract guiding template. For decisions to commit a crime this is called a crime template. For decisions to commit insurgent attacks this can be called an attack template, and more specifically in this case, an IED attack template.[13]

Individual insurgents or networks of insurgents conduct attacks when there is a triggering event and a process by which they can locate a target or a victim that fits within an attack template. Insurgent actions change the bank of accumulated experience and alter future actions. This is also called scripting, and one of the goals of the counterinsurgent should be to rewrite the insurgent's script by introducing failure into their operations.

The following is an example of how this process could be applied to forming an IED attack template. A lightly defended convoy of military vehicles traveling down a pre-identified section of roadway is observed by an insurgent. This acts as a triggering event that fits his IED attack template, and the insurgent attempts to attack the convoy with an IED. If the attack is successful the template is reinforced. If the attack fails, or if an insurgent is captured or killed the template must be revised. During this period of revision, subsequent attacks may be prevented or delayed until the template can be rewritten, often resulting in a net decrease of attacks over time.

**Start**

Insurgent
Network of Insurgents

→ Triggering Event →

Activity
Attempted

**Insurgent Activity
Templating
Process**

Past Experience
Range of Motivations
Range of Opportunities

←

Success /
Failure
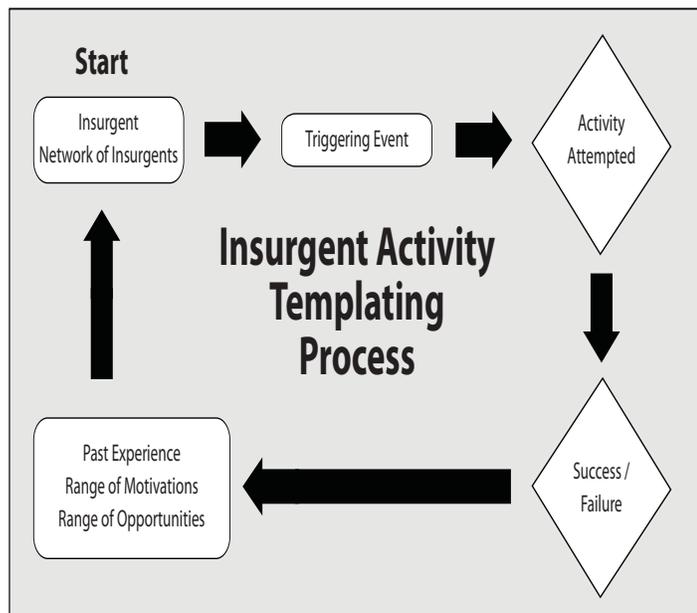
***Rational Choice Perspective.*** The Rational Choice Perspective focuses on the insurgent's individual decision making process. Its main assumption is that insurgent activity is purposeful behavior and that it is designed to benefit the insurgent. The Rational Choice Perspective also attempts to see the act from the insurgent's point of view. Clarke describes the Rational Choice Perspective as seeking to "understand how offenders make crime choices when driven by a particular motive within a specific setting, which offers the opportunities to satisfy that motive."[14] It assumes the insurgent thinks before acting and takes into account some benefits and costs in committing an attack.

Although insurgents make rational decisions, their rationality is bounded by risk, uncertainty, and the operational constraints that they face. Clarke theorizes that the "offender's calculus is mostly based on that which is most evident and immediate, while neglecting the more remote costs and benefits of crime or its avoidance."[15]

Specificity is also an important aspect of the Rational Choice Perspective. To understand an insurgent's choices, it is necessary to analyze each specific type of attack. The reason for this specificity is that each type of attack has different objectives and is influenced by very different situational factors. For example, there are several different types of bombing attacks, including IEDs, car bombings, and suicide bombings.

This is not to say that insurgents who conduct one type of bombing would never conduct another, it simply states that conducting a suicide bombing attack is quite different from planting an IED. Each type of attack is conducted against entirely different targets, with different types of bombs, and different objectives. Insurgents have to make different choices when conducting different types of attacks, and therefore each type of attack must be analyzed specifically.[16] Specificity makes modus operandi a primary consideration within the rational choice perspective.

These three theories can be categorized by the level of explanation that they address. Routine Activity Theory looks at insurgent behavior from the societal level; Crime Pattern Theory addresses the Meso or local area, and the Rational Choice Perspective addresses the individual. Each theory treats situ-

ational opportunities as a cause of insurgent behavior, and focuses on what an insurgent actually does while engaging in these activities. Clarke and Felson argue that together these three theories tell us that insurgent opportunities can be changed by society and the local community, while the individual insurgent makes decisions in response to these changes. They further state that "altering the volume of crime opportunities at any level will produce a change in criminal outcomes."[17] Therefore, altering the volume of insurgent opportunities at any level will also produce a change in the outcomes of insurgent activities, in particular, violence and crime.

## The Opportunity Structure of Insurgency

Clarke and Newman have identified a basic opportunity structure that is required for crime to occur, and have theorized that terrorism and insurgency require the same opportunity structure. The opportunity structure of terrorism and insurgency consists of targets, tools, weapons, and facilitating conditions.[18] They call these the "four pillars of terrorist opportunity," and state that they are a "result of technology, the physical environment of society, and the systems and services that help it to function."[19] The opportunity structure can be analyzed as described below.

*Targets.* Clarke and Newman identify eight characteristics of targets that make them attractive to terrorists and insurgents and express them through the acronym EVIL DONE.[20] EVIL DONE is a tool that assists in identifying and prioritizing potential targets through the eyes of an insurgent.[21]

**E**xposed: Targets that are highly visible and attract attention , such as the Twin Towers in New York City.

**V**ital: Targets that provide critical necessities for the daily functioning of society, such as transportation systems, utilities, and communication systems.

**I**conic: Of symbolic value, such as the Pentagon or religious shrines.

**L**egitimate: An acceptable target in the eyes of the enemy's public.

**D**estructible: Any target that can successfully be destroyed or disabled.

**O**ccupied: In order to inflict as many casualties as possible.

**N**ear: Close to the insurgents base of operations or those easily accessible by mechanized transportation, making them close in time.

**E**asy: Targets that are accessible with minimal security, and are within the insurgent's operational capacity to attack.[22]

*Tools.* Newman defines the tools of insurgency as "products that are used in the course of an attack."[23] Motor vehicles, mobile phones, false identity documents, and information about the target are almost always used by insurgents during the course of an attack. Ordinary criminals also seek out and use many of these same tools. There are generally three ways that the tools of insurgency can be controlled:

✦ Modify the products so that they cannot be used for criminal purposes.

✦ Make the products more difficult to obtain illegally.

✦ Track the use of the products.[24]

*Weapons.* There are nine characteristics that make weapons attractive to insurgents, and are expressed through the acronym MURDEROUS.

**M**ulti-purpose: Weapons that can be used against different type of targets.

**U**ndetectable: Weapons such as plastic explosives that can pass through security checkpoints.

**R**emovable: Easily transported.

**D**estructive: Explosives are more destructive than small arms. A fully automatic weapon will be more destructive than a handgun.

**E**njoyable: Terrorists and insurgents, like criminals and soldiers, become attached to their weapons.

**R**eliable: Dependability is an important factor in mission success.

**O**btainable: The ability of an insurgent to acquire the weapon by whatever means.

**U**ncomplicated: Weapons cannot be more sophisticated that the insurgent's ability to use them.

**S**afe: Explosives are less safe for an insurgent than firearms.[25]

*Facilitating Conditions.* Clarke describes facilitating conditions as the, "social and physical arrangements of society that make specific acts of terrorism possible."[26] Facilitating conditions make it ESEER for insurgents to conduct their operations, and are expressed by the same acronym.

**E**asy: Examples include cash, as a means of exchange, and governmental corruption.

**S**afe: Governments inability to authenticate and individual's identification.

**E**xcusable: Kinsmen injured or killed as a result of collateral damage.

**E**nticing: Cultural and religious endorsement of heroic acts of violence.

**R**ewarding: Some insurgents are paid for their services. Other insurgents may seek status, absolution, or the promise of sex in the afterlife. [27]

Opportunity structures operate at the strategic, operational, and tactical levels of an insurgency, but it is at the tactical level where the opportu-

nity structure of an insurgency is most profound. Newman argues that the first step to understanding the opportunity structure of an insurgency is to identify it at the tactical level. Tactical level opportunity structures are identified, "by focusing on the specific economic, physical, cultural, and social elements within the environment, on the ground where the insurgents operate."[28] By identifying the targets, tools, weapons, and facilitating conditions at the tactical level, we can trace the links between what are essentially local insurgent activities, and the operational and strategic conditions that both enhance and constrain them.[29]

## The Five Principles of Situational Prevention

SCP theory introduces 25 opportunity-reducing techniques. According to Clarke and Newman the principal value of these techniques is to increase the repertoire of possible interventions used to reduce specific forms of insurgent violence and crime. The 25 techniques are designed around five main principles that research has shown to affect the decision making process of criminal offenders. These five categories are also the core principles of SCP: increasing effort, increasing risk, reducing rewards, reducing provocations, and removing excuses.[30] Charts articulating the principles with their corresponding techniques and suggested COIN related interventions are shown in subsequent pages.

The first two principles of increasing effort and risk are cost variables. There are five techniques designed to increase the perceived level of effort to commit an attack, and five techniques that are designed to increase the perceived risk in conducting an attack. The third principle of reducing anticipated rewards is a benefit variable. The five techniques within this category are intended to reduce the insurgent's anticipated rewards. The last two principles of removing excuses and reducing provocations can be considered supplemental variables. Each of these categories also has a set of five techniques designed to remove excuses (justification, rationalization) for violence, and immediate provocations or temptations for committing an attack.

SCP theory argues that situational changes should be made that seek to increase the perceived amount of effort and risk, decrease anticipated rewards, and remove excuses and provocations. The theory advocates for a balance between increasing perceived costs and decreasing perceived benefits. An imbalance will either result in an attack being conducted, or an over allocation of security resources. Specifically, when an imbalance indicates benefits exceed costs, an insurgent will make the rational choice to commit the attack. When the imbalance increases perceived costs beyond what is needed to counterbalance anticipated rewards, an attack is deterred, but this may result in an over allocation of security resources.

Adapting SCP theory to COIN operations then leads to the following linear propositions:

1. Increasing the effort required to commit specific insurgent activities leads to a reduction in those activities.

2. Increasing the risk involved in committing specific insurgent activities reduces leads to a reduction in those activities.

3. Reducing the anticipated reward of engaging in specific insurgent activities leads to a reduction in those activities.

4. Removing excuses for engaging in insurgent activities leads to a reduction in those activities.

5. Reducing provocations to commit insurgent activities leads to a reduction in those activities.

These propositions are taken directly from situational crime prevention theory and, by extension, the rational choice perspective.

## The 25 Techniques of SCP

The first set of five techniques are designed to increase the effort required for insurgents to engage their targets, acquire their weapons, use their tools, exploit facilitating conditions, and maintain their organization. When operations become more difficult an insurgent system will be forced to expend more effort and resources to successfully maintain its operational tempo. Clarke and Newman argue that, "if we can raise the level of effort high enough for some their tasks, we may see them either give up on a particular target or take much longer to execute their terrorist mission."[31] The five effort reducing techniques are shown in the following table with some possible COIN related interventions.

Increasing the risk of being killed, captured, or mission failure is a cost consideration within an insurgent's individual decision making process.

| Situational Prevention Principal | Technique | COIN Related Intervention |
|---|---|---|
| **Increase Effort** | 1. Harden Targets | T-Barriers, shatter proof glass |
| | 2. Control Access | Gating, fencing, entry phones, swipe cards |
| | 3. Screen Exits | Tickets needed, export documents, property tagging |
| | 4. Deflect Offenders | Street closures, parking restrictions, no loitering |
| | 5. Control Tools and Weapons | Disable unregistered cell phones, RFID/GIS tracking of weapons |

Even a suicide bomber faces risk, the risk of mission failure. The five risk increasing techniques are shown in the table below with possible COIN related interventions.

| Situational Prevention Principal | Technique | COIN Related Intervention |
|---|---|---|
| **Increase Risk** | 1. Extend Guardianship | Deterrence patrolling, take routine precautions |
| | 2. Assist Natural Surveillance | Lighting, defensible space design, hotline reporting numbers |
| | 3. Reduce Anonymity | National ID Card, register SIM cards in cell phones, biometrics |
| | 4. Utilize Place Managers | Reward vigilance, care takers, employee training |
| | 5. Strengthen Formal Surveillance | CCTV, alarm systems, security guards, metal detectors |

Reducing the anticipated rewards of insurgent and terrorist activity is becoming recognized as an effective strategy, not only in reducing that activity, but also in hampering insurgent recruitment efforts. Marc Sageman says that it is important to take the "glory" out of engaging in these activities, as glory is a type of reward.[32] The five reward reducing techniques not only help prevent attacks, but mitigate the subsequent damage from successful attacks, denying the insurgents their anticipated rewards.

| Situational Prevention Principal | Technique | COIN Related Intervention |
|---|---|---|
| **Reduce Rewards** | 1. Conceal Targets | Low profile vehicles, avoid identifying signage and markings |
| | 2. Remove Targets | Limit unnecessary convoys, removable electronics in vehicles |
| | 3. Identify Property | Stamp small arms, GPS tagging, property markings, vehicle ID numbers (VIN) |
| | 4. Disrupt Markets | License vendors, controls on classified ads |
| | 5. Deny Benefits | Use of publicity to highlight hypocrisy of insurgent acts, design guidelines to reduce casualties |

Reducing Provocations and Removing Excuses are the final two principles of situational prevention, and each of these principles offer five additional techniques that assist in allaying insurgent violence and make it inexcusable.

| Situational Prevention Principal | Technique | COIN Related Intervention |
|---|---|---|
| **Reduce Provocations** | 1. Reduce frustrations and stress | Treat public courteously, expanded seating, efficient queing (line management) |
| | 2. Avoid disputes | Seperate rival factions, fight enemy's stragegy not his forces |
| | 3. Reduce emotional arousal | Avoid provocative announcements, clear ROE |
| | 4. Neutralize peer pressure | Marginalize agitators, say no campaigns |
| | 5. Discourage imitation | Rapid clean up of attack scenes, censor details of modus operandi |

| Situational Prevention Principal | Technique | COIN Related Intervention |
|---|---|---|
| **Remove Excuses** | 1. Set Rules | Clear ROE, clear rules for public demonstrations, clear regulations, codes of conduct |
| | 2. Post Instructions | No parking, no entry, no cell phones |
| | 3. Alert Conscious | Require ID and signature, visable electronic surveillance |
| | 4. Assist Compliance | Barriers, public restrooms, litter bins, designated parking areas |
| | 5. Control Drugs and Alcohol | Alcohol free events, public shaming |

The value of these techniques of situational prevention is that they offer a practical means to apply the principles of opportunity theory to the reality of the asymmetric battlefield. Use of the 25 techniques would expand our repertoire of interventions, and enable a security force to intervene in the causal chain events to prevent or reduce the occurrence of insurgent violence and crime.

The 25 techniques also provide a way of systematizing an insurgency reducing strategy. Situational prevention must be a continual process to be an effective part of counter insurgency operations. Criminals, terrorists, and insurgents are adaptive. They will make rational decisions to exploit new opportunities whenever they become available. This is one of the limits of situational prevention; there is never a final solution.[33]

## Conclusion

Insurgent behavior, like all behavior, is a function between the person and the environment. As such, insurgent activities depend on the conjunction between the insurgents' motivation (of whatever nature and whatever source) and the situational opportunities presented to them within their environment (whether defined in terms of risks, efforts or rewards of their acts).[34] Insurgent opportunities can be changed by society and the local community, while the individual insurgent makes decisions in response to these changes.

The 25 techniques of Situational Prevention provide a means to reduce the volume of insurgent opportunities, and affect insurgent decisions by altering their perceptions of risk and anticipated rewards. Altering the volume of insurgent opportunities at any level will also produce a change in the outcomes of insurgent activities, in particular, violence and crime. ✳

### Endnotes

1. Marcus Felson , R. V. G. Clarke, *Opportunity Makes the Thief: Practical Theory for Crime Prevention* (London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 1998), 1. This introduction is modeled from Felson and Clarkes introduction and extended from criminology to COIN.

2. Ibid.

3. "Field Theory–Kurt Lewin at " http://wilderdom.com/theory/FieldTheory.html. Accessed 3 March 2010.

4. R. V. G. Clarke and Graeme R. Newman, *Outsmarting the Terrorists* (Westport: Praeger Security International, 2006).

5. Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia: University of Pennsylvania Press, 2008), 48.

6. Ronald V. Clarke, "Situational Crime Prevention: Its Theoretical Basis and Practical Scope," *Crime and Justice* 4 (1983), 225-256, p1.

7. Felson, 5.

8. Ibid.

9. Ibid., 6.

10. Ibid.

11. Ibid.

12. Pat Brantingham and Paul Brantingham, "Crime Pattern Theory," *Institute for Canadian Urban Research Studies*. Accessed 2 February 2010.

13. Ibid.

14. Felson, 7.

15. Ibid., 14.

16. Ibid., 7.

17. Ibid.

18. Clarke and Newman, 9.

19. Ibid.

20. Graeme R. Newman, "Reducing Terrorist Opportunities: A Framework for Foreign Policy," *Crime Prevention Studies* 25 (2009), 33-60.

21. Rachel Boba, "EVIL DONE," Crime Prevention Studies 25 (2009), 71-92. Boba scales the criteria to develop a methodology to score and rank targets consistently across target types and between different analysts.

22. Newman, 33-60.

23. Ibid.

24. Clarke and Newman, 117.

25. Newman, 33-60.

26. Clarke and Newman, 117.

27. Newman, 33-60

28. Ibid.

29. Ibid.

30. Clarke and Newman, 188-189.

31. Ibid., 189.

32. Sageman, 177.

33. Clarke and Newman, 6.

34. Ibid.

*Major Gibbs is a Psychological Operations Officer currently assigned to the Naval Postgraduate School (NPS) in Monterey, California. He is pursing Master of Science Degrees in Defense Analysis and Joint Information Operations. Prior to attending NPS I was assigned to the 1st PSYOP BN at Fort Bragg, North Carolina. He has served as a PSYOP Operational Detachment Commander, HSC Commander, and the Battalion Assistant Operations Officer and deployed twice to Iraq in support of OIF.*

# Bringing Baker Street to Fort Huachuca:
## Enlisting Sir Arthur Conan Doyle to Teach Intelligence Analysis
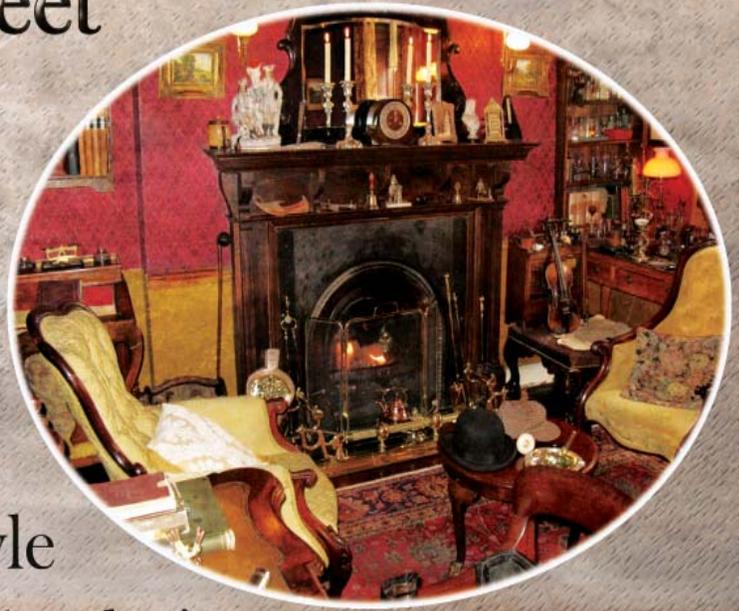


**by Captain Julie Paynter**

## Introduction

The best mechanic is the one who understands how and why an engine (or any other mechanical apparatus) works, and the best small unit tactical leader is the one who understands tactics as opposed to just being able to reproduce a diagram in a field manual. Likewise, the best intelligence officers understand the basis of doing intelligence analysis and use that ability to adapt to the constantly changing conditions in combat, particularly in a counterinsurgency (COIN) environment. It is of little use to be able to produce the products needed for steps 1 through 4 of the intelligence preparation of the battlefield (IPB) process if one is unable to provide a clear and coherent analysis, or bottom line up front, for the commander. Yet too often this critical skill appears overlooked as intelligence professionals are taught what procedures to use, products to make, and the best ways to present information.

While these skills are necessary, they are all meaningless if the analysis behind the product or the presentation is shallow or flawed. Perhaps this is part of the reason that Major General Flynn contends that Microsoft Word, not PowerPoint, should be the tool of choice for intelligence analysts.[1] Some individuals have a natural analytical ability, others need training to learn to analyze and think critically and methodically about problems. What is clear is that using PowerPoint presentations will not fill this gap. This article will propose a method for using fiction to teach intelligence personnel how to think under the conviction that once a person understands this they can learn the procedures and processes that are so heavily emphasized in the U.S. Army Training and Doctrine Command's materials such as field manuals and training circulars.

## Sherlock Holmes–Intelligence Analyst

A common complaint about the intelligence profession and junior enlisted analysts in particular, is that they cannot communicate clearly in writing. When once asked the best way to improve SAT verbal skills, a college admissions advisor responded simply: "Read." Reading quality writing is something that most analysts do too little of for various reasons. Two key reasons for this are an increasing reliance on visual media (It is not uncommon to hear someone say "No, I didn't read it, but I did see the movie") and the inaccessibility of professional reading lists.

The current *Center for Military History's Reading List for Cadets, Soldiers and Junior NCOs* includes 11 works, some of which, like John Keegan's *The Face of Battle*, are undeniably dense.[2] Similarly, the Fort Huachuca Commanding General's Reading

List contains over 100 works broken down into various categories like Iraq, Afghanistan, Iran, etc. Of the entire 120, only two are fiction (*Once an Eagle* and *The Bridge on the Drina*) and few are first person narratives, such as *If You Survive*, which are often more relatable and readable. I am not arguing with the merits of the works, but with the fact that they are increasingly inaccessible to a generation raised on YouTube, the ESPN 10 Second highlight, and text messaging.

A common theme of the reading lists is that they often overlook fiction. While it would be unwise to rely solely upon novels to learn about the geography of sub-Saharan Africa, it is equally unwise to disregard the merits of fiction as a teaching tool. It is engaging, varied and often more easily understandable than military scholarship. During an iteration of a course on Advanced Analytics, the most discussed reading was a large section of Orson Scott Card's *Ender's Game*, easily the most accessible reading in the course. Another common novel mentioned as a teaching tool is *The Ugly American,* which is a thinly veiled criticism of the typical American foreign civil servant.

Perhaps the best example of using fiction as a teaching tool are *The Defence of Duffer's Drift* by Major General Sir Ernest Swinton and its more recent companion, *The Defense of Jisr al Dorea* by Michael L. Burgoyne and Albert J. Marckwardt. Military Science professors and commanders at every level of maneuver use the vignettes to teach tactics to small unit maneuver leaders because they are memorable, easy to read and full of teaching points. Unfortunately, there is nothing similar specifically for the tactical intelligence officer or analyst. One solution is to look to one of the original fictional analysts and one of the best-known characters of all time: Sherlock Holmes. The short stories by Sir Arthur Conan Doyle have many excellent attributes for use in an intelligence curriculum. They are well written, engaging, and most people have at least a passing familiarity with the material. As well as being short and concise, they most importantly demonstrate many of the techniques commonly used in intelligence work. Those techniques include Human Intelligence (HUMINT), the importance of local culture and history, the use of network and pattern analysis, tactical patience and information discernment.

## Critical Information or "White Noise"?

It is the last of these techniques, information discernment, which is increasingly relevant as our main problem becomes too much information rather than too little. The intelligence professional has to be able to determine what is relevant, what is critical, and what is "white noise." Conan Doyle highlights the criticality of this skill in *A Study in Scarlet* when Holmes astonishes Watson by admitting that he didn't know that the earth revolved around the sun. More astonishingly, he promptly vows to forget the fact stating that

> ***"...It is a mistake to think that that little room [the human brain] has elastic walls and can distend to any extent. Depend upon it, there comes a time when for every addition of knowledge you forget something you knew before. It is of the highest importance, therefore, not to have useless facts elbowing out the useful ones".[3]***

One could argue the usefulness of planetary mechanics but to Holmes the concept was irrelevant, just as much that might seem relevant in COIN is not and vice versa. For example, Holmes' comprehensive knowledge of cigar ash seems random and useless just as knowledge of the historical pastures in rural Afghanistan might seem at first glance. Holmes, however, solves several crimes by discerning what type of cigar the culprit was smoking. The fact that a shepherd is in the wrong pasture might be the hint that a terrorist attack is imminent. Relevance, like beauty, is in the eye of the beholder, but it is critical to know that not all information is created equal.

## Holmes on HUMINT

Another area where the intelligence professional can learn from Holmes is in the use of HUMINT. Most COIN experts, to include the authors of FM 3-24, Counterinsurgency and FM 3-24.2, Tactics in Counterinsurgency, note that HUMINT is the most critical type of intelligence in fighting an insurgency, which in combating the criminal undercurrents of Victorian London is essentially what Holmes was doing. The stories provide myriad examples of HUMINT used well, and poorly, most notably in *The Solitary Cyclist*. Holmes sends Watson to a small town to try to garner information on a few of the neighborhood's occupants. Watson returns and proudly reports, much to Holmes' derision, that he interviewed the leasing agent for the

home in question. Holmes' disgust is obvious and he suggests that Watson should have:

> *"gone to the nearest public house. That is the centre of country gossip. They would have told you every name from the master to the scullery maid….What have we gained by your expedition?...That the Hall is tenanted by Williamson. Who's the better for that?"*[4]

Later in the story, Holmes does indeed visit a public house and is able to elicit the information that he needs. This story could easily be a modern day parallel of the leaders and analysts who rely on information from host nation governments and official channels rather than attempting to ask those who might really know–the local populace. In *The Sign of Four*, the reader is introduced to Holmes' informal HUMINT network, the Baker Street Irregulars, a gang of "street Arabs" who can "go anywhere, see everything, overhear anyone."[5] While the Army can't employ children as sources, this is strikingly similar to some of the known reconnaissance and intelligence gathering techniques of both Al Qaeda and the Taliban.

## Cultural and Historical Awareness

One of the areas where the U.S. Army is most lacking is in cultural and historical knowledge of the areas we are currently fighting (Iraq, Afghanistan) or are likely to be (Africa). Here lies another area where Conan Doyle was years ahead of the contemporary COIN and law enforcement doctrine. In *The Valley of Fear*, Holmes offers a pamphlet on the history of the house in which the crime was committed to the responsible Scotland Yard inspector who refuses the offer scornfully. Holmes calmly responds that,

> *"Breadth of view, my dear Mr. Mac, is one of the essentials of our profession. The interplay of ideas and the oblique uses of knowledge are of extraordinary interest" (2: 225).*[6]

In this case, the key to the crime is that the home contains a hiding spot previously utilized by King Charles, and the pamphlet noted its presence. While no real life problem is this neatly wrapped, the fundamental point is that local knowledge is irreplaceable and Doyle makes it in such a fashion that the reader remembers its criticality.

Throughout the stories, but particularly in *The Final Problem*, Holmes battles a man, Professor Moriarty, who is according to Holmes, "the orga-

nizer of nearly half that is evil and all that is undetected in this great city." More importantly, to the COIN analyst the central figure is much like the head of an insurgency as "He only plans…The agent may be caught…but the central power which uses the agent is never caught-never so much as suspected."[7] Holmes, however, is able to unravel the threads of his web following a small mistake that allowed him to trace the network and find both the central figure and his direct subordinates providing an excellent lesson in the importance of link and network analysis.

Perhaps more important is the fact that Doyle, through Holmes, demonstrates the importance of tactical patience in conjunction with defeating the network. Throughout the story Holmes' life is threatened (he is eventually killed…for a while), but he refuses to have the criminal arrested. When pressed by Watson, he explains, "It would be to ruin the work of three months. We should get the big fish but the smaller would dart right and left out of the net".[8]

The story also shows the danger of capturing only the small fish, as Moriarty eventually escapes and initiates a fatal encounter with Holmes. The subsequent story, *The Empty House*, has one of Moriarty's subordinate leaders attempting to reconstitute the network. Taken together, the two demonstrate the need for accurate network analysis and the need for tactical patience to ensure that the network can't easily reconstitute or, perhaps worse, fracture and then germinate similar to Al Qaeda in Iraq following the death of Abu Musab al Zarqawi.

## Pattern Analysis

One of the most heavily taught and used techniques for intelligence analysis is pattern analysis. In *The Five Orange Pips*, murderers target three family members after sending a letter containing five orange seeds. From basic assumptions about the postmark locations and dates of the letters, Holmes is able to determine that the criminals are part of a crew on a sailing ship. He is forced to spend a large amount of time correlating the dates and locations to a log of all the sailing ships entering port in England in order to determine the specific ship that is the most critical portion of this example.

Holmes drew upon outside data and painstaking research to discern the pattern, which, as anyone who has done pattern analysis knows, is extremely realistic. For example, sniper attacks at a certain location and time may be due to a repetitive patrol schedule but the analyst has to correlate patrol routes and times with sniping events to discover the pattern. Or improvised explosive device emplacement might be conducted by a farmer taking crops to market but that won't be evident unless common routes and pattern of life for farmers in the area are tediously mapped.

There are countless examples of times when knowing that something was out of place was key to stopping a terrorist attack. Brigadier General Wayne Hall and Dr. Gary Citrenbaum dub this technique Anomaly Analysis, defined as "discerning meaning in departures from the normal or common order, form or rule; absence of that which is expected".[9] Conan Doyle's writing provides one of the most memorable instances of anomaly analysis. In *Silver Blaze*, Holmes investigates the disappearance of a valuable racehorse from his stable. When asked by the local police if there are any points that he wants to make, Holmes states "To the curious incident of the dog in the night time" to which the officer responds "The dog did nothing in the night time." "That," quips Holmes "was the curious incident".[10]

That the dog didn't bark leads Holmes to conclude that someone who knew the dog took the horse from the stable rather than the marauding stranger who is the popular suspect. Another example, though not as pithy, comes from the same story when Holmes deduces from the fact that three sheep have inexplicably gone lame in the nearby pasture that the horse's trainer was going to try to lame him tempo-

rarily. Such seemingly innocuous occurrences are critical to determining when an attack is going to take place–for example, when children aren't playing in a street or when a market is less crowded than typical–or what neighborhoods have recently been infiltrated, or many other aspects of unraveling an insurgency.

## Predictive Analysis

Perhaps the most difficult aspect of intelligence work is predictive analysis but it also one of the most critical. Doctrine states that IPB contain an Enemy Most Likely Course of Action and an Enemy Most Dangerous Course of Action, which are simply predictive analyses regardless of whether it is a high intensity conflict or COIN environment. Once again, Doyle provides an easily teachable example of successful predictive analysis. In *The Red Headed League*, Holmes is able to prevent a massive bank robbery based on what appears to be a practical joke played on a pawnshop owner. Holmes' initial suspicions are aroused against the man's assistant because he works for half-wages (an anomaly), and are further heightened by the assistant's reported interested in photography and constantly "diving down into the cellar like a rabbit into its hole to develop his pictures".[11]



Holmes, however, strolls by the shop and notes dirt covering the man's trouser knees, allowing him to deduce that the assistant has been tunneling. Looking at maps of the area, it is evident that the target is the nearby bank. While this is a vastly oversimplified summary of the story, and the story

itself is much simpler than tracing an insurgent cell in a teeming city like Mosul or the remote Pashtun region of Afghanistan, it is still a valuable lesson in the importance of using indicators to predict future activity and to get inside the enemy's decision cycle.

## Intelligence Report Writing

Writing intelligence reports is tedious and difficult, but it is imperative that the report or summary contain all relevant information to allow the reader to draw conclusions. While the summary should itself contain analysis, there might be other conclusions that can be drawn and which will be lost if all of the information is not coherently written. In a nod to MG Flynn, Conan Doyle's stories also present an excellent text for learning to write. They are clearly cataloged, all relevant information is presented and the focus on nuance and meaning in the prose is an invaluable lesson to the writers of intelligence summaries, especially those tempted to use a thesaurus to liven up the document. For example, in *A Scandal in Bohemia* Holmes points out to Watson that he sees but does not observe.

> *" 'Quite so,' he answered...'You see, but you do not observe. The distinction is clear. For example, you have frequently seen the steps which lead up from the hall to this room.'*
>
> *'Frequently.'*
> *'How Often?'*
> *'Well, some hundreds of time.'*
> *'Then how many are there?'*
> *'How many? I don't know.'*
> *'Quite so! You have not observed. And yet you have seen. That is just my point. Now, I know that there are seventeen steps, because I have both seen and observed' "*[12]

There are quite a few lessons to draw from this passage, but one major point is the power of the nuances of written language and the importance of word choice in writing.

While it is Holmes' methodical deductions that present the most lessons for conducting analysis, the stories also highlight the importance of having the ability to write. *The Adventure of the Blanched Soldier*, written by Holmes rather than Watson, his faithful biographer best demonstrates this. Doyle presents the tale much less coherently in terms of reaching a conclusion and it reads more like a treatise or a dissertation. It is proof of Holmes' statement that he is "...lost without my Boswell" ("A Scandal in Bohemia".)[13] Pretending for a moment that the two characters actually existed, if it weren't for Watson, Holmes would still have been a deductive genius, but would anyone have known or cared? Similarly, an intelligence analyst may do excellent analysis that could save lives and lead to dismantling an insurgent cell, but if that analyst can't convey their information, is it of any use?

## Conclusion

Thus, much like *The Defence of Duffer's Drift* for the maneuver Soldier and leader, the Sherlock Holmes stories bring together in an easily accessible and teachable forum the two most important traits for any intelligence professional: the ability to think critically and the capability to convey that analysis to others in writing. There are many other lessons to draw from the stories as well. One could use Holmes' investigations of crime scenes to teach Site Exploitation and his carefully alphabetized catalog of people and crimes is a useful example of the importance of recording and organizing all conceivably relevant data, to name but two.

Most importantly, the lessons are interactive and memorable. As one writer put it, "It is not only that once you have read Sherlock Holmes you never forget him; it goes far deeper than that; it is that you felt there was a never a time when you had not read him".[14] This is not a comment that will ever describe intelligence doctrine. It is not possible to teach all the skills that an intelligence analyst needs through fiction alone. However, much can be taught, with the advantage that it is more easily accessible and comprehensible than doctrine and it is memorable meaning that it may increase retention and later use. Most importantly, the forced interaction inherent in reading and discussion, rather than the passive nature of receiving a PowerPoint presentation, means that the student understands rather than mimics, the skills taught allowing the analyst to manipulate and apply them to the many varied situations found in a COIN intelligence environment.

## Endnotes

1. MG Michael T. Flynn, CPT Matt Pottinger, and Paul D. Batchelor, *"Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan,"* Voices from the Field, January 2010, 23-24.

2. U.S. Army Center for Military History, *Recommended Professional Reading List: SUBLIST 1–Cadets, Soldiers, Junior NCOs*, 8 June 2009. Retrieved 20 February 2010 at http://www.history.army.mil/html/reference/reading_list/list1.html.

3. Arthur Conan Doyle, *Sherlock Holmes: The Complete Novels and Stories* (2 Volumes) (New York: Bantam, 1986), Vol. 1:13.

4. Ibid., Vol. 1: 841.

5. Ibid., Vol. 1: 184-185.

6. Ibid., Vol. 2: 225.

7. Ibid., Vol. 1: 740.

8. Ibid., Vol. 1: 748.

9. BG Wayne Michael Hall, (Ret.) and Gary Citrenbaum, PhD, *Intelligence Analysis: How to Think in Complex Environments* (California: ABC CLIO), 2010.

10. Doyle, Vol. 1: 540.

11. Ibid., Vol. 1: 267.

12. Ibid., Vol. 1: 241-242.

13. Ibid., Vol. 1: 243.

14. Theodore Dalrymple, "The Eternal Detective" *National Review Online*, 31 December 2009. Retrieved 13 March 2010 at http://nrd.nationalreview.com/article/?q=MWRlMGYwN2I0YjdkZDY1MWM5ODk1NjJmYzM0YTc2ZTU.

*Captain Paynter is currently assigned to HHC, 504th BfSB at Fort Hood, Texas. She has served with the 3rd Armored Cavalry Regiment as an MI Company XO and the Regimental Assistant S2 during OIF 07-09, and as the Speechwriter to the III Corps and Fort Hood Commanding General.*

FORT HUACHUCA 1877

# 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 sterilla.smith@us.army.mil. Our fax number is 520.538.1005. Submit articles by mail on disk to:

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

Contact phone numbers: Commercial 520.538.0956 DSN 879.0956.

# The Military Intelligence Corps 2011 Hall of Fame Inductees

**Colonel G. Dickson Gribble, Jr. (U.S. Army, Retired)**

Colonel G. Dickson Gribble, Jr. entered the Army in 1969 and attended the Engineer Officer Candidate School. Lieutenant Gribble was then assigned to Germany, where he served in company level positions such as Company Executive Officer and Assistant Operations Officer, culminating with assumption of command of Bravo Company, U.S. Army Security Agency Field Station in Rothwesten, Germany.

In 1976, Captain Gribble was selected as an instructor for the Military Intelligence (MI) Officer Advanced Course. In 1979, he assumed the duties and responsibilities as Operations Officer for the 14th Signal Regiment (EW), British Army of Rhine– the British Army's only tactical Signals Intelligence (SIGINT) and Electronic Warfare (EW) unit. Drawing on knowledge gained during his tenure at the Intelligence Center, CPT Gribble was instrumental in developing and refining operational concepts for SIGINT/EW support to tactical forces operating in the British General Deployment Plan operational area.

In 1984, Major Gribble was assigned as the Majors Assignment Officer and later as the Chief, MI Branch, at the U.S. Army Personnel Center in Arlington, Virginia. At this time, he managed more than 750 majors and approximately 2,800 lieutenants and captains.

Lieutenant Colonel Gribble, while serving as the Commander, 204th MI Battalion, 66th MI Brigade in Germany, worked with Field Station Augsburg leadership to develop and exercise a plan to transition the Field Station's strategic mission from its fixed station base to mobile wartime operations. During back-to-back assignments as the Director, National Security Agency (NSA), Fellow and Chief of SIGINT Plans and Policy on the DCSINT staff, LTC Gribble became the Army lead for the emerging Regional Signal Operations Center concept.

In 1992, Colonel Gribble assumed command of the 704th MI Brigade, which included the Army Technical Control and Analysis Element. In 1996 during his command at the 713th MI Group and Menwith Hill Station in the United Kingdom,

Menwith Hill Station was selected as the Army's best SIGINT operation and represented the U.S. Army in the annual Travis Trophy competition. His accomplishments were also recognized by award of the prestigious U.S. Ambassador's Award for excellence in British/American programs.

After 30 years of distinguished military service, in 1999, Colonel G. Dickson Gribble, Jr. concluded his military career as Chief, Global Access Division, Directorate of Technology at NSA. His awards include the Defense Superior Service Medal with Oak Leaf Cluster, the Legion of Merit with Oak Leaf Cluster, the Meritorious Service Medal with four Oak Leaf Clusters, the Army Commendation Medal, three Armed Forces Expeditionary Medals, and two Humanitarian Service Medals.

## Chief Warrant Office Five Alfred J. Myles (U.S. Army, Retired)

Chief Warrant Officer Five Alfred Myles entered the Army in July 1971 and completed basic training at Fort Polk, Louisiana. In 1974, then Specialist Myles attended Imagery Intelligence (IMINT) Analyst training at Fort Huachuca, Arizona, and was then assigned to Company A, 1st MI Battalion at Fort Bragg, North Carolina. While at Fort Bragg, he became the NCOIC of the Imagery Section with the FORSCOM Mobile Training Detachment which trained active, reserve, and National Guard units in MI tactics, techniques, and procedures.

In 1978, Staff Sergeant Myles was assigned to the Doctrine Development Division at Fort Huachuca, where he wrote the Army correspondence course and Skill Qualification Test for IMINT Analysts. In February 1981, SSG Myles was directly appointed to Warrant Officer One and assigned to the Intelligence, Threat and Analysis Center (ITAC) in Washington, D.C. During his time at ITAC, Chief Myles was a major contributor to the discovery of the new Soviet main battle tank (T-80).

In 1983, Chief Myles was assigned to the Imagery Detachment, 470th MI Group at Fort Clayton, Panama. During this assignment, he spearheaded the imagery support to the U.S. Embassies, U.S. Southern Command, and its allies in Central and South America. Chief Myles was instrumental in developing imagery signatures to identify insurgent and drug trafficking activities. He also coordinated the layout of a giant mosaic to support the security

efforts for the El Salvadorian Peace Talks in 1984.

In 1997, as a Chief Warrant Officer Four, he was assigned to the MI Warrant Officer Training Branch as Course Manager for the IMINT Technician Certification Course. In 1998, CW4 Myles became the Imagery Advisor to the Saudi Arabian Intelligence School in Al Khaj, Saudi Arabia, where he spearheaded the development of an Imagery Advanced Course and taught the Saudi Arabian cadre how to teach this course. In 2000, Chief Myles became the first IMINT Warrant Officer to achieve the rank of Chief Warrant Officer Five, the highest rank a Warrant Officer can achieve.



Chief Myles completed his 33 year Army career at Fort Huachuca assigned as the Chief, Warrant Officer Training Branch where he was a major contributor to the Warrant Officer training and development programs and the Officer Education System. Chief Warrant Officer Five Myles' awards include the Legion of Merit, four Meritorious Service Medals, three Army Commendation Medals and two Army Achievement Medals.

## Colonel William Torpey (U.S. Army, Retired)

Colonel William Torpey was commissioned as an MI officer after graduating from Officer Candidate School in 1970. Immediately upon completing MI Officer Basic training, Lieutenant Torpey was assigned to the 8th Infantry Division, Baumholder, Germany, in the first wave of MI Officers assigned as S2s to combat maneuver units in Europe. He served three highly successful years as an Armor Battalion and Infantry Brigade S2.

Upon return from Europe, LT Torpey served as an instructor and company commander at the Army Intelligence School, Fort Devens, Massachusetts. Upon completion of the MI Officer Advanced Course, Captain Torpey was assigned to the 2nd Infantry Division, Korea, where he commanded the 329th Army Security Agency Company, providing multidiscipline intelligence collection along the Demiltiarized Zone.

In 1979, CPT Torpey was assigned to Fort Meade, Maryland as an Operations Officer, Battalion Executive Officer and S3 of the 704th MI Brigade. As the operations officer for the newly established Army Collection, Processing, Analysis and Reporting element at the National Security Agency, he was responsible for coordinating national agency support to tactical forces. This was one of the MI's first successful reachback operations.

In 1984, Major Torpey returned to Germany where he served as the Imagery Intelligence (IMINT) Officer, 66th MI Brigade, responsible for synchronizing theater IMINT force structure and imagery support to U.S. ground forces. He later served as Executive Officer, 204th MI Battalion and as the Commander, 108th MI Battalion, deployed along the East German border.

Lieutenant Colonel Torpey was assigned to Fort Leavenworth, Kansas in 1989, as the Intelligence Observer Controller in the Battle Command Training Program and as an instructor in the Tactical Commanders Development Course where he advanced the intelligence battlefield operating system.

In 1991, LTC Torpey assumed the position of MI Branch Chief on the heels of the first Gulf War when the Army's Officer Corps would be reduced by 33 percent. LTC Torpey and his management team implemented efficiencies, preserved force structure, and established positive rapport with the field to sustain an aggressive MI career development program.
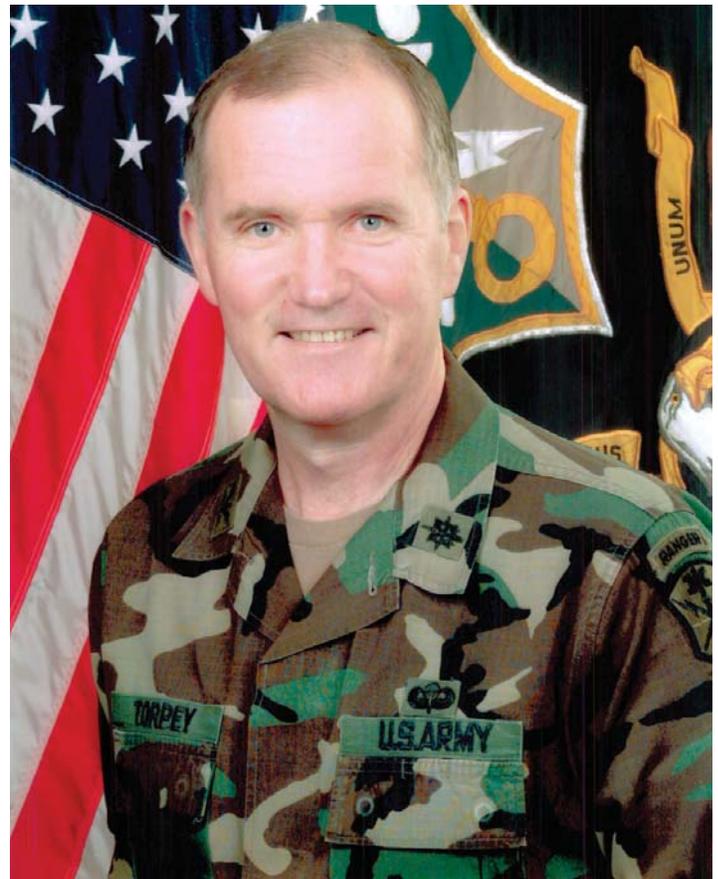


Colonel Torpey was selected as the Defense Attaché to Ireland in 1994, where he spearheaded efforts to modernize a neutral country's defense force, promoted bi-lateral training opportunities and contributed to Ireland's participation in Partnership for Peace. In 1998 he concluded his distinguished 30 year career as the Deputy Commander of the U.S. Army Intelligence and Security Command.

Colonel Torpey's awards include the Distinguished Service Medal, Defense Superior Service Medal, Defense Meritorious Service Medal, Meritorious Service Medal with four Oak Leaf Clusters, Army Commendation Medal with three Oak Leaf Clusters, Defense Service Medal with Bronze Service Star and the Army Service Ribbon. Colonel Torpey is a graduate of the U.S. Army Airborne and Ranger Schools.

# 2012 Military Intelligence Corps Hall of Fame Nomination Criteria



1. Commissioned Officers, Warrant Officers, Enlisted Soldiers or professional civilians who have served in a Army intelligence unit or in an intelligence position in the U.S. Army are eligible for nomination.

2. Only nominations for individuals will be accepted. Individuals cannot self-nominate. No unit or group nominations will be considered.

3. Nominees may not be serving on active duty and must have been retired a minimum of three years before consideration; however, they may be employed by the U.S. Government in either a civilian or contractor position, to include continued service in an intelligence role. Government civilians who have not previously served in uniform but who are otherwise qualified and have been retired a minimum of three years may be considered.

4. Temporary retirees for medical or other reasons and members of the Active Reserve or National Guard are not eligible until they have transitioned to permanent inactive or retired status.

5. Although nominees must have served with Army intelligence in some capacity, the supporting justification for their nomination may include accomplishments from any portion of their career, not merely their period of service in Army intelligence. For example, an NCO who served in Army MI and then, after retirement joined the Defense Intelligence Agency as a civilian, is eligible for Hall of Fame consideration once he/she has been retired three years from service in uniform, by virtue of his or her Army service. However, his or her justification may include achievements from both military and civilian careers, even though his or her civilian intelligence service was not in an Army intelligence unit.

6. A nominee must have made a significant contribution to Military Intelligence that reflects favorably on the Military Intelligence Corps. When appropriate, the nomination may be based on heroic actions and valorous awards rather than on documented sustained service and a significant contribution to Army intelligence.

**Nominations should be sent to:**

Office of the Command Historian, U.S. Army Intelligence Center, ATTN: ATZS-HIS, 1889 Hatfield Street, Building 62723, Fort Huachuca, Arizona 85613-7000. DSN 821-4113 or commercial (520) 533-4113. Email: lori.tagg@us.army.mil or timothy.quinn@us.army.mil. Nominators will be notified of a packet's receipt and the date of the next Nomination Board.

# LTG Sidney T. Weinstein Award for Excellence in Military Intelligence Criteria

In 2007, the LTG Sidney T. Weinstein Award for Excellence in Military Intelligence (MI) was established to recognize the outstanding achievements of one Army captain within the MI community who embodies the values and ideals for which the late General Weinstein stood. General Weinstein, who passed away in 2007, is fondly remembered as the father of modern MI. He was a leader, mentor, role model, friend, and dedicated family man. He once said about MI Soldiers, "[You've] got to be tactically and technically proficient, but by God, *Duty, Honor, Country*' is not a bumper sticker."

Nominations are being accepted for the 2012 Weinstein Award through March 2, 2012. To be eligible, a candidate must be an MI Officer of the rank of Captain in the Active Army, Army Reserve, or Army National Guard. He/she must have performed actions which positively promote, impact, advance, and bring honor to the MI profession during the period January 1 to December 31, 2011. The candidate must possess either an MI Officer Area of Concentration (AOC) or a 15C AOC, be fully eligible for continued service for at least one year after award presentation (i.e., through June 2013), and not in a promotable status as of September 30, 2012. No posthumous awards will be presented.

Candidates also must meet the height and weight standards specified in AR 600-9, maintain a current passing grade on the Army Physical Fitness Test (waived for deployed nominees unable to take the APFT), and must not be under an unfavorable personnel or UCMJ action. Recipients of the Weinstein Award are recognized annually at a luncheon during the MI Corps Hall of Fame Week in September at Fort Huachuca, Arizona.

Nominations for the 2012 Weinstein Award must be received no later than March 2, 2012. Mail complete nomination packets to Command Historian, ATTN: LTG Sidney T. Weinstein Award, U.S. Army Intelligence Center, 1903 Hatfield Street, Fort Huachuca, Arizona 85613-7000. Soft copy nominations may also be emailed to lori.tagg@us.army.mil. For questions/assistance or to obtain full nomination procedures, please contact Lori Tagg at (520) 533-4113/DSN 821-4113.



**1987**

**Defining Moments in MI History**

**ALWAYS OUT FRONT**

The Military Intelligence Corps was activated on 1 July at Fort Huachuca as a part of the U.S. Army's regimental system, a move that was approved by the Chief of Staff of the Army in December 1985. The Commandant of the U.S. Army Intelligence Center and School also became the Chief of Military Intelligence concurrent with the activation of the corps. The MI Corps became the first branch to include civilians.

"[The establishment of the Military Intelligence Corps is] a recognition and celebration of our evolution from a plethora of diverse and separate intelligence agencies into the cohesive Military Intelligence community we enjoy today."
-MG Julius Parker, Chief, Military Intelligence, upon the activation of the MI Corps, 1987

TRADOC CULTURE CENTER
ONE STOP SHOP
FOR ALL THINGS CULTURE

**The TRADOC Culture Center (TCC) is your culture center and the Army's One-Stop-Shop for all things culture related. Service Members are the customer, and the TCC tailors products and training to meet the needs of the customer.**

Smart Books : Smart Cards : Pocket Guides : Interactive Training : Videos



**BG Gregg C. Potter**

**CG, USAICoE
Fort Huachuca**

### Why is Culture Important?

Cross-cultural competency (3C) is a critical combat multiplier for commanders at all levels that enables successful mission accomplishment. Possessing cultural understanding is one of the critical components for Soldiers who interface with the local population. At a minimum, soldiers must possess cultural awareness. Leaders must demonstrate cultural understanding and be proficient in applying cultural knowledge effectively to achieve mission objectives. The TCC can help Soldiers gain this mission essential proficiency. Lessons learned from 10 years of operational deployments clearly indicate that 3C is a huge and indispensible combat multiplier.

⭐ **OVER 160,000 SERVICE MEMBERS TRAINED** ⭐

The TCC supports Soldiers and leaders throughout the Army and other services in numerous ways. It conducts ARFORGEN/predeployment training for any contingency; trains culture trainers; and produces professional military education (over 160,000 military personnel trained since 2004). The TCC will create or tailor any products deploying units require.

**SMART CARDS**



The TCC has developed several distance learning products available for facilatated instruction or individual student use. As an example, two seasons of "Army 360" that the TCC produced contain 19 episodes of missions run in six countries. "Army 360" is an interactive media instruction (IMI) training product which meets the Army Learning Concept 2015 learner-centric requirements. The TCC is in the process of turning the "Army 360" IMI into digital apps which will be easily accessible for all Soldiers. The TCC produced an Initial Military Trainee (IMT) training product for the initial entry level Soldier called "IMT-BCT What is Culture?" We are also producing a BOLC IMI product. Both products are or will be available via the TCC website. The TCC is expanding other products into the apps arena as well as developing additional distance learning products to provide new 3C training and sustainment.

**INTERACTIVE TRAINING**



ARMY 360°

IMT-BCT

**SMART BOOKS**



The TCC produces cargo pocket-sized training products to include smart books and smart cards, as well as digital downloads for smart devices. Areas covered include Iraq, Afghanistan, North Korea, Democratic Republic of Congo, and more. Let us know what we can produce for you. For a complete list of materials, see:

**https://ikn.army.mil/apps/tccv2/**.

The TCC is your One-Stop-Shop to achieve individual and unit 3C. We will do whatever you require to help you accomplish your mission. Let us know what the TCC can do for you, your One-Stop-Shop for all things culture.

**REQUEST TRAINING NOW!**

at https://ikn.army.mil/apps/G3MTT/

Specify what the unit needs are and we will deliver training that fits your objectives.

**DOWNLOAD TRAINING TO YOUR SMART PHONE:**
https://ikn.army.mil/apps/tccv2/

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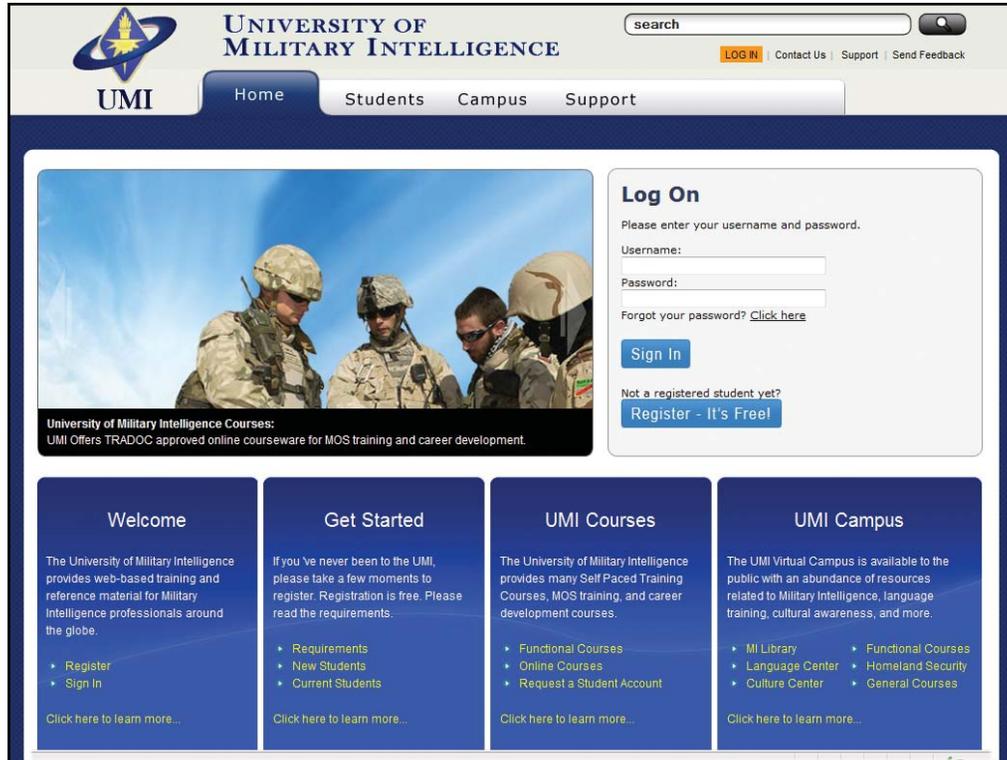


**The University of Military Intelligence (UMI)** is a training portal of MI courses maintained by the U.S. Army Intelligence Center of Excellence (USAICoE) at Fort Huachuca, Arizona for use by authorized military (Active, Reserve, National Guard) and non-military (e.g., DOD civilian, Department of Homeland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

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

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

---

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

---

# Defining Moments in MI History



When the American Black Chamber closed down, the Army decided to enlarge its cryptology operations and appointed William Friedman as Chief Cryptanalyst of the U.S.Army Signal Corps. In 1930 the Signals Intelligence Service was created, staffed by Friedman, three junior cryptanalysts and two clerks. In 1940 they cracked the Japanese PURPLE machine cipher. The deciphered messages were called MAGIC and restricted to only a handful of men in the government. Asked what effect Signals Intelligence had on World War II, an admiral exclaimed, " It won the war."

---

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

# Captain Nadia L. Traylor
## 2011 Recipient
## Lieutenant General Sidney T. Weinstein Award
## for Excellence in Military Intelligence





Captain Nadia L. Traylor was born in Kingston, Jamaica and was raised in Waldorf, Maryland. She attended Florida A&M University, where she reigned as the 2003-2004 Ms. Army ROTC, and graduated magna cum laude with a Bachelors degree in Criminal Justice and a concentration in Juvenile Delinquency.

In 2004, she was commissioned a Military Intelligence (MI) Officer and attended the MI Officer Basic Course at Fort Huachuca. Upon graduation, Captain Traylor was assigned to 2nd Squadron/17th Cavalry, 101st Combat Aviation Brigade, 101st Airborne Division (AASLT) as the Squadron Assistant S2 in support of Operation Iraqi Freedom (OIF) IV. While deployed she was selected as the Human Intelligence Platoon Leader in Bravo Company, 1st Special Troops Battalion, 1st Brigade Combat Team.

Following the deployment, Captain Traylor was selected to serve as the Bravo Company Executive Officer prior to attending the MI Captains' Career Course at Fort Huachuca in April 2007. Upon graduation, Captain Traylor was assigned to 3rd Armored Cavalry Regiment (ACR) as the Signals Intelligence (SIGINT) Officer in support of OIF 07-09. Subsequently, she served as the Analysis Control Element Chief while maintaining the entire SIGINT mission for Ninewa Province consisting of five outstations and five Signal Terminal Guidance Teams.

Since redeployment in 2009, Captain Traylor has served as the 66th MI Company Commander, 3rd ACR. She trained and led her Soldiers into Operation New Dawn in 2010.

Her military awards and decorations include the Bronze Star Medal with one Oak Leaf Cluster; Meritorious Service Medal; Army Commendation Medal with two Oak Leaf Clusters; Iraq Campaign Medal; Global War on Terrorism Expeditionary Medal; Air Assault Badge; German Arms Proficiency Badge-Bronze, and the Knowlton Award.

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

PIN: 102237-000