FM 2-0

MIPB

Military Intelligence Professional Bulletin

April-June 2010 PB 34-10-2

INTELLIGENCE

"Intelligence in Full Spectrum Operations"

FROM THE EDITOR

This issue features two articles by Colonel Franz, Chief, Information Dominance Center (IDC), ISAF and Lieutenants Colonel Pendall and Steffen on how the International Security Assistance Command has implemented an information–sharing architecture to create a comprehensive common operating picture across the Afghan theater. The IDC is the most decisive information and knowledge management effort ever executed in Afghanistan with a focus on governance and development, key aspects that most impact the daily lives of Afghans.

Colonel Cox presents the case for a new intelligence discipline, Document Exploitation or DOMEX. He presents the historical context and follows through to today's operations with comments and recommendations. Major Harris and Captain Bronson describe lessons learned and observations from the deployment of the first active duty Maneuver Enhancement Brigade to Afghanistan with the mission to manage terrain and C2 operations. Major Assadourian discusses a holistic approach to developing security metrics. First Lieutenant Hancock explores the emerging field of Memetics and implications for memetic operations in the military environment. Claudia Baisini and James Nyce make a case for the inclusion of Experiential Learning techniques in traditional military training to meet the challenges of fighting in non-traditional operating environments. Chief Warrant Officer Two Negron discusses the capabilities of the Tactical Exploitation System-Forward for use in a Communications Intelligence function. Vee Herrington, USAICoE's Chief of the U.S. Army's MI Library at Fort Huachuca, describes an ongoing experiment to incorporate eReaders into training.

Readers will also find articles on the 2010 MI Hall of Fame inductees and the 2010 recipient of the LTG Weinstein Award within the issue. As the Doctrine reengineering efforts continue, we offer a focus article on the recently released FM 2-0, Intelligence.

In an effort to catch up, the October December 2009 issue is now the July September 2010 issue. That means there will be no October December 2009 issue. You will find all of the articles and information scheduled for that issue in the July September 2010 issue. As the Editor, I apologize for any inconvenience to both the writers and readers of MIPB. If you have any questions regarding this please email to MIPB@conus.army.mil.

Mark your calendars: The 2010 Intelligence Warfighters Summit—The Critical Enabler for Full Spectrum Operations is scheduled for 6 through 10 December at Fort Huachuca.

Sterilla A. Smith
Editor

MILITARY INTELLIGENCE

PB 34-10-2 Volume 36 Number 2 April - June 2010

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

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

FEATURES

DEPARTMENTS

By order of the Secretary of the Army:
Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1018001

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

ALWAYS OUT FRONT

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

Currently, the intelligence warfighting function includes a formidable set of capabilities across all echelons from "mud-to-space." This flexible force of personnel, organizations, and equipment collectively provides commanders with the timely, relevant, accurate, predictive, and tailored intelligence they need. We provide the intelligence that continuously supports the commander in visualizing the operational environment (OE), assessing the situation, and directing military actions through intelligence, surveillance, and reconnaissance synchronization and the other intelligence tasks.

The intelligence warfighting function is comprised of nine powerful intelligence disciplines. Eight of those disciplines essentially feed the discipline of all-source intelligence which in turn is focused on the commanders' requirements. Technological advances have enabled single-discipline analysts to leverage other analysts and information and to conduct multi-discipline analysis to an extent not possible in the past. However, all-source intelligence is still the nexus that integrates information and intelligence from all units and the other intelligence disciplines.

Future OEs will be greatly impacted by globalization. "Globalization and growing economic interdependence, while creating new levels of wealth and opportunity, also create a web of interrelated vulnerabilities and spreads risk even further, increasing sensitivity to crises and shocks around the globe and generating more uncertainty regarding their speed and effect" according to the National Defense Strategy, June 2008.

Key aspects of globalization include—

- Non-state groups, organized crime, and cultural and environmental change will stress already fragile social and political structures.
- American science and technology communities, both commercial and Department of Defense, will compete with some growing economies for technical advantage.
- By 2020, organized crime is likely to thrive in resource-rich states now experiencing political and economic transformation.
- By 2025, urban growth will concentrate in coastal areas. The majority of urban populations will live within 60 miles of coastlines.
- By 2030, the world's urban population will be over 4.9 billion fostering:
  - Interdependent economies.
  - The interaction of differing societies and cultures.
  - More powerful non-state actors.
  - Porous international boundaries.
  - The inability of some nation-states to fully control their territory, economy, and to provide security and services.
- By 2030, competition for access to and control of natural resources (energy, water, and food) will dramatically increase areas of potential conflict.
- "…Cyber security risks pose some of the most serious economic and national security challenges of the 21st Century" according to the Presidential Cyberspace Policy Review, May 2009.

The Joint Operational Environment 2010 observes that, "with very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests. Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains."

In future OEs as U.S. forces conduct increasingly complex operations, Army intelligence will con-

(Continued on page 4)

CSM FORUM

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

Currently, the U.S. is in an era of persistent global conflict. It is a new era where our warfighters have to think outside the box to understand and defeat our enemies of today. MI Soldiers must learn and adapt the intelligence disciplines to support the warfighter in countering these threats to our Nation.

I will be retiring in June 2010 after 26 years of service to the U.S. Army and the Army Intelligence Corps and I would like to use this last opportunity to recount some of the MI success stories I have witnessed and to remind MI Soldiers about their heritage. MI personnel have been a part of the Army since its founding in 1775, but it wasn't until July 1962 that a number of intelligence and security organizations were combined to form this branch of service. On 1 July 1987, the MI Corps was activated as a regiment under the U.S. Army regimental system. Currently, most of the Corps falls under the U.S. Army Intelligence and Security Command (INSCOM). INSCOM had originally been formed to meet the intelligence needs of the Cold War. However, by adapting and tailoring its multi-discipline capabilities, the command had successfully positioned itself for the 21st century and is now prepared to confront an increasingly diverse world threat and the new menaces posed by terrorism, weapons proliferation, and cyber war.

Throughout my time as the MI Corps Command Sergeant Major, I visited many MI units from around the world to observe training and operations. With each visit, I noted great successes of our Corps. In the process, I have also noted areas where those units could improve. I've taken these notes back to the Intelligence Center of Excellence here in Fort Huachuca, Arizona to better improve the training we provide to new Soldiers of the Corps.

During my travels I have seen the greatness that there is in units such as the 525th Battlefield Surveillance Brigade (BFSB) which successfully completed a 15 month deployment to Iraq on December 2008 and is now preparing for another deployment in support of Operation Enduring Freedom. One of the many success stories for the 319th and 519th MI Battalions is Operation Defeat Al Qaeda in the North; an operation employing the gamut of intelligence sensors such as Human Intelligence (HUMINT), Counterintelligence (CI), Aerial Surveillance, Long Range Surveillance, and many more.

Another BFSB that has astounded me is the 504th out of Fort Hood, Texas. The 504th BFSB has come a long way since its first unit designation as the 137th Signal Radio Intelligence Company (Aviation) during World War II. Today, the 504th has a Network Support Company, a Forward Support Company, and a Long Range Surveillance Troop which further help our intelligence efforts across the globe.

Let us not forget our MI efforts in South and Central America, led mainly by the 470th MI Brigade. With its aerial exploitation, interrogation, and electronic warfare battalions, the 470th MI Brigade continues to fight the good fight for U.S. Army Southern Command in countries such as Colombia, Honduras, and Argentina.

I could continue to name all the MI units that bring the U.S. Army success, but I want to mention the one MI brigade whose battalions strive to the fullest to create the Intelligence professionals for today and the future–the 111th MI Brigade. The 111th continues to successfully shape and mold our HUMINT and CI Soldiers, our Intelligence Analysts, our Imagery Analysts, and our Signals Intelligence Soldiers, our Intelligence officers and warrant officers, and the newest addition to the Fort Huachuca School house–the MOS 09L Linguists.

We should all understand that we are a nation in multiple conflicts and the mission to handle each

(Continued on page 5)

tinue to prove even more critical by providing Army warfighting commanders with predictive, knowledge-based intelligence. As stated in the National Intelligence Strategy, August 2009, the Intelligence Community (IC) must ***"Operate as a single integrated team, employing collaborative teams that leverage the full range of IC capabilities*** to meet the requirements of our users, from the President to deployed tactical military units."

Some current conceptual documents postulate that future operations will be significantly different from past operations in which intelligence was merely viewed as a supporting operation. Today, and in the future, intelligence must not only drive operations but ***precisely*** drive operations. Therefore, Army intelligence must be prepared to:

- Operate in complex and urban terrain among the local population. This task requires a combination of existing and new technical means and expanded collection capabilities to exploit previously unexploited signatures.
- Develop a new Military Intelligence (MI) mindset and culture that includes expanded capabilities to conduct political, military, economic, social, information, infrastructure, physical environment, and time collection, analysis, and reporting. This includes the realization that understanding the dynamics of the local population and culture in stability operations can often be as important as maneuver against and targeting of threat cells and organizations. Most operations in the future will continue to center on people, requiring an intelligence force with a firm grasp of the operational variables and civil considerations.
- Develop more detailed and precise intelligence and knowledge against networks and individuals to achieve unparalleled operational success. This requires a flexible intelligence structure armed with the many necessary skill sets prepared to task organize as required, thus becoming more agile.
- Proactively, rather than reactively, integrate new technology–for example, communications, information processing, sensing, and hand held devices–and effectively tap into global data and information stores. This will assist Army intelligence in efficiently synchronizing the enterprise and managing the vast amounts of classified intelligence and open-source information (which is still growing exponentially). The endstate is to build an overarching federated and networked analytical enterprise.

The challenge we must meet is to develop agile, innovative, critically thinking, and culturally aware MI Soldiers, leaders, and civilians for this future OE. These professionals must possess a balance of interpersonal skills and technical competence necessary for an effective military team. Our future success relies upon methodical yet creative and adaptable MI Soldiers and leaders that are not risk-adverse and can find a way to meet the commander's requirements.

I am confident that the intelligence warfighting function and the MI Corps are up to these challenges and we will continue to make very significant contributions to our Army.

Always Out Front!

(Continued from page 2)

of these conflicts will always entail intelligence requirements. Every day, these intelligence requirements need to be fulfilled by strong-willed Soldiers who extract, analyze, and report information in order to help combat commanders make timely decisions, save lives, and neutralize enemy threats to their missions and their Soldiers.

One point I have always tried to make with many of the units I have visited is that Army Intelligence is not just fighting our wars and battles in foreign lands, but from our own soil as well. As you are reading this, a CI Soldier is working to keep our nation safe by protecting our intelligence information; an Imagery Analyst is receiving aerial imagery from different battle fronts and analyzing the images to provide intelligence products. Bottom line up front–an MI Soldiers does not need to have a combat patch to show that he or she is taking part in the fight.

I want to thank all of the Soldiers of our beloved MI Corps. Without your efforts, our Armed Forces would be blind in battle. Although the U.S. Military is in a struggle for the long-haul on several different fronts around the world, your professionalism and dedication as MI Soldiers has always and will always keep our ground commanders one more step ahead of our foes. I am proud to know that this Corps of "Quiet Professionals" will always prevail in times need. Before I close, I want to remind you all of the creed that defines the Intelligence professional:

I am a Soldier first
but an Intelligence Professional
second to none.

With pride in my heritage,
but focused on the future.
Performing the first task of an Army

To find, know, and never lose the enemy.

With a sense of urgency and of tenacity,
Professional and physical fitness,

And above all:
Integrity–for in truth lies victory.

Always at silent war while ready for a shooting war; the silent warrior of the Army team.

Soldiers of the MI Corps, thank you for your excellent service to the Army and the United States of America.

Always Out Front!

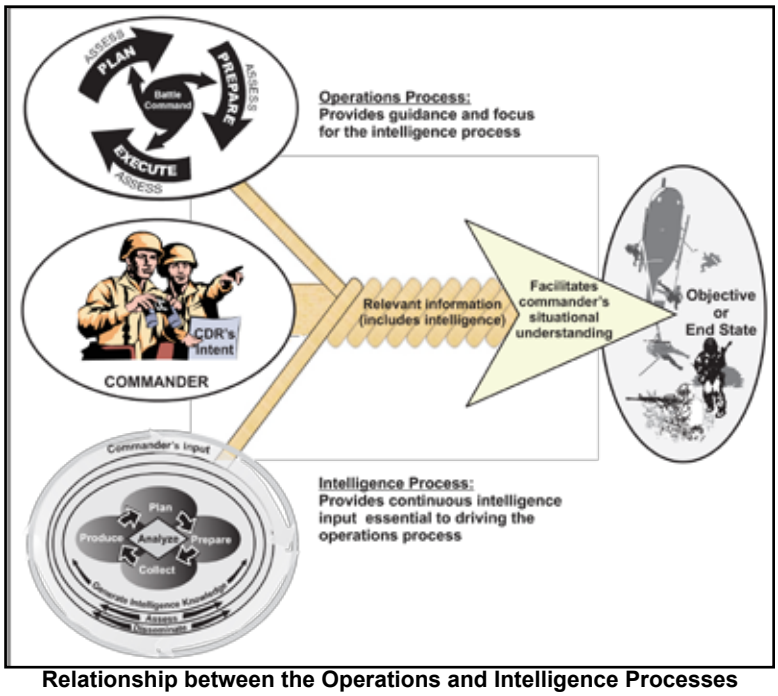
Army Strong!

(Continued from page 3)

Focus on FM 2-0

by Major Michael A. Brake and Sterilla A. Smith

FM 2-0 Intelligence (March 2010), the Army's keystone manual for Military Intelligence (MI), introduces several major changes to intelligence doctrine. Recent lessons learned from various operational environments (OE), extensive transformational changes in MI structure, and major revisions in Joint and other Army doctrine dictated revisions to this FM.



Relationship between the Operations and Intelligence Processes

The Army's operational concept is *full spectrum operations* within diverse OEs requiring continuous, simultaneous combinations of offensive, defensive, and stability or civil support operations. Intelligence facilitates understanding of portions of the operational and mission variables (i.e., enemy, terrain and weather, and civil considerations) to support the commander in decisionmaking process to achieve success on the battlefield. The most important role of intelligence is to drive operations by supporting the commander's decisionmaking.

New Concepts and Emerging Capabilities within FM 2-0

The ***Intelligence Warfighting Function***, replacing the MI Battlefield Operating System concept, is one of six warfighting functions (movement and maneuver, intelligence, fires, sustainment, command and control and protection.) It is the related tasks and systems that facilitate understanding of the OE, enemy, terrain, and civil considerations. The effectiveness of the intelligence warfighting function is measured against these criteria: accuracy, timeliness, usability, completeness, precision, and reliability. Effective intelligence must also be relevant, predictive, and tailored to support the commander's concept of the operation.

Within the FM, the intelligence tasks are updated to include: support to force generation; intelligence, surveillance, and reconnaissance (ISR); support to situational understanding, and support to targeting and information superiority, all of which are driven by the needs of the commander.

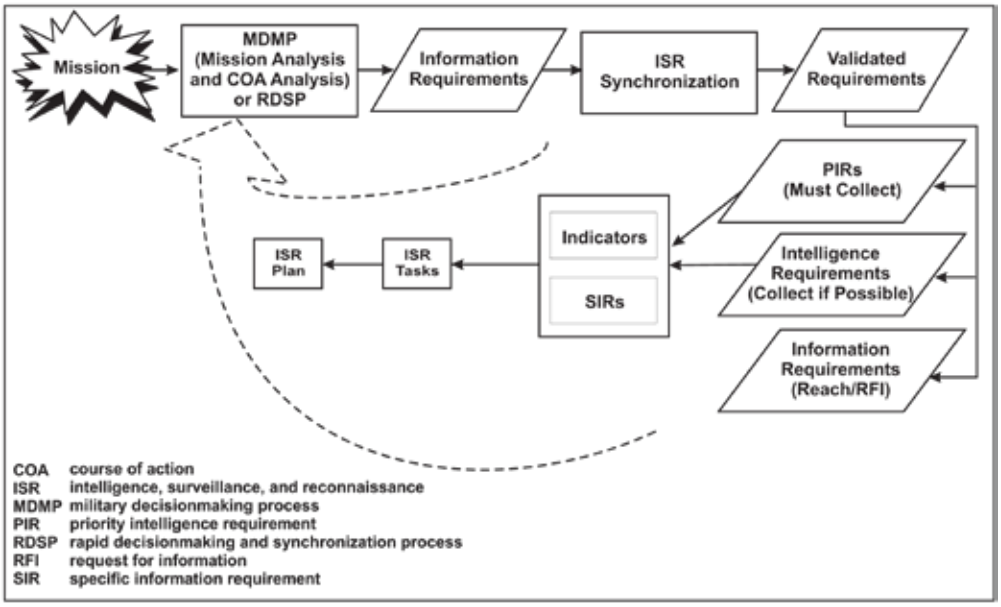
The intelligence warfighting function architecture, a flexible force of personnel, organizations, and equipment also provides specific intelligence and communication structures at each echelon from national through tactical levels.

The ***Intelligence Process*** was updated to combine the collection and processing steps and to place greater emphasis on the ***Commander's Input*** as commanders are responsible for driving the intelligence process. While it is not a part of the intelligence process itself, commander's input is the primary mechanism used to focus the intelligence warfighting function. Information gained through the "assess continuing activity" triggers the intelligence staff to request the commander's input.

The commander's input directly influences a unit's ISR effort. Each commander determines which intelligence products are developed as well as the products' formats. Commanders provide input at their discretion and at any point during the intelligence process. The staff must then carefully focus ISR plans

on answering the commander's ***requirements*** and enable the quick retasking of units and assets as the situation changes.

For intelligence purposes, there are three types of requirements that result from ISR synchronization–PIRs, intelligence requirements, and information requirements. Each requirement is broken down into discrete pieces to answer that requirement. These pieces are referred to as indicators and specific information requirements (SIRs), which facilitate the answering of the requirements. The indicators and SIRs are used by ISR planners to develop the ISR plan. The illustration (right) shows the process of developing requirements and integrating them into the ISR process.

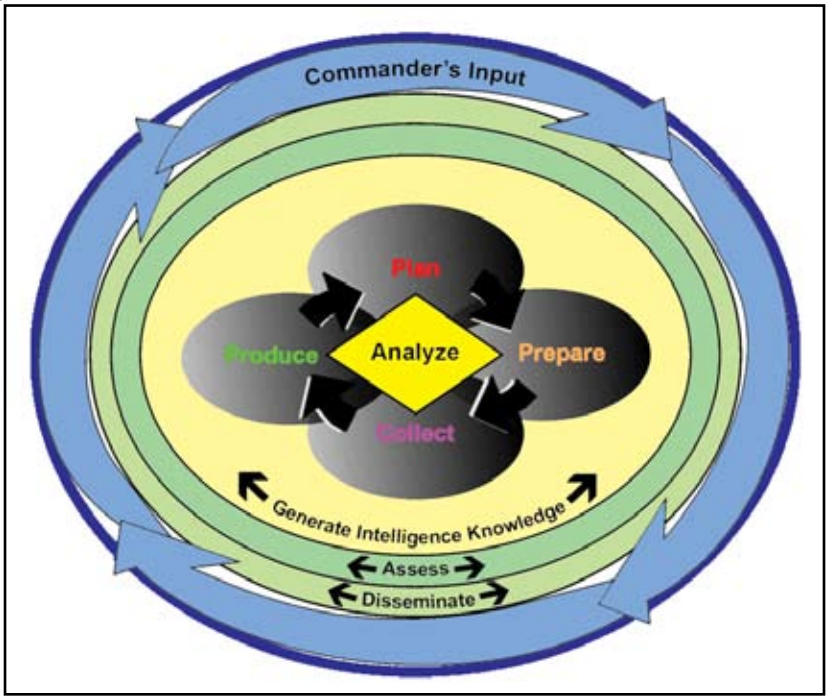


Requirements development and integration into the ISR process

FM 2-0 now defines an ***intelligence requirement as a type of information requirement developed by subordinate commanders and the staff (including subordinate staffs) that requires dedicated ISR collection for the elements of threat, terrain and weather, and civil considerations.*** Intelligence requirements must be answered to facilitate operations. They require ISR collection assets to be assigned for their collection, second in priority to PIRs.

Another change to the Intelligence Process was the addition of a fourth continuing activity occurring across the four steps of the intelligence process, ***Generate Intelligence Knowledge.*** This activity formalizes the intelligence description of the OE with appropriate emphasis on operational (PMESII-PT) and mission (METT-TC) considerations.

Generate intelligence knowledge is a continuous user defined activity driven by the commander. It begins before mission receipt and continues throughout the operation by providing the necessary relevant knowledge about the OE for the conduct of operations. This activity occurs whenever there is a need to analyze and understand the broad scope of the OE beyond the narrow focus of a specific mission.



The Intelligence Process

It serves as the foundation for performing intelligence preparation of the battlefield (IPB) and mission analysis. As soon as the intelligence officer and other staff sections begin to collect data on the OE, they organize that data into databases that meet the commander's visualization requirements. The primary products of generating intelligence knowledge are the initial data files and the initial intelligence survey.

Generate intelligence knowledge continues beyond the initial planning of the mission and provides additional context to the mission-specific planning that occurs after the initial IPB.

Generate intelligence knowledge includes five tasks. Each of the first four tasks is translated into a database or data files based on the commander's guidance to support his visualization:

- Develop the foundation to define threat characteristics.
- Obtain detailed terrain information and intelligence.
- Obtain detailed weather and weather effects information and intelligence.
- Obtain detailed civil considerations information and intelligence.
- Complete studies.

Generate intelligence knowledge is also the basis for developing a unit's initial ***Intelligence Survey***. Developing the intelligence survey is a process that assists intelligence officers in identifying ISR asset collection capabilities and limitations within the projected area of operations (AO) for potential employment in support of force generation. Developing the intelligence survey is a five step process:

- Develop comprehensive information, collection capability, and analytical baselines for the projected AO.
- Determine key intelligence gaps.
- Determine key gaps in analytical and ISR collection capabilities.
- Develop an understanding of the information and intelligence that can be collected with unit intelligence assets and, when appropriate, ISR assets in the projected AO, as well as how and where it may best be collected.
- Determine a method of understanding when changes to the information, collection capability, or analytical baselines occur that are significant or of intelligence interest.

The intelligence survey is developed over time and continuously updated. It provides the unit intelligence officer with an initial assessment that forms the basis for recommending intelligence asset apportionment and the best use of the unit's intelligence assets within the projected AO. It takes into account technical and tactical considerations across all disciplines. For example, one portion of the projected AO may be unsuited for unit Signals Intelligence (SIGINT) asset collection due to terrain or lack of threat transmitters. The same area may be well suited for human intelligence (HUMINT) collection teams (HCTs). The intelligence officer may recommend to the commander that unit SIGINT collection assets not be deployed to that area and that additional HCTs would be a valuable source of intelligence collection in that same area.

This assessment includes determining what nonstandard ISR assets, including quick reaction capabilities and off-the-shelf capabilities and systems, are available. Additionally, when reviewing concept plans and operation plans, intelligence officers use the intelligence survey to update the plan based on new technologies, capabilities, or sources of information and intelligence.

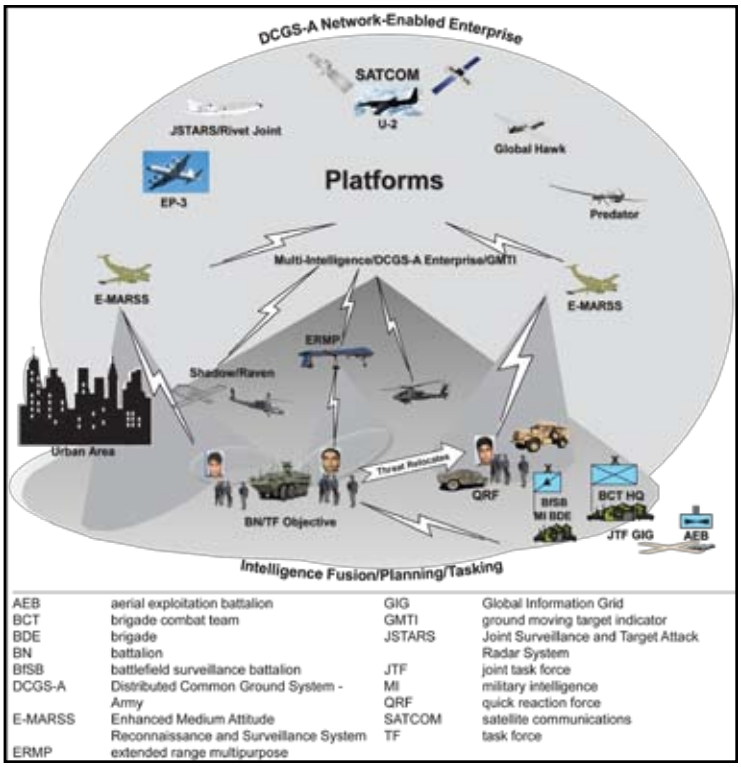
The survey also assists in determining what communication capabilities will be required for projected intelligence operations and addresses any apparent gaps in intelligence standing operating procedures. Additionally, it is the basis for determining what additional or specialized intelligence assets the unit may require.

Within the framework of the intelligence warfighting function, the intelligence tasks and the intelligence process, intelligence personnel focus further on conducting intelligence from an ***Army Intelligence Enterprise*** perspective. An enterprise is a cohesive organization whose structure, governance systems, and culture support a common purpose. This approach educates and empowers leaders to take a holistic view of organizational objectives and processes. It encourages leaders to act cohesively, for the good of the whole, to achieve required output with greater efficiency.

The Army intelligence enterprise is the sum total of the networked and federated systems, and efforts of MI personnel (including collectors and analysts), sensors, organizations, information, and processes that allow the focus necessary to use the power of the entire intelligence community. Its purpose is to provide technical support and guidance as well as an information and intelligence architecture that efficiently and effectively synchronizes ISR operations and intelligence analysis and production to produce intelligence to

support the commander's situational understanding. The illustration (right) exemplifies the tactical portion of the Army intelligence enterprise.

As an emerging capability, the ***Distributed Common Ground Station-Army (DCGS-A)*** provides a net-centric, enterprised ISR, weather, geospatial engineering, and space operations capability to organizations of all types, at all echelons—from battalion to joint task force levels. DCGS-A will be the ISR component of the modular and future force Battle Command System and the Army's primary system for ISR tasking, posting, processing, and conducting analysis concerning the threat, terrain and weather, and civil considerations at all echelons.



AEB	aerial exploitation battalion	GIG	Global Information Grid
BCT	brigade combat team	GMTI	ground moving target indicator
BDE	brigade	JSTARS	Joint Surveillance and Target Attack Radar System
BN	battalion		
BfSB	battlefield surveillance battalion	JTF	joint task force
DCGS-A	Distributed Common Ground System - Army	MI	military intelligence
		QRF	quick reaction force
E-MARSS	Enhanced Medium Attitude Reconnaissance and Surveillance System	SATCOM	satellite communications
		TF	task force
ERMP	extended range multipurpose		

Example of the tactical portion of the Army intelligence enterprise

DCGS-A core functions are:

- Receipt and processing of selected ISR sensor data.
- Control of selected Army sensor systems.
- Facilitation of ISR synchronization.
- Facilitation of ISR integration.
- Fusion of sensor information.
- Direction and distribution of relevant threat information and intelligence.
- Facilitation of the distribution of friendly and environmental (weather and terrain) information.

Other New Concepts and Emerging Capabilities

Biometrics Enabled Intelligence is the intelligence information associated with biometrics data that matches a specific person or unknown identity to a place, activity, device, component, or weapon that supports terrorist or insurgent networks and related pattern analysis; facilitates high-value individual targeting; reveals movement patterns, and confirms identities (DODD 8521).

Commanders require the ability to link identity information to a given individual. Biometric systems are employed to deny threat forces freedom of movement within the populace and to positively identify known threats. These systems collect biometric data and combine them with contextual data to produce an electronic dossier on the individual.

The ability to positively identify and place an individual within a relevant context adds a level of certainty that significantly enhances the overall effectiveness of the mission. Personal identification enabled by biometric technology can help identify and locate specific individuals in support of targeting. This capability is necessary for force protection and security missions as well as when an operational capability is required to achieve an advantage in all operational themes and across the spectrum of conflict.

Human Terrain Analysis Teams assist with socio-cultural research and analysis. As part of building their situational understanding, commanders consider how culture (both their own and others within the AO) affects operations. Culture is examined as part of the mission variable-civil considerations. Understanding the culture of a particular society or group within a society significantly improves the force's ability to accomplish the mission.

Document and Media Exploitation (DOMEX) is the systematic extraction of information from all media in response to commander's collection requirements. When conducted properly, DOMEX operations are intended to:

- Maximize the value of intelligence gained from captured enemy documents.
- Provide the commander with timely and relevant intelligence to effectively enhance awareness of the enemy's capabilities, operational structures, and intent.

- ✦ Assist in criminal prosecution or legal processes by maintaining chain of custody procedures and preserving the evidentiary value of captured materials.

For DOMEX products to be a force multiplier, the rapid exploitation of captured materials must occur at the lowest echelon possible. DOMEX assets pushed down to the tactical level provide timely and accurate intelligence support to warfighters. This practice not only enables rapid exploitation and evacuation of captured materials, but also hastens the feedback commanders receive from the higher echelon analysis.

Red Teaming provides commanders with an enhanced capability to explore alternatives during planning, preparation, execution, and assessment. Whenever possible, commanders employ red teams to examine plans from a threat's perspective. A red team is a special staff section whose members primarily participate in planning future operations and plans cells unless integrated into another cell. Red team members anticipate cultural perception of partners, enemies, adversaries, and others. They conduct independent critical reviews and analyses.

Red teaming provides commanders alternative perspectives by challenging planning assumptions, assisting in defining the problem and end state, identifying friendly and enemy vulnerabilities, and identifying assessment measures. These alternative perspectives help commanders account for the threat and environment in plans, concepts, organizations, and capabilities. These perspectives also address the standpoints of multinational partners, enemies, adversaries, and others in the AO.

Actionable intelligence is an example of bringing the characteristics of effective intelligence together with the effective integration of intelligence into ongoing operations to support the commander. Army personnel have used the concept of actionable intelligence to reflect the joint concept of critical intelligence. In current operations, the concept of actionable intelligence is used by Army personnel to describe information that answers operational requirements (See JP 2-0). Army personnel also use it to describe specific commander's guidance in the attack guidance matrix to a sufficient degree and with sufficient reliability to support the commander's targeting decisions.

Ideally, the staff thoroughly integrates intelligence into the operations process to ensure the collection and reporting of timely, relevant, accurate, predictive, and tailored information and intelligence. This integration is accomplished by using the characteristics of effective intelligence as well as conducting a successful ISR plan through detailed ISR synchronization and integration, so commanders can fight the threat based on knowledge rather than assumptions.

Critical thinking is disciplined reasoning which allows individuals to formulate ideas about what to believe or do. It involves determining the meaning and significance of what is observed or expressed. It also involves determining whether adequate justification exists to accept conclusions as true, based on a given inference or argument.

Critical thinking is essential to understanding situations, identifying problems, finding causes, arriving at justifiable conclusions, and formulating sound courses of action. The intelligence staff must be able to tell the commander clearly and accurately "what they know and why they know it; what they think and why they think it."

Other Additions and Updates

The number of intelligence disciplines addressed in FM 2-0 has increased from seven to nine by adding Geospatial Intelligence and Open Source Inelligence.

An appendix has been added to discuss the general content of the Intelligence Running Estimate, the Intelligence Estimate, and the Intelligence Summary.

The language support appendix has been updated adding to include a discussion of language technology.

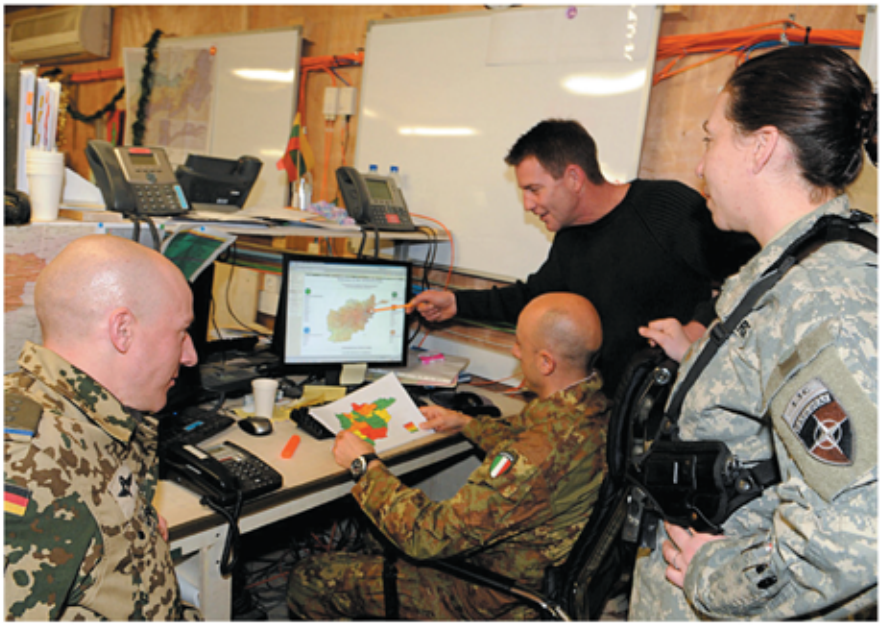
Command's Information Dominance Center Fuels Comprehensive Operations

New way to share information aims at streamlining processes and improving collaboration efforts.

By Col. George Franz, USA; Lt. Col. David Pendall, USA; and Lt. Col. Jeffery Steffen, USA

The International Security Assistance Force Joint Command in Kabul, Afghanistan, is implementing an information-sharing architecture that will create and enable a comprehensive common operating picture, derived from multiple systems, networks and classifications. It is designed to be the most decisive information and knowledge management effort ever executed within Afghanistan. This level of battlespace management and synchronization never has been attempted on this scale within NATO or the coalition force. The integrative effort could have significant effects on current and future civil-military operations across the Afghan theater.

Understanding the complex operational environment in Afghanistan means seeing the local conditions and activities and how they impact the populace. Before the Islamic Republic of Afghanistan, the International Security Assistance Force (ISAF) and nonmilitary partners can work together to gain the support of the Afghan people, they must understand how their efforts are viewed and what can turn the citizens away from supporting the government. This means understanding not only the nature of security threats posed by insurgents and terrorists and the like, but also the aspects of governance and development that have the greatest impact on the population's daily lives. U.S. and coalition forces need to adjust what they report and how that information is reported, but more importantly, they must change the organizational process used to turn data into the knowledge shared with all organizations—military, industry and government. Efforts in Afghanistan are supported by an international team, and the data sources, analytical approaches and knowledge management paradigms should reflect that same international diversity.



Capt. Oliver Loritz, GE A (l), a regional analyst; Maj. Andrew Carbonaro, ITAR (2nd from l), governance analyst; Ric Diaz (2nd from r), an analyst for Pakistan issues with the U.S. Defense Department; and Maj. Justine Krumm, USA, Information Dominance Center (IDC) production chief, International Security Assistance Force (ISAF), collaborate on a project. The IDC harnesses civil and military expertise and serves as a multinational information center.

The ISAF Joint Command (IJC) is reorganizing its staff and its approach to meet the commander's critical information requirements (CCIR) by creating an inclusive information center to assemble, analyze and disseminate operational information in a timely, accurate and

The ISAF Joint Command (IJC) in Kabul, Afghanistan, reached initial operational capability last October. Led by Lt. Gen. David Rodriguez, USA, the command is the operational-level headquarters for ISAF in Afghanistan. The five subordinate regional commands, Afghan Security Force partners and international organizations work closely with the IJC and are active participants in the information-exchange and -sharing environment harnessed by the IDC.

comprehensive way. The IJC's Information Dominance Center (IDC) was organized specifically to address the information challenge faced by all partners in the Afghanistan effort. The IDC represents a new approach for synthesizing data so that decision makers at all echelons understand the complex informational environment with a common view.

For the majority of the organizations operating in Afghanistan, the problem is not a shortage of data. This is particularly true after eight years of operations and interaction with military units, local and national leaders, regional and global media, fact-finding teams, government and nongovernment survey organizations, and other groups. The issue is both data overload and the glare of ambiguous, contradictory, inconsistent, latent and incomplete reporting that cause U.S. and coalition forces to divert their attention away from the underlying dynamics and relationships of the key organizations, individuals and actions that really matter in the Afghan operating environment.

Afghanistan is a nation of more than 25 million, with more than 20 ethnic groups, hundreds of tribes and the presence of foreign support on both sides of the political endeavor. The overall complexity surpasses any other conflict area in the world. Given the requirement to act in an environment that is by definition unpredictable and unforgiving, decisions must be made in the face of contradictory, inconsistent, incomplete and perishable information. Truth changes—and the lens used to view the landscape matters. Within this unstable information "ecosystem," the commander asks open-ended questions as part of a sustained inquiry and requires his organization to be capable of producing detailed, nuanced and comprehensive explanations and predictive assessments.

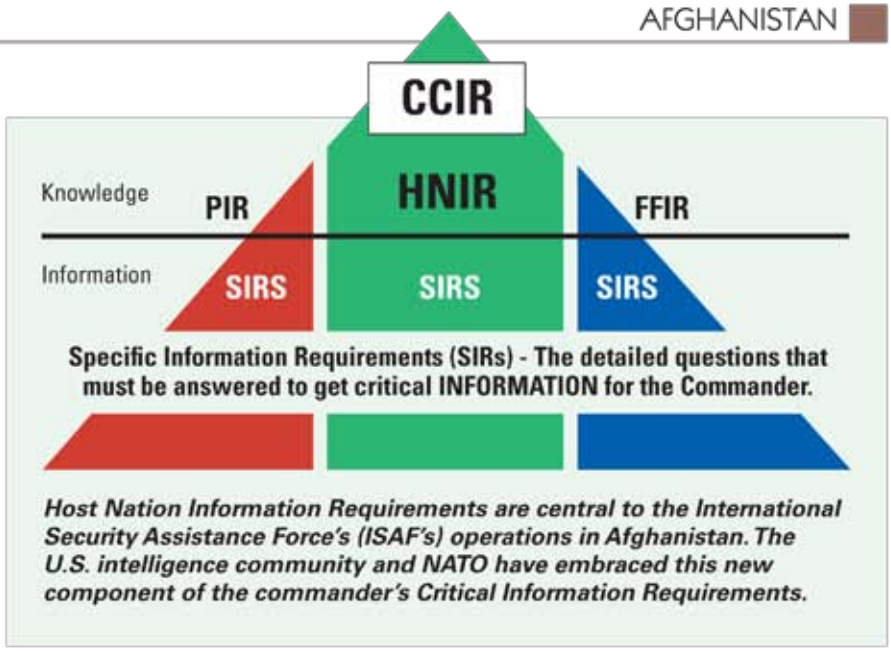
Expecting to gather all data, information and knowledge across all functional, technical and geographic areas in Afghanistan is unrealistic. A hierarchy must be in place in place to facilitate common understanding of the complex informational ecosystem. These information requirements must be more than just questions—they must be the right questions that drive effective population-based counterinsurgency operations.

Doctrinally, the CCIR prioritizes collection, analysis and dissemination. Unfortunately, there has been no deliberate or effective mechanism or process to identify, share, analyze and disseminate the crucial, population-centric information within the current bounds of the CCIR. As an initial step, the IJC has expanded the definition of critical information. The Host Nation Information Requirements (HNIR) are a dedicated set of the CCIR for the IJC and its subordinate units. They report on the critical factors affecting the people in Afghanistan and expand the scope of the CCIR.

All the elements and actions required to transform facts and isolated bits of information into action require both technology and human intellectual capital. Linear processes are formed from data, information, knowledge and understanding leading to action; feedback loops and collaborative partnerships that pool and share resources, especially expertise, extend well beyond the capacity and purview of the individual sections. Synthesis requires cross-functional teams of experts—senior leaders maintaining constant contact with the environment that affects the analytic organization—and integration of the strengths of diversity within the team.

Information must extend beyond organizational boundaries, and the organizational structure must adapt to reflect the diversity, depth and sensitivity of the information available in order to provide an effective understanding of the operational environment to all partners. Extending broader access to diverse databases is crucial in order to prevent myopic views of the environment, develop a thorough understanding and create comprehensive assessments.

Inherent to the communication architecture of the IDC is the ability to push classified information to the lowest level possible while ingesting from multiple unclassified data sourc-

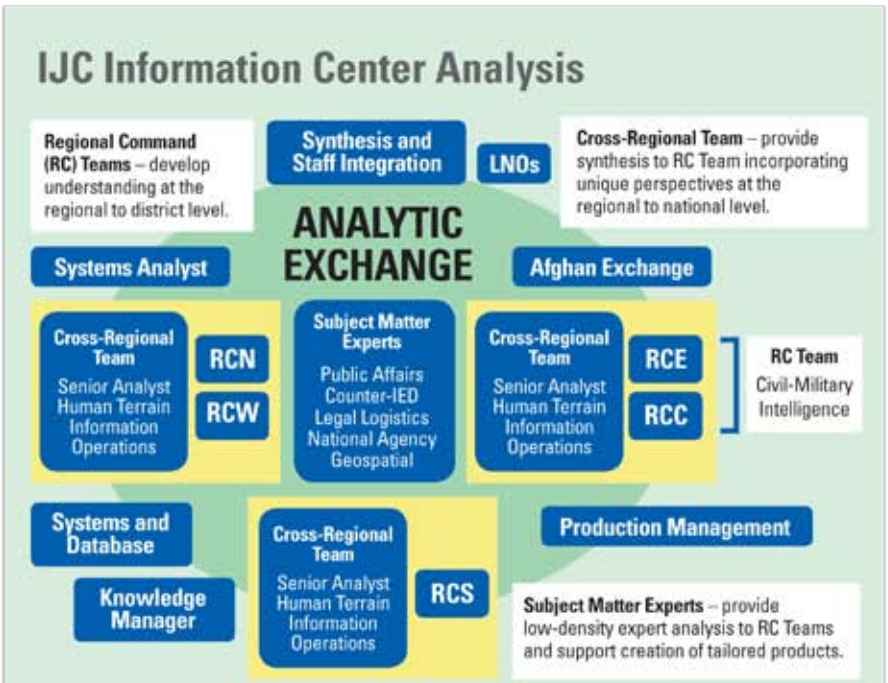


Host Nation Information Requirements are central to the International Security Assistance Force's (ISAF's) operations in Afghanistan. The U.S. intelligence community and NATO have embraced this new component of the commander's Critical Information Requirements.

es. Contributing to the collaborative effort also is a critical component of the IDC's architecture. Populating classified and, more importantly, unclassified databases and portals will enable significantly greater collaboration through interaction with the Islamic Republic of Afghanistan and government and nongovernment organizations that lack access to the classified mission systems.

The IJC leverages three tools to enable a common understanding. First, Web portals will ensure the greatest availability of finished products to all partners. The IJC's Microsoft SharePoint portal on the Afghan Mission Network, which was integrated with NATO's Document Handling System and the NATO Intelligence Toolbox, enables the storage, retrieval and dissemination of finished products representing the synthesis and analysis of all partners. For deliberate collaboration and information sharing with partners that only have access to unclassified networks, the IJC leverages two Internet sites with complementary structures and customers: the Civil-Military Overview and the Ronna-Afghan Web portal. The IJC continues coordinating with partner organizations in Afghanistan to ensure that appropriate content is shared among these sites, the Afghan Mission Network and other networks.

The second tool is an Afghanistan-focused wiki-like information repository. This so-called "Afghan wiki" provides an information-sharing environment for data, information and assessments that generally are stable in the mid- to long-term periods. This resource will be replicated onto other networks, including the unclassified network on the Ronna-Afghan Web portal. Sharing information with all partners is critical to synchronize planning and operations in this environment.



The ISAF Joint Command's Information Dominance Center is an organizational and procedural change aimed at addressing the complexity of the operational environment in Afghanistan. The center, which features an integrated information technology infrastructure, breaks new ground for NATO and coalition partners.

The third tool is a database that enables cross-staff, cross-function and cross-partner structured data sharing. In late 2009, members of ISAF's intelligence community fielded the Combined Information Data Network Exchange (CIDNE), which has continued to be adapted to satisfy multiple operational requirements. The companion to CIDNE on the unclassified network allows structured data to transfer between nearly all classified networks within the constraints of security policies. The unclassified version will be available through the Ronna-Afghan Web portal as the site matures through early 2010.

The IDC leverages these tools to facilitate collaboration across ISAF headquarters, all echelons of command, and government and nongovernment partners. Combined with a means to populate an unclassified portal with associated wiki pages and other collaborative Web sites, these tools will ensure the greatest dissemination of relevant, accurate and timely informa-

tion that remains current from regular updates provided by individuals and organizations with access to the most complete data.

Previous efforts to process and distribute data and information across the ISAF, Afghan and nonmilitary team have proved to be insufficient. Now, internal reorganization has increased the rigor, depth and breadth of information processing and analysis for all consumers teaming in this international effort. No single staff element monopolizes the functional, technical and professional expertise required to synthesize the diversity of information into a relevant product for decision-making processes.

In a counter-insurgency environment, the HNIR represent the most important aspects of that environment that must be integrated and understood to ensure cohesion of effort throughout the complex combination of actors in Afghanistan. IDC experts assembled from across the staff, including both civilian and military, NATO and Afghan, have the functional expertise to provide complementary views of the environment and the ability to ensure broad dissemination of relevant assessments.

The IDC also serves another key function—that of widening the aperture for data and information input, analysis and dissemination. The effect is that all of the IJC's partners will increase the "surface contacts" at the local level throughout the country. The IJC's reporting process supports cross-functional processing of information and ensures the data validation, further refining analytic insights across the functional or technical fields. Ultimately, the key to enabling the leaders at the local level in Afghanistan's districts and provinces is to accurately represent their information requirements as conduct-partnered operations within local communities. These operations include personnel from ISAF and the Afghan army and police forces collaborating together.

The IDC's knowledge management processes are key to all partners having a common understanding. Creating a data repository and a reference library that supports analysis will provide the IJC commander and staff with a comprehensive view of the operational environment.

The concept and organization of the IDC was based on a need to address the information challenge in Afghanistan. Providing equal access to data and knowledge across all partners and networks is a fundamental change in approach for collection, analysis and dissemination of mission-related information in ISAF. By integrating data, information and knowledge into one information organization with an integrated information-system architecture, the IJC's Information Dominance Center enables decision makers at all echelons, in government and nongovernment organizations and throughout the Islamic Republic of Afghanistan. The IDC continues to use innovation, organization and technology to enable common understanding in the face of a complex informational environment.

Col. George Franz, USA, is chief, Combined Joint Analysis and Control Element, International Security Assistance Force (ISAF) Joint Command (IJC), Kabul, Afghanistan.

Lt. Col. David Pendall, USA, is the chief CJ2 planner for the IJC Future Operations Planning Team in Kabul, Afghanistan.

Lt. Col. Jeffery Steffen, USA, is a senior analyst in the IJC. He serves as the host nation information requirements (HNIR) coordinator for the IJC.

• • •— •—

WEB RESOURCES

Civil-Military Overview: ***www.cimicweb.org/Pages/CMOwelcome.aspx***

International Security Assistance Force: ***www.isaf.nato.int***

Ronna-Afghan Web Portal: ***https://ronna-afghan.harmonieweb.org/Pages/Default.aspx***

Host Nation Information Requirements: Achieving Unity of Understanding in COIN

Reprinted from Small Wars Journal, posted 15 January 2010 at http://smallwarsjournal.com/blog/journal/docs-temp/348-franz.pdf.

by Colonel George J. Franz, Lieutenant Colonel David W. Pendall, and Lieutenant Colonel Jeffery D. Steffen

Introduction

Understanding the complex operational environment (OE) in Afghanistan means seeing the local conditions and activities and how they affect people's lives. If the Government of the Islamic Republic of Afghanistan (GIRoA) and NATO's International Security Assistance Force-Afghanistan (ISAF) are truly focused on gaining the support of the people, we must better understand the lens through which the people are watching our efforts play out and we must know what may drive them away from supporting the government. This means understanding not only the nature of the threats to security posed by negative influences, insurgents, and terrorists but also the aspects of Governance and Development that most impact their daily lives. Host Nation Information Requirements (HNIR) is a category of reporting on these critical factors affecting the people in Afghanistan.

More important than the structure of government, people are most concerned about the extension of governmental services and the ability for their national and local officials to deliver basic necessities and support for a functioning community–to include security. But the OE in Afghanistan is much more complex, nuanced and dynamic than just answering the question of satisfactory governance–rendering a basic collection of facts, polling data, anecdotal references and statistics insufficient for true understanding within the partnered commands.

The ISAF Joint Command (IJC) instituted a bottom up, inclusive information system to answer key information gaps and assist ISAF and Afghan Partners with clear commander critical information requirements (CCIR). More than just asking the right questions, the ISAF and Afghan operating forces along with civilian partners in the field, must understand what the answers are that will drive resources and prioritization, providing better insight into the real issues and perceptions at local levels. The IJC has created a reporting system and fusion process to bring this information to the command in a timely, accurate and comprehensive way.

The Need for HNIR, Why Now?

Things have gotten worse for the Afghan people since 2005. Despite significant financial and security contributions of the international community and from the Afghan people, in terms of dollars, time and lives, many areas of Afghanistan are now less secure and less governed. The reasons are likely two-fold: a strategy that embraced counter-insurgency (COIN) concepts but failed to apply it at the operational and local levels, and a near-absence of synchronicity coupled with disunity of effort among ISAF, the International Community and the Government of Afghanistan, to include the Afghan security ministries. These two root problems have been identified by informed and not-so informed observers. The inability to adjust course has been stymied by inertia to change, organizational culture, complacency, in some cases apathy and greed; and perhaps most importantly, an inability to develop, see, share, and understand information falling outside traditional information spheres.

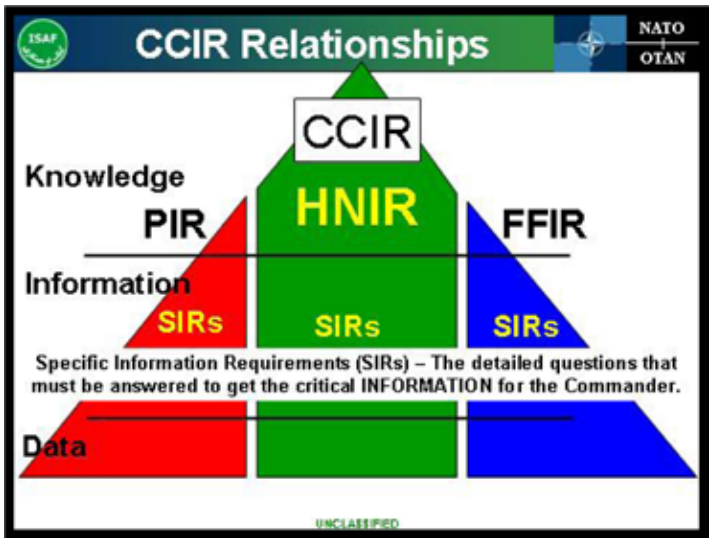
The current doctrinal approach to CCIR in a COIN environment is insufficient to address the key el-

ements that affect the perceptions and support of the population. This information gap hovers directly over the Center of Gravity in a COIN environment–the people's support to the Host Nation government. With this informational gap, commanders in the past have been served disparate bits of information from across the staff, functional experts, battlefield circulation, and special advisors. There was no deliberate mechanism or process to effectively identify, share, analyze, and disseminate the crucially important, population-centric information within the current bounds of CCIR. There must be an expansion or broadening of the definition of *Critical Information*.

The U.S. Army's manual for COIN and NATO guidelines emphasize the importance of the support of the local population as both the national government and insurgency vie for power, authority, influence, and active support. With the populace actively supporting the national and local government, the support for the insurgency withers. Careful and deliberate operations further relegate insurgents to the extreme margins of society with no tangible influence over the population. So, if this is the crux of the issue–societal and political competition involving the use of coercive force, then we require a better means to design, collect and assess the critical components of the OE that produce a supportive population, and feed that assessment into the COIN operational decisionmaking processes.

NATO CCIR currently contains three primary components; one is threat-focused, one details the commander's own forces, and the third is oriented on operational security priorities. Closing the information gap between threat forces, commonly understood as *priority intelligence requirements* (PIR) and *friendly force information requirements* (FFIR) and *essential elements of friendly information* (EEFI), is the key to operating effectively in a counterinsurgency. Within this gap lie many answers and the insight to address operational and tactical decisions about where to adjust operations, apply additional resources, engage with key civil leaders, and improve support to essential services.

This gap exists because of the many organizational approaches and often stove piped staff processes used to gather information regarding the population and the civil environment. Said another way–the gap is not there because the information



is not available, the gap is there because the information is not viewed as operationally critical information and is not systematically shared, processed, and analyzed as part of the CCIR.

Provincial reconstruction teams (PRTs) diligently report information about projects, key district leaders, status of infrastructure and "atmospherics." Within the same operational space, the U.S. Army Corps of Engineers, nongovernmental organizations (NGOs), combat forces, host nation partners, and the media all report similar or widely dissimilar information within an alphabet soup of reporting channels and independent information sharing processes. And in the end, the commander and senior staff are left to sort out the answers to some of the most important questions in the COIN environment. Expanding the CCIR to include information gathered on the influencers of the population from within the area of operations and establishing an effective data sharing and reporting system would close this information gap.

The key to enabling the military commanders at the local level in the districts and provinces of Afghanistan is accurately representing their requirements as they *shape*, *clear*, *hold*, and *build* within their battlespace. These decisions of military, but more importantly, civilian capacity-building resource allocation are discussed, prioritized, integrated, and funded in the national- and sub-national working groups. HNIR provides that holistic view of the local operating environment and will empower key leaders with the necessary assessments to negotiate within authoritative working groups that make district-

level decisions. Indeed, the IJC must advocate the local commander's district-level awareness across the spectrum of operations into the decisionmaking processes of military, governmental, nongovernmental, and civilian organizations. Only then will the Regional Commands and subordinate elements benefit from the unity of effort across all levels of command and government.

What are HNIRs?

HNIRs represent a commander-driven cultural change within the ISAF Joint Command. They are more than just questions—they are tailored and are the "right questions" to drive effective population based COIN. HNIR enable the commander to make informed decisions and allow him to more effectively conduct the full spectrum of military and civilian activities that will achieve popular support for government. Information at local levels is systematically collected by organizations across the command, fused, and analyzed to produce knowledge and understanding.

HNIR is information the commander needs about *friendly nation* institutions or organizations in order to partner effectively, develop plans, make decisions, and integrate with civilian activities. Depending on the circumstances, information may include the status of provincial, district or local governance, economic development, infrastructure, or security forces. Other examples include:

- Popular support–sympathizers and active supporters.
- Population conditions, beliefs, and structures.
- Infrastructure, services, and economy.
- Governance development, capacity, and tactics–central government, engagement/empowerment of traditional governmental structures, overall governance, power brokers.
- Host Nation security force development, capacity, and impacts (tactical and institutional.)

The scope of HNIR is designed to be comprehensive. These information requirements are far broader than "intelligence," rely on functional experts and integrated processing, and every organization is a potential contributor and "sensor" in the field. The challenge is to harness the staff expertise and information flow to inform the commander and staff so that the context, subtleties, and biases inherently important in COIN are surfaced and understood.

The intelligence function is an important component in answering the HNIR but the preponderance of information will come from unclassified contributors. The information is available in a variety of reporting processes or can be readily obtained by overt means, and often from non-military sources. Whereas intelligence is usually related to data and specific information an enemy is deliberately trying to conceal or keep secret, the information on the friendly nation characteristics and local circumstances is visible and collectable in the normal course of operations and trust-based interaction among partners in a COIN environment. Certainly, there is a place for intelligence collection to provide certain details and discern the existence of deception or bias within the HNIR, but the vast majority of the information is openly exchanged.

Specific examples of HNIR may include:

- What influences are inhibiting the extension of governance in district X? (Governance)
- Who are the key influencers and community leaders that will determine the right projects for economic development? (Development)
- What partnership activities should we take to ensure sustainable freedom of movement for the population? (Security)
- What resources are required to facilitate the access to justice for the district Y? (Justice)
- What grievances are present and are inhibiting trust between the local tribal elders and the district administrators? (Governance)
- Where and when can we enhance the growth of government capacity to serve the population? (Governance)

Understanding with Context

We approached the development of HNIR with a key related question at the forefront of the process design: How can we contextualize the HNIR questions to help our experts identify collectable data and information that will lead to an informed assessment supporting the commander's decisions?

***Examples*:** The number of sitting judges (data point) doesn't matter to the *Rule of Law* if they see no cases nor make judgments (harder to measure). What would indicate change in the Rule of Law? How about tribally accepted *Informal Justice*? In fact, thinking through the judicial question leads to another—how to assess satisfaction with the ju-

dicial system, formal or otherwise. For instance, while a district may have a full complement of three judges and supporting administrative staff, the population may not assess the judicial system as effectively rendering justice if the judges don't see many cases, are viewed as corrupt, or do not make timely rulings.

If a project is being considered for a local community, has that project been approved by local elders and village leadership or is it being pushed from a higher level official without consultation in the community for actual need or support? Are the funds flowing through the province to the district and then to the community contractor? Is the contracted price fair or is the price a reflection of corruption and graft?

While these examples can seem like simple "metrics," and it is true they may serve that purpose, they also provide answers to the fundamental and contextually important questions required to assess the OE in terms of seeing the terrain and understanding the perspectives of the population.

The commander must be served with answers to real and complex issues without losing context as data is brought forward and presented as "truth." If the commander is served only with threat information (PIR) and friendly force information (FFIR), decisions can (and often do) skew toward security operations and leave civil considerations and capacity questions unresolved. If we go too fast in the security line of operations we may outpace efforts in governance and development, leading to unmet expectations and worse yet, failure, in the eyes of the population. We then have a net loss in popular support and trust, creating new conditions for the insurgents to exploit.

With HNIR in place, we can better assess and understand the whole environment and Host Nation capability, thus synchronizing all efforts through HNIR information sharing and ground up, local refinement. The GIRoA governance and security partners, nongovernmental partners, PRTs, and ISAF forces that have the boots and "shoes" on the ground will gather and share this information. ISAF Joint Command forces and partners will support and enable a common situational awareness through coordinated and synchronized reporting and sharing of information with Host Nation, international organizations, national embassy staffs and United Nation's (UN) representatives.

Why is this different? It is about maneuvering information to the commander. It is about achieving more effective partnership through shared "unity of understanding."

Enabling HNIR

Enabling and synchronizing HNIR integration is a cross-organization, multi-functional, and unity of effort driven task. Full-time and thematic analysis will coalesce at a single location with tethers from the information integration center reaching back to each staff specialty and their experts. This center will rely upon central databases ingesting classified and unclassified information from multiple sources and agencies providing data and assessment at all levels of operations, in and outside the area of operations. This brings challenges of size and composition of the analysis cell and the access to the central databases for all organizations who traditionally have provided limited horizontal dissemination of data.

The commander, through HNIR, will drive the process which will provide continuous friendly nation analysis essential to effectively executing the operations process. To develop initial requirements and to answer the overarching questions that would best support the commander and decisionmaking process, command intent documents, doctrinal references, interagency studies, and ISAF headquarters sources were available, all addressing key aspects of COIN.

Developing an approach to organize, prioritize, and synchronize the development, sharing, analysis, and dissemination of the HNIR started with leveraging the Intelligence Process and following the six adapted intelligence, surveillance, and reconnaissance synchronization activities: Develop requirements, develop HNIR synchronization plan, support HNIR integration, disseminate, assess HNIR operations, and update HNIR operations.

The horizontal integration of HNIR analysis is the key to ensuring current understanding of the nuances and subtleties in the OE throughout the staff and the staff integration and synchronization events at the headquarters. Leveraging web based tools for full and open access to assessments and specific integrated staff products will be the basis of effective sharing. A complementary dissemination process will be deliberate dissemination to all organizations,

internal and external to the command, based on specific informational requirements.

Enabling the Command: Building the Process, the Team, and Making this Work

Assessing and updating HNIR operations will fall on a cross functional center and working group that reviews the quality, quantity, analysis, and production cycle to ensure the HNIR are answered appropriately for the commander.

Expertise and Partnership. It became clear that each staff element would be able to provide only a portion of the information required, leaving the challenge to assign and qualify staff advocacy for each HNIR. This responsibility would require the staff section to validate the HNIR including developing indicators and specific information requirements; ensure collection; ensure data is ingested into common databases for easy access and analysis, and provide subject matter experts to work in and with an analytical cell designed to integrate HNIR assessments across the headquarters.

Step 1*: *Identify Advocacy and Expertise:

- Within the IJC and ISAF staff functions.
- Within governmental and NGOs from both the international community and Afghanistan.
- Within IJC subordinate commands and the ANSF.
- Within professional specialties from both international community and Afghanistan.

***Endstate*:** A fully developed contact network along organizational and professional authorities and expertise to refine HNIR and assist with the development of reporting criteria.

Developing the "Right Questions." Further analysis of the HNIR was required to identify or refine indicators or information requirements across the

staff. The first step was to determine which staff element would take the lead for developing and refining indicators based on staff functions and expertise. Experts in the fields may have additional or different indicators that help answer the HNIR. Identifying indicators and developing s*pecific information requirements* (SIRs) became the task of the staff proponent. These indicators and information requirements are analytical tools and describe the information required (including the location, where, when, and how the information can be collected and disseminated), outline specific observables that support the HNIR, and establish what must be collected, in what format, and how it is integrated into the information environment. Developing requirements in this complex OE, integrating feedback from staff functions and experts across the military and civilian community paints a powerful mosaic across all levels of command and leadership.

Step 2: Develop and Refine HNIR with Expert and Partnered Input to Produce SIRs.

- ✦ Develop indicators and SIRs–key analytical tools.
- ✦ Describe the information required which may include both the location where and the time during which the information can be collected.
- ✦ Outline specific observables that support the HNIR.
- ✦ Establish what must be shared, in what format, and integration into the information architecture.

***Endstate*:** A comprehensive list of SIRs that drives sharing of data and information that will facilitate greater understanding of the OE and support unity of effort with all mission partners.

The parallel effort to develop a coordinated approach to assemble HNIR information started with identifying all the elements that currently or potentially could have access to the required information across the command and staff but more importantly, identifying what other agencies and organizations were potential sources of HNIR-supporting information. This led to a multi-dimensional knowledge management matrix that included Regional Commands, IJC staff elements, higher headquarters, Afghan security and governmental organizations, international governmental organizations (i.e., the UN), NGOs, and all the associated Boards, Bureaus, Centers, Cells, and Working Groups developed to support organizational and strategic awareness and operations. Each contributes information at all echelons of command and across all levels of government.

Synchronization and Collection of Information. The IJC developed a HNIR sharing strategy and tasking process that recognizes the need to "ask" rather than "task" for much of the information. This is why unity of effort and senior leadership engaging in peer leadership–beside, below, and behind partnered organizations is so important.

***Step 3: Link SIR to the Source of the Information*.**

- ✦ Identify the organization, element, team or individual who can provide the information, through direction or cooperation.
- ✦ Providing access to the information sharing and dissemination architecture to facilitate full integration of information to all mission partners.

***Endstate*:** A synchronized sharing environment that integrates all sources and expertise available to support unity of effort through shared understanding of the environment.

Synthesis and Dissemination. The last step is to ensure synthesis and dissemination of the data, information, and assessments. We must make this HNIR knowledge available across the information environment. This means sharing horizontally across the command, vertically within the command, and externally to other key governmental and nongovernmental actors in the OE will contribute directly to the unity of effort.

Step 4: Synthesize and Disseminate.

- ✦ Develop a multi-functional environment, enabled by an analytic center, to synthesize available HNIR information across all specialties.
- ✦ Identify and fill information gaps.
- ✦ Share extensively across the information environment to facilitate common understanding of critical "atmospherics."
- ✦ Integrate into staff planning and information sharing events within and without the command.

***Endstate*:** Understanding of the Afghanistan OE, with district-level awareness, across the spectrum of operations. Sharing the knowledge with all mis-

sion partners to enable effective decisionmaking processes for military, governmental, nongovernmental, and civilian organizations.

Conclusion

As with most processes executed during COIN operations, this HNIR effort will never be complete. The intended outcome of creating an HNIR information sharing system is to increase the understanding of a complex OE and to present a coherent, comprehensive common operational picture, not piecemealed and reported as independent packets of data or information.

Based on analysis of eight years of operations in Afghanistan, a new category of critical information has emerged as the central driving force for the IJC commander. The design of the HNIR process is to bring Host Nation and population centric information to the forefront of command decisionmaking. The development of an Afghanistan Information Environment will enable a more open and holistic information sharing process; recognized across the command and by our partners as critical to developing a shared understanding of the environment, and enabling all partners to cooperate more effectively to achieve positive results. The IJC and its mission partners, in support of the GIRoA, are involved in a complex argument between an elected government and negative influences for the support of the population. As we do those things that most benefit the people of this country, understanding the environment in which they live will be the most critical knowledge we will all need to be successful. HNIR is just one step, albeit an important one for the IJC Commander and staff, in the right direction.

Colonel George Franz is the Chief, IDC for the ISAF Joint Command, Kabul, Afghanistan.

Lieutenant Colonel David Pendall is the Chief CJ2 Planner for the ISAF Joint Command Future Operations Planning Team in Kabul, Afghanistan.

Lieutenant Colonel Jeffery Steffen is the Knowledge Manager within the IDC for the ISAF Joint Command, Kabul, Afghanistan.

UMI

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).

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 newer browser and Adobe Reader, Adobe Flash Player, Adobe Shockwave Player, Windows Media Player, and/or a recent version of MS Office.

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.us/DOD_Authorization.asp, 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.

DOMEX: The Birth of a New Intelligence Discipline

by Colonel Joseph M. Cox

The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Army, Department of Defense, or the U.S. Government.

Introduction

Prior to 9/11, Document and Media Exploitation (DOMEX) capabilities were neither well defined nor sufficiently developed or understood to adequately support combat operations. Despite lessons learned from previous conflicts, U.S. forces entered the War of Terror without mechanisms to properly collect, process, and disseminate intelligence derived from DOMEX. In the past 18 months, the volume of captured digital information from law enforcement, intelligence, and civil court cases has exploded. Recent investigations of Umar Farouk Abdulmutallab, the alleged terrorist who attempted to detonate plastic explosives on board a commercial airliner, and U.S. Army Major Nidal Malik Hasan, the man accused of killing Soldiers at Fort Hood, rely extensively on close examination of personal computer data by federal law enforcement agencies. These are just two cases amid an avalanche of harvested digital media that create a national security issue which merits a system that can reliably sift intelligence and quickly share it in order to protect lives and preserve security.

In response to a recent congressional inquiry, two respected leaders of the Intelligence Community (IC) commented that "there is no doubt that "*DOMEX provides critical intelligence unavailable through any other discipline.*"[1] Without question, our DOMEX capabilities have evolved into an increasingly specialized full-time mission that requires a professional force, advanced automation and communications support, analytical rigor, expert translators, and proper discipline to process valuable information into intelligence.

This article will examine the historical roots of DOMEX operations to present day activities, explain why DOMEX should be an intelligence discipline, review how the Army improved DOMEX capabilities, and what steps can be taken to enhance operations, and then offer recommendations on how the IC and the Department of Defense (DOD) can better organize, train, man, and equip itself to meet DOMEX challenges in the future.

Historical Context

The U.S. military and other branches of our government relied on what was originally titled Document Exploitation (DOCEX) for as long as we have practiced the art of intelligence. Discovering the enemy's intentions through examination and exploitation of captured documents was nothing new. In warfare, exploitation of adversary documents normally begins at the point of capture and progressively becomes more detailed and sophisticated as the document moves through a process of triage, translation, and promulgation.[2]

The Civil War provides many examples of troops capturing and attempting to exploit enemy documents. The assassination of President Lincoln caused a detailed review of captured Confederate documents once thought trivial or of little value for military operations, seeking proof that Southern leaders were linked to the assassination plot.[3] By 1920, the U.S. Army War Department intelligence regulation emphasized the value of DOCEX: "Experience has shown that the information derived from documents is second in value only to that secured by the actual examination of prisoners. Too much stress cannot be laid upon the importance of the rapid and systematic examination of every document captured."[4]

Unfortunately, DOCEX was never a high priority in terms of training and resources as the Army entered World War II. In Europe, the 1st Army had a total of five personnel assigned to their DOCEX team for combat operations from January 1944 to May

1945.[5] This team would disseminate intelligence reports after documents were reviewed and translated, usually 48 hours after capture. But with the capture of between 250 to 1,000 pounds of documents each day, the organization was of marginal assistance to tactical operations.

1st Army reached several conclusions about DOCEX intelligence: "documents arrived too late for operational exploitation" and "sufficient personnel were not trained to help Corps and Division levels".[6] Through the Korean War and into Vietnam, DOCEX remained relevant and necessary to gain intelligence on the enemy, but it was viewed as something temporary in nature. When we needed it, we built organizations to meet the demand, then forgot about lessons learned after conflicts ended.

Why was U.S. Army DOMEX Not Prepared for 9/11?

The first problem was that after Vietnam, U.S. Army DOCEX missions and functions were doctrinally pinned to interrogators: "the first intelligence specialists who could examine or exploit captured documents, in addition to interrogating prisoners of war, and will scan documents and extract information."[7] Accordingly, DOCEX procedures became firmly rooted within the interrogator Field Manual (FM) under the human intelligence (HUMINT) discipline.

The second problem was the direct result of placing DOCEX responsibilities on interrogators within HUMINT. There simply weren't enough collectors (CI and interrogators) to accomplish the DOCEX mission. As the Army reduced its force size in the early 70s under a transformation initiative called "Army of Excellence (AOE)," it became apparent that an interrogation force would not be a large one. Close study of the AOE with respect to interrogator strength revealed early concerns that there weren't enough interrogators in Army inventories to conduct HUMINT missions and equally support DOCEX missions.[8]

What Were the Consequences of Not Being Prepared?

One intelligence leader stated: "DOCEX didn't work; we did our own DOCEX when we could. Otherwise, it was sent to some CJTF-76 DOCEX section for processing that was virtually a black hole because I never received any feedback from anything we sent forward. We just didn't have the manpower at our level to conduct any type of extensive DOCEX."[9] From the outset of Operations Enduring Freedom/Iraqi Freedom (OEF/OIF), there was a shortage of trained HUMINT collectors and they were a precious resource. Major General Barbara Fast, the Multi-National Corps-Iraq C2, stated that "it became imperative once we were in Iraq to establish a strong HUMINT capability to understand the situation on the ground, but we lacked the number and some of the skills required to be as successful as we needed to be."[10] Predictably, the scant numbers of HUMINT collectors were in high demand just for their core mission sets: tactical questioning, debriefings, source operations, and interrogation of detainees. *DOCEX wasn't a priority*.

DOMEX Goes National

As the military struggled with DOMEX activities between 2001 and 2003, the first tangible effort to institutionalize DOMEX at the National and strategic level came with the creation of Defense Intelligence Agency's (DIA) National Media Exploitation Center (NMEC) in 2003.[11] The NMEC was created to serve as the lead government agency for the rapid processing, exploitation, dissemination and sharing of all acquired documents and media between strategic/national through tactical/local levels across the Intelligence, Counterintelligence (CI), military, and Law Enforcement (LE) communities to enhance the safety and security of the Nation.[12]

The swift expansion of DOMEX enterprise created many different efforts across the IC and DOD which required significant funding from congress. In 2005, the U.S. Senate Select Committee on Intelligence (SSCI) conducted an audit to review the practices of collecting, processing, translating, and reporting intelligence obtained from overtly captured and/or clandestinely acquired paper documents and electronic media.[13] The SSCI wanted to analyze and evaluate the intelligence value of DOMEX efforts and assess the budget implications for sustaining DOMEX over the long term. The SSCI audit findings concluded that:

- DOMEX had become an integral source of valuable intelligence information supporting both tactical operations in OEF/OIF and Iraq and strategic analysis in national intelligence agencies,[14] but there was a perception of slight duplication of effort and redundancy in terms of reporting intelligence.

- The IC allowed the DOMEX expertise to atrophy after each major conflict which caused a routine "reinvention of the wheel" phenomenon. This proved insufficient, and allowed for an information vacuum to exist during periods when policy makers and military planners most need DOMEX data.
- IC leadership needs to make tough decisions in the near term in order to improve the efficiency and effectiveness of DOMEX activities.[15]

The Office of the Director of National Intelligence (ODNI), as the head of the IC, oversees and directs the implementation of the National Intelligence Program and, by extension, provides oversight to DOMEX intelligence activities. The ODNI published Intelligence Community Directive (ICD) 302 in July 2007 assigning national DOMEX oversight to the Assistant Deputy Director of National Intelligence for Open Source Intelligence (ADDNI/OS), the NMEC, and the IC agencies.

One item within ICD 302 represents the center of gravity for the publication–NMEC became the DNI center for the national DOMEX enterprise and became chartered to:

- Support the development of the ODNI's DOMEX strategy, policy, and programmatic recommendations.
- Ensure prompt and responsive DOMEX support to meet the needs of intelligence, defense, homeland security, law enforcement, and other U.S. Government consumer, to include provision of timely and accurate collection, processing, exploitation, and dissemination of DOMEX.
- Implement policies and guidance on DOMEX including handling and dissemination polices.
- Develop training and tradecraft programs that expose all IC personnel to the benefits of DOMEX.

What the U.S. Army Fixed in DOMEX, What Can Be Improved, and What Can Other Services Learn?

For over 50 years, and until recently, U.S. Army intelligence doctrine preserved the DOMEX function within the HUMINT discipline and failed to maintain sufficient capability to conduct the mission. A post-mortem appraisal of the U.S. Army's OEF/OIF DOMEX experiences along the DOTMLPF framework offers lessons learned for other services:

Doctrine–DOCEX incorrectly resided under HUMINT with interrogators as lead.

Organizations–No Army units, to include intelligence units, were structured to conduct the function.

Training–Training was never formalized. Theaters established their own procedures and training. No effective blueprint existed for standardized DOCEX instruction.

Materiel–There was no family of systems to cover a DOCEX end-to-end approach.

Leadership–HUMINT staff directorates were overwhelmed.

Personnel–No professionalized force to accomplish the mission.

Facilities–Not applicable. DOMEX shortfalls were not caused by inadequate infrastructure.

The 2008 U.S. Army Training and Doctrine Command (TRADOC) and 2007-2009 Office of the Secretary of Defense overlapping studies assessed conventional and special operations forces and determined that a relatively small number of core and enabling capabilities was essential to sustaining an intelligence campaign against a networked adversary. The studies revealed one of the driving capabilities of the "find, fix, finish, exploit, access, and disseminate" cycle was DOMEX.[16]

Here are some thoughts and recommendations within the DOTMLPF framework which require immediate attention from the U.S. Army, and which other military services can digest, to capitalize on critical momentum generated by DOMEX over a relatively short period of time:

Doctrine. Figure 1 highlights that DOMEX spans all five steps of the Joint intelligence cycle and should be viewed as an intelligence discipline. JP 1-02 states that an intelligence discipline is "a well defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources."[17] Without a doubt, DOMEX meets the doctrinal specifications outlined in the joint publication.

It's also noteworthy to point out that ICD 302 states that "DOMEX activities support a wide range of intelligence activities, including all source analysis, Open Source Intelligence (OSINT), HUMINT, Signals Intelligence (SIGINT), Geospatial Intelligence

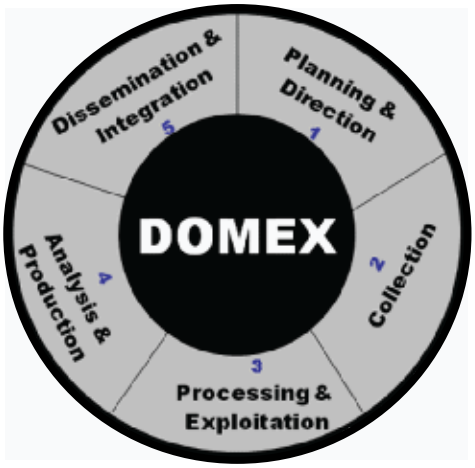
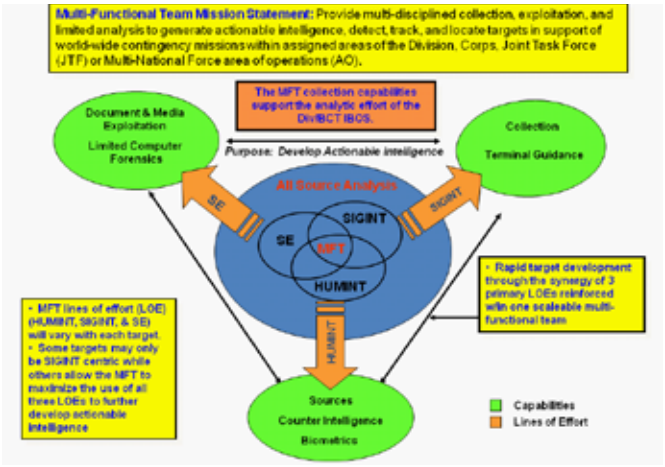


Figure 1.

(GEOINT), and Measurements and Signatures Intelligence (MASINT)–DOMEX reporting and analysis are considered intelligence products".[18] Aside from correct recognition of DOMEX as an intelligence discipline, the U.S. Army must also correct several doctrinal disconnects to set a better course for the future. Below are four key doctrinal items that Army intelligence leaders must address:

1. The most recent final draft of FM 2-0 Intelligence incorrectly states that DOMEX is "an emerging capability" but goes into profound detail spelling out the fundamentals of all other intelligence disciplines.[19] The FM misses a tremendous opportunity to devote a short chapter to DOMEX and bring together the central thoughts and themes thinly spread throughout the document into a single, concise framework that reinforces what DOMEX actually is–an intelligence discipline. *Recommendation*: Use FM 2-0 to state that DOMEX is an intelligence discipline.
2. TRADOC's Concept Capability Plan (CCP) for Intelligence, Surveillance, and Reconnaissance (ISR) for 2015-2024 fails to clearly articulate Army DOMEX capabilities required to succeed as we face future threats. The CCP barely mentions the term DOMEX and incorrectly states that DOMEX capabilities are required with HUMINT.[20] This doctrinal miscue makes it look as though TRADOC is out of step with current Army intelligence and ISR doctrine. *Recommendation*: TRADOC must develop a comprehensive DOMEX capabilities list in the CCP.
3. FM 2-22.3 HUMINT Collector Operations incorrectly maintains that "DOCEX" vice DOMEX is a HUMINT collection function and mixes DOMEX in the core HUMINT missions of tactical questioning, debriefing, source operations, and interrogation.[21] This must be changed immediately. We already know that Army DOMEX operations were not successful in the early stages of OEF/OIF because we expected interrogators to conduct the mission based on our doctrine. *Recommendation:* Publish an interim change to the FM and clarify DOMEX functions and responsibilities.
4. The U.S. Army Intelligence Center of Excellence (USAICoE) diligently worked the timely release of Training Circular (TC) 2-91.8 DOMEX Enabled Intelligence.[22] The publication codifies DOMEX doctrine and general tactics, techniques, and procedures from tactical to strategic environments. Unfortunately, based on restrictions on the number of FMs, the TRADOC Commander limits MI Doctrine to only four FMs. A DOMEX FM could better serve as a blueprint for other military services to follow as they develop their organization and training models. *Recommendation:* The U.S. Army should convert the TC into an FM and title the FM "DOMEX Operations" not DOMEX–Enabled Intelligence. Saying that there is DOMEX–enabled intelligence is akin to stating there is bullet-enabled infantry.

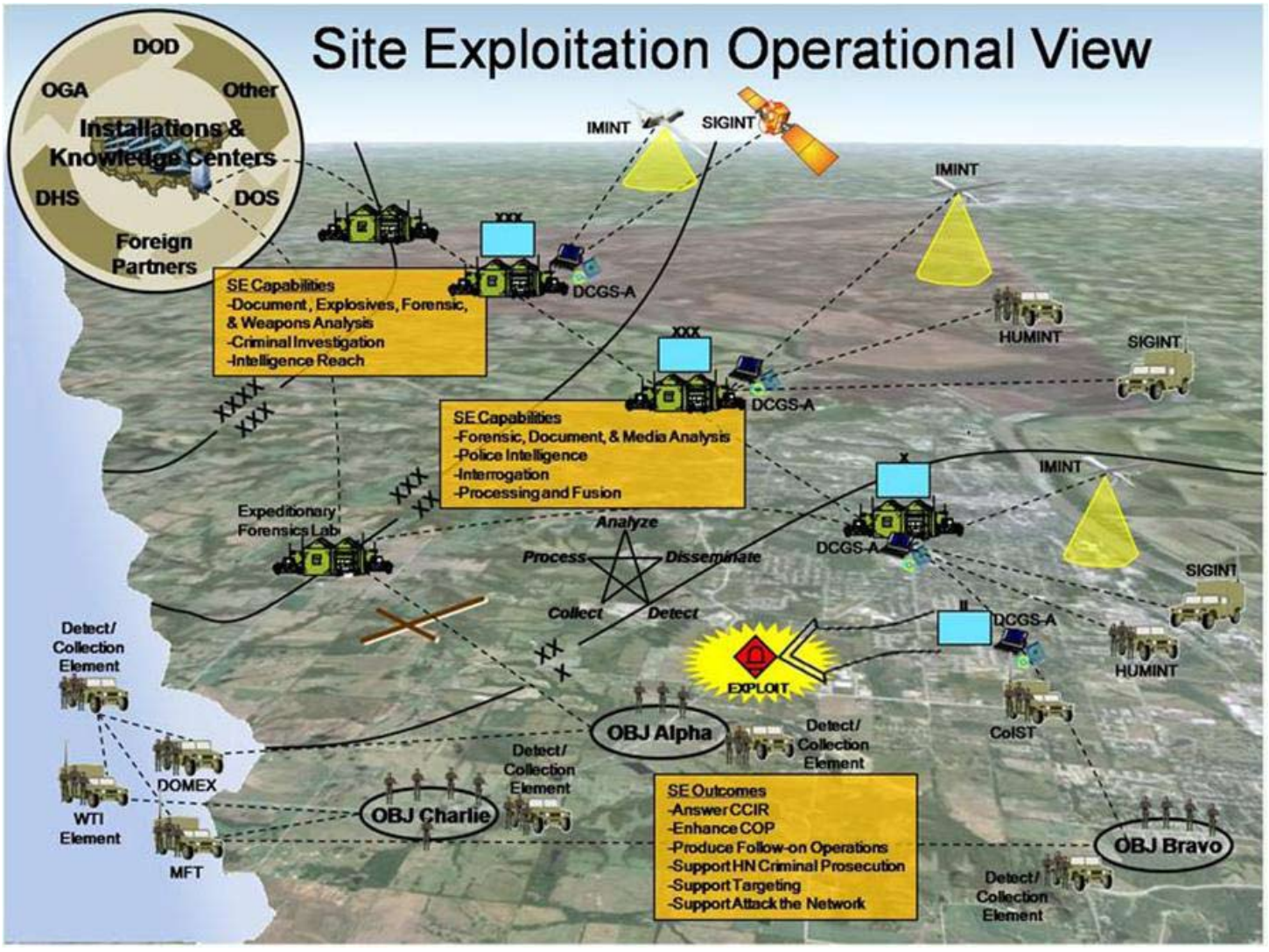
Organization. The need for tactical DOMEX capabilities *across the services* has never been greater; the services must address this organizational gap immediately. The Army learned that designating HUMINT Collection Teams (HCTs) for DOMEX missions was a poor strategy.[23] The Department of the Army (DA) G2 quickly recognized this and established Multi-Functional Teams (MFTs) within the Army's Battlefield Surveillance Brigade. The MFT task organization uses four intelligence military occupational specialty



(MOS) career fields: 35L CI Agent; 35M HUMINT Collector; 35N SIGINT Analyst; 35P Cryptologic Communications Interceptor/Locator, and 35S Signals Collector/Analyst.[24]

Each MFT fields sufficient personnel and equipment to exploit captured enemy materials (documents, media, and personal electronic devices), link biometrics data within the collection effort, and fuse tactical all source intelligence efforts for battalion and brigade S2s. *Recommendation*: Other military services should develop a similar approach as the MFT model within their intelligence organizations in order to provide a trained, tactically oriented, professionalized force to conduct DOMEX below National levels.

Training. The Army and other services must bring order and discipline to our DOMEX training approaches to professionalize a DOMEX force that is responsive to global demands, not just the urgent needs in Iraq and Afghanistan. DOMEX collection is not a task limited to intelligence Soldiers. Any Soldier can collect materials which require exploitation. Just as all Soldiers must be prepared to fight as infantry, they must also serve as information collectors. This is the premise for the "Every Soldier is a Sensor" model. Tactical collection skills are taught to Soldiers in all MOSs under the umbrella of Site Exploitation (SE) training. In SE, Soldiers enter and actively observe details at a site, use their cognitive skills to recognize information, materials, and personnel at the site that may help to answer the commanders' information requirements.[25] The graphic below portrays the relationship of the SE functional capabilities within levels of command and highlights the use of the Distributed Common Ground System-Army.



With respect to U.S. Army intelligence training, I recommend that a new MOS be designated that specifically covers DOMEX (exploitation of documents, media, and personal electronic devices) or at a minimum, an additional skill identifier (ASI). Currently, USAICoE provides baseline intelligence skills training for eight enlisted intelligence MOS career fields, the five MOSs mentioned in the MFT organization and MOSs 35F Intelligence Analyst and 35G/H Imagery/Common Ground Station Analyst.[26] Only MOSs 35M and 35T Military Intelligence Systems Maintainer/Integrator receive some DOMEX training. This is a start but it's not enough. *Recommendation*: At a minimum, I recommend that the MOSs 35F, 35M, 35L receive DOMEX training as well. Mobile training teams from the Defense Cyber Investigations Training Academy (DCITA) and National Ground Intelligence Center (NGIC) could also assist USAICoE to provide specialized computer forensic training to Soldiers.[27]

Materiel. Because DOMEX functions were historically linked to HUMINT as a function, a HUMINT reporting system was the only Program of Record (POR) to support DOMEX. The CI/HUMINT Automated Tool Set provided an HCT with a capability to collect, process and disseminate information obtained through document exploitation.[28] It wasn't nearly capable enough to satisfy a broad range of DOMEX equipment and software requirements to fully exploit information within computers, portable storage devices, video imagery, and a host of other items.

Today's the Army's DOMEX equipment suite offers significant advances over what was available to theater forces three years ago. The U.S. Army Intelligence and Security Command, DA G2, and the Army DOMEX program manager worked hard to field a standardized set of DOMEX equipment that met operational needs in support of OIF/OEF across the Army and ensure that the equipment was compatible with inter-agency standards. The Army must align these QRC efforts into PORs which seamlessly integrate across existing core, collection, processing, and dissemination intelligence systems.[29]

Leadership. From a tactical and operational staff perspective, G2/J2/C2 (HUMINT) staffs are in position to supervise DOMEX. The 2X staff directorates are fully engaged in coordinating and managing numerous HUMINT and CI collection activities across the areas of operation; they cannot be responsible for the management and integration of DOMEX assets on the battlefield. I believe that we should closely examine the pilot strategy, underway in U.S. Forces Afghanistan, which created a J2E–the "E" standing for exploitation. By separating DOMEX from the HUMINT organization and assigning an intelligence officer to manage the DOMEX intelligence cycle, we are better postured to provide quality control of the entire DOMEX system. We can also look at methods to fuse science and technology (biometrics, crime scene forensics, etc.) along the DOMEX path to leverage opportunities to positively link individuals to networks. I expect lessons learned from the J2E concept will make a solid case for keeping DOMEX out of direct HUMINT management.

Personnel. Each service must determine which personnel in their force will be the primary operators of DOMEX equipment and assess what support personnel are required to maintain their programs. Support personnel are required to cover maintenance requirements and operate across the five functions of the Joint intelligence cycle. It's also important that the services track their DOMEX trained personnel with an ASI or separate MOS. Military officer and enlisted personnel management systems need to recognize and codify the new skill sets. Perhaps now is the time to develop and codify the multi-functional intelligence staff officer that has training in DOMEX tasks. These leaders will help intelligence manage three additional tasks (analyze, disseminate, and assess) that continually occur.

Thoughts on the Future of DOMEX

The true significance of DOMEX lies in the fact that terrorists, criminals, and other adversaries never expected their material to be captured. The intelligence produced from exploitation is not marked with deception, exaggeration, and misdirection that routinely appear during live questioning of suspects.[30] As our adversaries continue to move from paper to digital-based technologies, the exploitation of digital media, personal elec-

tronic devices, and video will require even more personnel and resources to maintain decision advantage. The ODNI has outlined *six DOMEX priorities* for the IC in order to create, mature, and sustain an efficient national DOMEX capability with a global reach.[31] Within the framework of these priorities, I offer some thoughts and recommendations:

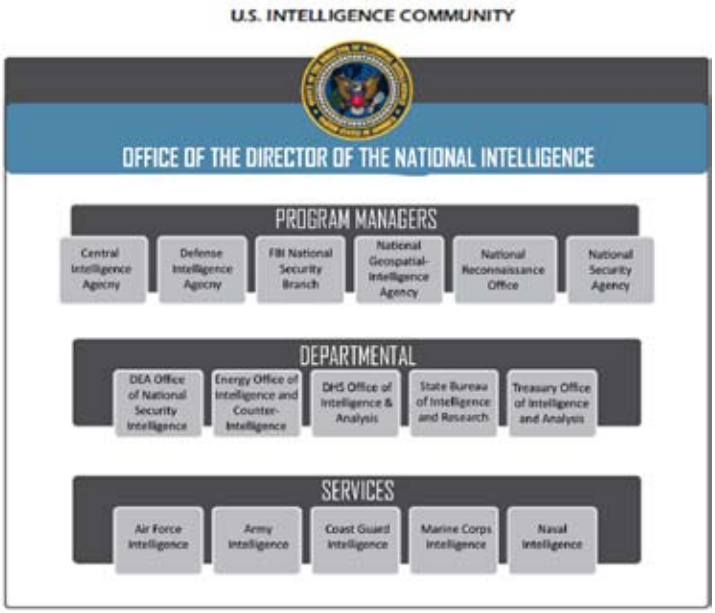
Effective Governance. *I recommend that the ODNI establish DOMEX as an intelligence discipline via an ICD.* ICD 302 states that DOMEX activities will support a wide range of intelligence activities.[32] Making DOMEX an intelligence discipline would be fully in line with the Under Secretary of Defense for Intelligence (USD-I) draft DOD DOMEX Directive.[33]

Collaborative and Integrated Planning/ Programming/Execution. If you search the Internet for the term "DOMEX," a web page from the U.S. Department of Justice's National Drug Intelligence Center (NDIC) will appear and readers can learn how the center supports National level policymakers and the IC by preparing strategic analytical studies on the trafficking of illegal drugs. NDIC provides real-time support to LE and ICs by conducting DOMEX associated with counterdrug and counterterrorism investigations. Like NDIC, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the DOD run their own DOMEX programs to support the missions and requirements of their unique organizations.

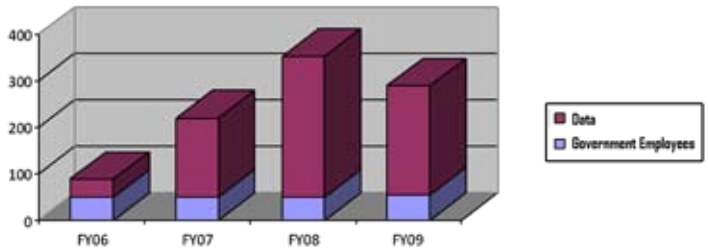
Unfortunately, these organizations have many cultural and security firewalls which limit their ability to provide access to their intelligence holdings to the IC stakeholders. We must continuously work to open these barriers through improved cooperative arrangements that provide the right information to a wider audience in order to reduce our intelligence gaps.

ICD 302 created the DOMEX Executive Committee (DOMEXCOM)[34] which includes senior members from the DIA, CIA, FBI, Defense Cyber Crime Center (DC3), U.S. Army, National Security Agency (NSA), Department of Homeland Security (DHS), and the Drug Enforcement Administration. The DOMEXCOM is great forum to hammer out agreements and roadmap strategies to enhance effectiveness of DOMEX across the IC. *I recommend that the ADDNI/OS request that each military service provide a representative to the DOMEXCOM if the U.S. Navy, U.S. Marine Corps, and U.S. Air Force desire successful DOMEX programs.*

Development of NMEC as our National DOMEX Enterprise CoE. I *recommend that the DOD/USD-I convert the NMEC into a National DOMEX Agency (NDA) to become the Program and Mission Manager for the IC*. By converting NMEC to the NDA to govern DOMEX, we would then follow the same approach used in the creation of the National Geospatial-Intelligence Agency (NGA) to produce GEOINT; NSA to produce SIGINT,[35] and CIA to be the center of gravity for HUMINT.[36] If there is no NDA, then NMEC will fail to meet its responsibilities as detailed in ICD 302 and not be in a position to "advise and assist the ODNI in identifying requirements, developing budgets, managing finances, and evaluating the IC's performance."[37]



If we don't commit ourselves to long overdue organizational changes, make DOMEX an intelligence discipline, and expand NMEC resources then the IC will not be able to achieve DOMEX goals and missions established by ODNI. One noteworthy



data point reveals that since Fiscal Year 2005, DOMEX data at NMEC has witnessed nearly a tenfold increase while government employees assigned to manage one of the most challenging intelligence missions in the IC has remained fairly flat (around 50 employees).

With the ever increasing demands for DOMEX, flowing from homeland security LE activities (FBI, DHS, etc.), we are now at a critical junction to either make a change to improve capacity to handle the volume of expected data or continue on course and risk not being in a position to thwart terrorist acts while in the early stages of planning.

The FBI's National Virtual Translation Center (NVTC) should be realigned within *the newly created NDA to gain more efficiency on the management of translation resources not only for timely and accurate translations of foreign intelligence, but for DOMEX as well.* The NVTC is currently the clearinghouse for facilitating interagency use of translators, partnering with elements of the U.S. Government, academia, and private industry to identify translator resources and engage their services. NVTC is a DNI Center, and the FBI is its Executive Agent. [38]

The USD-I should direct the establishment of a Military Support Branch in the NDA under the leadership of a one-star general. The military support branch should include liaison officers from each combatant command (COCOM) in order to improve global mission management of DOMEX activities. The support branch could help COCOMs link their DOMEX priorities into the NDA and better harness national DOMEX holdings to consumers supporting host nation counterterrorist efforts. Creation of a military support branch at NDA would follow similar constructs already in place at NSA and NGA. The lack of a military support branch assisting NDA prevents traction to fully synchronize and leverage DOMEX collection capabilities across the services and align large-scale DOMEX procurements and solutions for the services as research and development drives change.

The USD-I should direct that the U.S. Army designate the Army DOMEX Office (ADO) as DOD lead for service DOMEX program procurement. DA G2 designated NGIC as the dedicated DOMEX Program Manager responsible for the development and training of Army tactical DOMEX teams. In this capacity, the NGIC/DOMEX PM worked closely with NMEC over the past three years to field and sustain an Army tactical DOMEX presence in OIF/OEF. To better support strategic through tactical DOMEX research, development, test and evaluation appropriation initiatives, the ADO should serve as the DOD lead and action arm for the NDA. The ADO would be for DOMEX what the Army Cryptologic Office is for SIGINT, placing it in an ideal position to assist the other services reach their DOMEX equipment and standardization goals.

Deployment of a Federated DOMEX IT Infrastructure. *I recommend that the NMEC and ADO publish collection and processing standards to industry in order to select the best solutions for our DOMEX architecture.* Clearly an advanced IT infrastructure is required at the National level to help quickly organize, process, and disseminate captured information in virtually all formats in many languages. If the National DOMEX architecture is to truly be a "single, dynamic, integrated, and federated system, with cutting edge automation using the best-of-breed tools,"[39] then our collection and processing systems must tackle two distinct problems that Dr. Simon Garfinkel labels "deep" and "broad".[40]

The *deep* DOMEX problem covers the kind of document or data-storage device (a hard drive, DVD, or personal electronic device) that is captured and becomes available for analysis. The analytical goal is to find out everything possible about the data storage device. The DOMEX operators and analysts who receive a laptop, for example, want to know everything possible about it; not just the content, but the application programs, the configuration settings, the other computers with which these machines had come into contact, and so on.[41]

The *broad* DOMEX problem is the reverse. Instead of having unlimited resources to spend on a particular item, analysts are given a large number of digital objects and a limited amount of time to find something useful to their mission. In recent years the volume of captured digital information seized on the battlefield or within LE investigations has exploded. The landslide of digital media makes the broad problem quite compelling from both a national security and commercial perspective, a system that can reliably find the

"good stuff" can save money, time, and perhaps even lives.[42]

Future DOMEX collection systems (hardware and software) must provide solutions to cover the deep and broad DOMEX problems and minimize the number of stand-alone systems the operators must learn, use, and maintain. We should take advantage of equipment already fielded rather than providing more "boxes." This is not to say that there will not be some need for unique stand-alone systems to ensure needed capabilities. Each military service must ensure their DOMEX systems (hardware) fit within their Command, Control, Communications, Computers, and Intelligence construct and integrate into a cohesive and seamless entity within the national system.

Global Presence. Global presence starts by linking state and federal LE entities through Homeland Defense mechanisms and into our National ICs (CIA, DOD, and other government agencies). For example, we must be able to share and connect intelligence from a captured computer in Kuala Lumpur, Malaysia to our federal LE efforts to opportunities for our adversaries to conduct successful attacks.

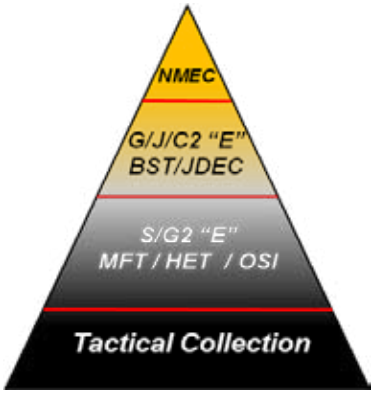
NOTE: All DOMEX operations conducted by Army intelligence personnel must comply with the legal restrictions in AR 381-10, and be conducted within the guidelines of U.S. law and applicable policies.

DOMEX practitioners who posses linguistic skills or provide access to linguists, must be strategically positioned (forward based) throughout our COCOMs to capitalize on opportunities as the present themselves. Ideally, the NDA could provide fly-away teams who are trained to operate in austere environments and have ready access worldwide to essential equipment, communications, and immediate reachback to the IC.[43]

Professional Skills and Training. Despite heavy investment in DOMEX training programs since 9/11, there has been uneven emphasis across organizational and training programs as ICs focus on their needs and culture. Inconsistency in content, quantity, and quality of training across the DOMEX community persists through varied processes for developing training requirements and standards. The result is costly duplication of effort, uneven performance during deployments, and significant unmet training requirements, particularly with regard to DOMEX analysis and technology integration.

The military services and IC must maintain a professionalized DOMEX force that follows a standardized and certifiable training program. We also lack a single set of standards or roadmap that outlines which DOMEX skills are required to meet basic, intermediate, and advanced DOMEX requirements at every level (tactical through strategic).

There are numerous training venues which are considered "accredited" to meet DOMEX mission requirements but there is no published community directive or message that aligns the total IC. Successful DOMEX operations hinge on proper collection; all military services must be organized to conduct *tactical collection* in land or maritime operations. Most importantly, the IC and DOD must be prepared to assist other nations in understanding the value of DOMEX and aid in training their forces as well. The proper inventory and collection of captured materials is no longer confined to intelligence personnel, anyone can collect. That cultural shift is based on lessons learned from combat operations. "It became clear that the existing intelligence gathering, analysis, and evidence collection methods were all inadequate for countering an insurgency, our ability to successfully prosecute intelligence operations was directly linked to the ability of our Soldiers to collect, preserve, and exploit evidence."[44] The organizational requirements above tactical collection are primarily intelligence-based and make up the processing, exploitation, and dissemination process. This is the layer that includes personnel from the Army's Multifunctional Teams, the Marine Corps HUMINT Exploitation Teams, U.S. Air Force Office



of Special Investigations, or sailors from the Office of Naval Intelligence.

One thing is certain–all military services must identify DOMEX training requirements for their forces and develop an appropriate communications infrastructure to relay DOMEX intelligence laterally and upward into the national intelligence system. *I recommend that the ADDNI/OS or USD-I designate the Navy and Marine Corps Intelligence Training Center, and USAICoE as the primary DOMEX institutional training bases for the military services*. The roles and functions of the Joint Military Intelligence Training Center and the DCITA as authorized training venues need to be clearly spelled out within an ICD or USD-I message to clarify their interaction with the IC and DOD DOMEX education system.

We must take several additional steps to strengthen each of the six ODNI priorities in order to achieve an enduring DOMEX capability across the national, military, intelligence, homeland security, and law enforcement communities, at all levels–strategic, operational, and tactical.

Conclusion

We have reached the point where a national decision is required to designate DOMEX as an intelligence discipline and to create a National DOMEX Agency. Similar conditions and decisions were made over 50 years ago as our government created agencies for HUMINT and SIGINT. If the strategic objectives are to extend intelligence to all who need it and to facilitate Homeland Defense through extensive collaboration, then if we fail to create a National DOMEX Agency, then I believe DOMEX will return to its previous condition of atrophy across the IC and DOD and our nation will not be in a position to effectively safeguard itself from multiple threats.

Endnotes

1 Response to Congressionally Directed Action, LTG Maples and Dr. Briscoe, 1 March 2009.

2 Kevin M. Woods, *Captured Records–Lessons from the Civil War through World War II*, Institute for Defense Analysis, 2009.

3. Ibid.

4. Intelligence Regulations, U.S. War Department, Washington, DC, 1920, 39-40.

5. Jared B. Schopper, "*The Collection and Processing of Combat Intelligence During Operations in Northern Europe*," Command and General Staff College Monograph, June 1964, 82.

6. Ibid., 84.

7. FM 30-15, Intelligence Interrogation, March 1969, 3-7.

8. Mark S. Partridge, "*Asking Questions: Will Army Tactical Interrogation Be Ready For War?*" School of Advanced Military Studies Monograph, 17 December, 1986, 37.

9. *Operational Leadership Experiences Project*, Combat Studies Institute, Fort Leavenworth, Kansas, Interview with CW3 Kenneth Kilbourne, February 2009, 8.

10. Donald P. Wright and Timothy R. Reese, *On Point II, Transition to the New Campaign: Operation Iraqi Freedom*, June 2008, 195. (Interview with MG Fast, CJTF-7 C2)

11. ODNI, 2009 DOMEX Annual Report.

12. NMEC Mission Statement, 2009.

13. U.S Senate, Select Committee on Intelligence. Report Number 111-16, Period Covered–4 January 2007 to 2 January 2009, 42.

14. SSCI Audit of IC Domex, April 2007.

15. Dan Butler, Paula Briscoe, Roy Apselloff, ODNI, National Document and Media Exploitation Enterprise Vision Pamphlet, Message from DOMEX Seniors, April 2009.

16. Richard P. Zahner, "*Rebalancing the Army Military Intelligence Force*," AUSA Green Book, October 2009, 186.

17. JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 31 August 2005.

18. ODNI Intelligence Community Directive 302, Document and Media Exploitation, 6 July 2007.

19. FM 2-0, Intelligence (Final Draft), March 2009, 1-30.

20. TRADOC Pam 525-7-9, Version 1.0, 12 August 2008, 40.

21. FM 2-22.3, Human Intelligence Collector Operations, September 2006, 1-6.

22. TC 2-91.8, Document and Media Exploitation Enabled Intelligence (Final Draft), 25 July 2008.

23. FM 2-22.3, 2-6.

24. U.S. Army MI BN (BFSB) MTOE, DOCNO 34105GFC18, Para 206, Lines 02-17.

25. U.S. Army Combined Arms Center, Site Exploitation Concept of Operations (CONOPS), 2010-2016.

26. Army Enlisted Job Descriptions, About.com: US Military at http://usmilitary.about.com/od/enlistedjo2/a/35.-xiW.htm.

27. DOD Cyber Crime Center at http://www.dc3.mil/dcita/dcitaAbout.php.

28.CHATS AN/PYQ-3(V)3 at http://chams.it.northropgrumman.com/brochures/CHATS%20V3%20Factsheet.pdf.

29. Intelligence Programs and Systems, at http://www.globalsecurity.org/intell/systems/index.html.

30. NMEC, 2009 Resource Management Plan, 5.

31. ODNI, National DOMEX Enterprise Vision Pamphlet.

32. ICD 302, DOMEX.

33. USD(I), DOD Directive 3300.aa, Document and Media Exploitation (DOMEX), Draft.

34. ICD 302, DOMEX.

35. Mission statement at http://www.nsa.gov/about/mission/index.shtml.

36. Establishment of the National Clandestine Service, CIA, 13 October 2005 at https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr10132005.html.

37. Deputy Director of National Intelligence for Policy, Plans, and Requirements, *2009 National Intelligence: A Consumer's Guide*.

38. Ibid

39. ODNI, National Document and Media Exploitation Enterprise Vision Pamphlet,

40. Simson L. Garfinkle, *"Document and Media Exploitation,"* Association for Computer Machinery, accessed at http://queue.acm.org/detail.cfm?id=1331294.

41. Ibid.

42. Ibid.

43. ODNI, National Document and Media Exploitation Enterprise Vision Pamphlet.

44. Ralph O. Baker, "Developing Actionable Intelligence in the Urban COIN Environment," *Military Review*, March-April 2007.

Colonel Joseph Cox served as Commander, 519th MI Battalion (BfSB) during OIF 07-09 between September 2007 and December 2008. He is a 1987 graduate of OCS and has also served in the 525th MI Brigade; 82d Airborne Division; 75th Ranger Regiment; 205th MI Brigade, and the 525th BfSB. He recently completed a U.S. Army Senior Service College Fellowship Program in Washington, D.C. and is now the Commander, 501st MI Brigade, Korea. Colonel Cox may be reached at joseph.cox@us.army.mil.

Tactically Tailoring the Maneuver Enhancement Brigade

by Major Marilyn Harris and Captain Carolyn Bronson

Introduction

Army intelligence is supposed to "provide timely, relevant, accurate, and synchronized intelligence support to tactical, operational, and strategic commanders from force projection planning to the execution of full spectrum operations."[1] However, without the requisite intelligence collection means at the tactical level, a brigade commander cannot adequately visualize the battlespace or identify decision points to employ nonlethal and lethal resources against his full spectrum mission set. Lessons learned and observations from operations in Afghanistan revealed the importance of a battlespace owner (BSO) possessing dedicated tactical intelligence, surveillance, and reconnaissance (ISR) capabilities in a counter-insurgency (COIN) environment.

Non-Standard Brigade Combat Team (BCT)

During Operation Enduring Freedom IX, the 1st Maneuver Enhancement Brigade–the first active duty maneuver enhancement brigade (MEB), organized as Task Force (TF) Warrior, forward deployed to manage terrain and command and control operations within four provinces of Regional Command East, Afghanistan. The nascent MEB concept is the result of the Army's transformation to a modular structure whereby multifunctional brigades are tailored to conduct full spectrum operations. This was the inaugural combat deployment of a MEB during which it served as BSO. TF Warrior was uniquely tailored with a mix of international partners, several types of battalions, Provincial Reconstruction Teams (PRTs), an Agribusiness Development Team, a Human Terrain Team (HTT), two Police Mentor Teams (PMTs), and an Embedded Training Team (ETT) for its mission against the complex, adaptive, asymmetric threat of the COIN environment. Like the other deployed BCTs, the agile construct of TF Warrior allowed for the flexibility to simultaneously conduct decisive stability and support operations across four lines of effort (LOEs)–security, governance, development, and information.

Although the security conditions within much of the TF Warrior's area of operation (AO) were semi-permissive (meaning that security conditions were relatively good within much of the region), challenges existed in 7 of the 31 districts. Within those friction areas, TF Warrior units habitually conducted offensive operations in Taliban and Hezb-e Islami Gulbuddin insurgent controlled areas.

Extensive targeting–nonlethal and lethal, was conducted against all four LOEs. In all areas it was critical for the brigade commander to possess an accurate assessment of the operational environment (OE). Moreover his understanding of the threat against all four LOEs and the social and civil factors was the linchpin in determining the type and frequency of resources to commit in order to obtain the desired objectives of his campaign plan.

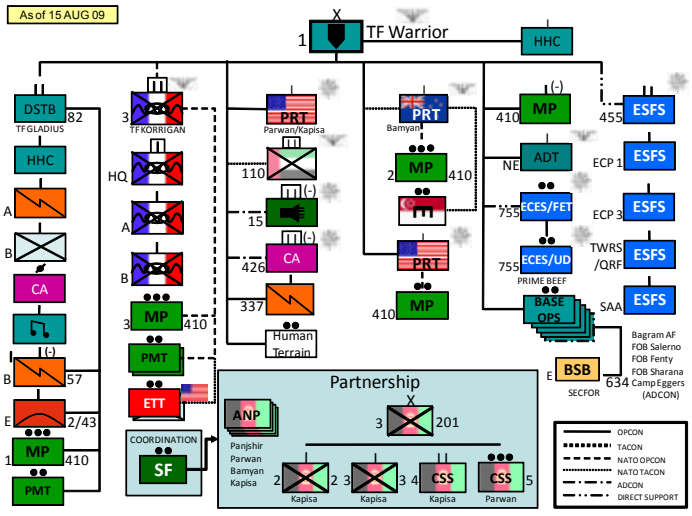


Figure 1. TF Warrior's Organization.

There were various sources of information available for the brigade commander to visualize his battlespace and aid him in the identification of decision points to employ nonlethal and lethal resources against his full spectrum mission set. Daily we received reports and assessments from PRT leaders regarding social dynamics, the status of development projects, area atmospherics, and their interaction with provincial and district leaders. The anthropologists within the HTTs were also a great source of information regarding area atmospherics (perceptions and population sentiment regarding coalition operations, local powerbrokers and the span of influence and control of anti-Afghan insurgent leaders and the threat they posed to TF Warrior's objectives.)

Similar information was provided by ETT, PMT units and patrol leaders. We also devised creative solutions to bridge the gap between information received from Coalition Forces and the Afghan people. Through an exchange workshop developed under our Police Intelligence Operations cell, we obtained information through host nation law enforcement and intelligence channels to corroborate information and obtain evidentiary material to provide intelligence that could answer "Warrior 6's" priority intelligence requirements (PIRs). Local Afghans and various casual contacts would provide information. However, critical intelligence gaps prevented this information obtained through human sources from being cross-cued with collection assets from other intelligence subdisciplines and subsequently prevented this information from being transformed into actionable intelligence.

MEB Limitations

While executing diverse missions across the broad geographic AO and complex OE, it was evident that there were organizational and materiel shortfalls and it was evident that the MEB was not properly resourced for its mission set. The brigade headquarters was robustly staffed with diverse functional and operations planning cells, however, the brigade itself contained no organic units other than its HHC and Signal Company. One key enabler that failed to be tactically tailored in support of TF Warrior's formation in light of the mission assignment, was a Military Intelligence (MI) enabler. Currently Battlefield Surveillance Brigades, a product of the Army's modularity concept which provide ISR support to Corp-level units, are not organized with tactical level unmanned aerial surveillance (UAS) platforms from which a brigade level BSO can request resources. As the Army increases the versatility of units through the transformation process to provide "BCT-like" capabilities, they also need to increase the capabilities of MI enablers, specifically surveillance and reconnaissance assets to support multifunctional organizations.

During the Afghanistan mission the lack of organic or attached ISR assets was a detriment to the effectiveness and combat capability of TF Warrior. The commander and staff conducted the military decisionmaking process to identify critical information about the OE that the commander required to make decisions. However, we essentially did not have access to the full capabilities of a traditional functional BCT whereby we could commit dedicated ISR assets to monitor whether we were seeing indicators of the commander's established PIR. Moreover, because we lacked the persistent collection systems from Imagery Intelligence (IMINT) and Signals Intelligence (SIGINT) sub-disciplines, we lacked the ability to ensure seamless horizontal and vertical situational understanding of our provinces.

Collection Gaps

The purpose of ISR is to enable commanders to direct military operations toward a defined objective area at a time and in a manner which allows him the best advantage. "ISR operations allow units to produce intelligence about the enemy and OE necessary decisions. . . . Timely and accurate intelligence encourages audacity and can facilitate actions that may negate enemy tactics and material."[2] The converse is also true. The lack of organic ISR assets and dedicated tactical level ISR assets resulted in information gaps that greatly hindered the ability of the TF staff to answer the commander's PIRs and hindered the staff's ability to effectively recommend asset employment strategies. The ability to have dedicated ISR assets would have contributed immensely in supporting the TF mission across all lines of effort.

For example, the limitation of dedicated ISR assets hindered our ability to detect patterns of movement among suspected enemy routes and prevented us from confirming or denying these enemy lines of communication. This ultimately limited our ability to detect enemy staging locations for attacks and

infiltration routes and exfiltration routes in vicinity of attack sites. There was limited visibility on suspected enemy supply routes, which precluded the TF from interdicting insurgent movements of weapons, ammunition and explosives.

In the development LOE, this paucity of assets prevented us from monitoring the many development projects that were in construction throughout the AO. These projects primarily included road and bridge construction and the establishment of new government facilities. Many of these projects were consistently threatened for attacks by insurgent forces. Key bridges were destroyed to preclude Coalition Forces aiding defending Afghan forces against insurgent forces. Once repaired these key areas continued to receive additional threats of attacks. The low visibility of these projects constricted our views of the overall security and progression of these projects, which directly affected the freedom of movement of the local populace.

There were numerous reports suggesting that key and influential personnel in government and Afghan security positions were cooperating with known insurgents throughout the AO. These reports remained unconfirmed due to a lack of dedicated assets that could assist in monitoring all activity of these individuals to known insurgents' AOs. In addition there was limited coverage of all activity in vicinity of mosques that were reported to be used for insurgent meetings and pre-staging locations for attacks. This limited our knowledge of any anti-coalition and anti-Afghan government rhetoric that was being used in support of insurgent information operations, which inevitably caused issues in our ability to promote a successful pro-Government of the Islamic Republic of Afghanistan and Afghan National Security Forces campaign targeting the local populace.

The overall effect of a lack of ISR assets dedicated to the TF was a huge limitation on lethal and non-lethal targeting opportunities on known insurgents and the overall ability to prevent/deter/detect insurgent activities. Just as "intelligence drives operations," the lack of adequate intelligence also drives operations. The inability to visualize the battle space subsequently hindered the movement and capabilities of all coalition units throughout the AO, and consequently hindered the progression of security, governance, development and information efforts throughout the TF AO.

Challenges–MEB ISR Comparison

Theater level ISR assets were recurrently allocated in support of TF Warrior operations for a limited duration during the execution of offensive operations. However, due to the dynamic nature of the OE, the sparsely allocated full motion video support did not provide us the required persistent surveillance capability. Limited duration ISR coverage is insufficient for a COIN environment. Due to shortages of Theater ISR assets, mission priorities often precluded the allocation of ISR in support of TF Warrior operations.

As a result of constraints, the MEB ISR assets were not on par with BCT peers. TF Warrior's ISR capabilities were severely limited in comparison to other BSOs. Although its OE was much more permissive, information requirements existed outside of the security LOE that were critical in aiding the commander to monitor measures of effectiveness of his decision points in governance, development and information LOEs. All BSOs should have dedicated ISR capability whether from organic, direct support or general support enablers. This augmentation should be considered during the sourcing phase for unit deployment to ensure units are properly tailored for mission execution.

Tailoring for the Operational Environment

Modified table of organization and equipment (MTOE) design shortfalls revealed that force developers should consider ISR augmentation of UAS platoon and tactical SIGINT support for the MEB during

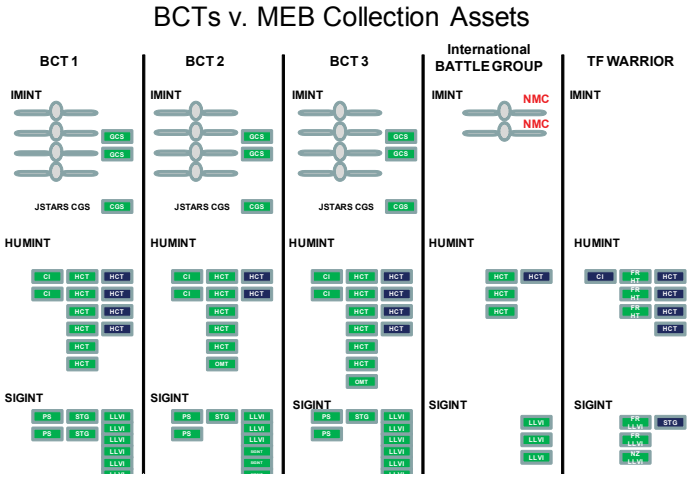


Figure 2. Comparison of ISR Collection Assets.

forward deployments. The absence of brigade and below level ISR assets (UAS and SIGINT) for persistent surveillance inhibited the brigade commander's ability to continuously monitor his named areas of interest and inhibited the unit's "find" capability during the targeting cycle. As mentioned this resulted in intelligence gaps of threat group patterns and ignorance of threat tactics, techniques, and procedures.

One of the drawbacks identified was that the targeting battle staff could not action time sensitive intelligence due to lack of organic assets to establish positive identification of threat personalities or confirm target location. Operations were often postponed because of the inability to confirm or deny enemy presence or conduct target acquisition. Our recommendation is for force developers to update the MTOE for the MEB, taking combat mission deployments into account and augment the MEB with an MI detachment.

An MI detachment (with MI company functions and capabilities) consisting of organic UAS platforms and tactical SIGINT assets and required personnel and equipment for tasking, processing, exploitation and dissemination should be allocated for each BSO conducting fullspectrum operations.

Detachment in support of a MEB

In addition to equipment and collection systems, the personnel MTOE of the MEB was inadequate for TF Warrior operations. In theater we discovered that our mission expanded beyond what we observed during the predeployment site survey and required the S2 section to have specialized expertise in various disciplines and access to other systems, databases and software that were utilized by the CJ2 staff for single-source processing of intelligence. All-source analysts had to execute the functions of specialized intelligence technicians and quickly underwent on-the-job training on SIGINT, Human Intelligence (HUMINT), and IMINT analytical tools and systems. We offer a strong recommendation for a change to the MEB personnel MTOE. The S2 section organization must be updated to reflect operational needs as much as possible. Single source intelligence disciplines (SIGINT, IMINT, and HUMINT) Soldiers should be part of the MEB MTOE to contribute to the total intelligence fusion process.

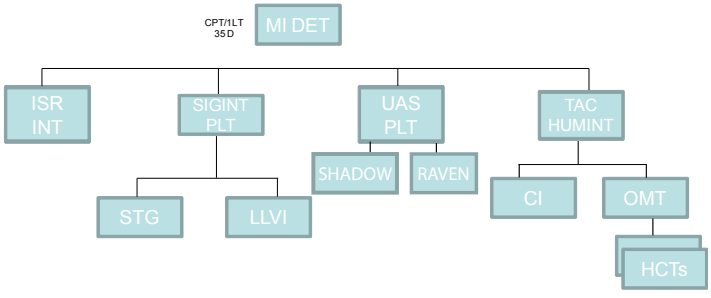


Figure 3. Recommended Structure of a MEB MI Detachment.

Personnel Recommendations for MEB S2 Section

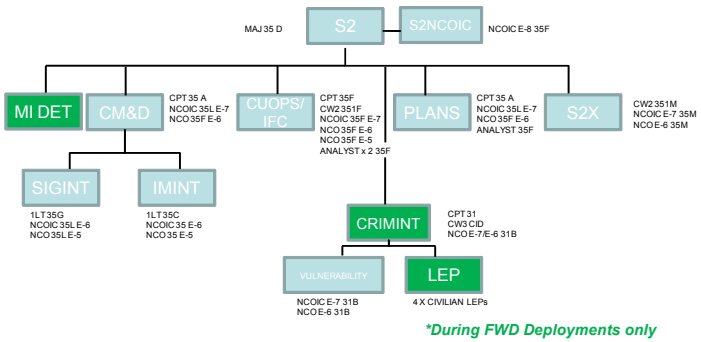


Figure 4. Recommended Personnel MTOE for the MEB S2 Section.

Conclusion

Force developers have the challenging task of providing the right unit to support combatant commanders in contingency operations. The 1st MEB successfully completed its mission as a "fourth BCT," however the lack of a dedicated MI collection unit attached for mission execution, was a detriment to the effectiveness and combat capability of TF Warrior. Due to the lack of dedicated collection resources, there were too many unknowns which prevented the brigade staff from accurately defining the OE for the commander. Moreover, we lacked the ability to adequately measure the effectiveness of both our nonlethal and lethal targeting efforts against all four LOEs. These observations from within the TF Warrior AO clearly revealed the importance of a BSO possessing dedicated tactical ISR capabilities in a COIN environment to complement other sources of intelligence.

References

1. FMI 2-01, ISR Synchronization, November 2008. 1-5, 1-6 para 1-28.

2. FMI 2-01. 1-2, para 1-11.

Major Marilyn Harris is the 1st MEB Intelligence Officer. She served as the 1st MEB S2 OIC in support of OEF. Previous assignments include the CFSOCC Collection Manager. MAJ Harris holds a Master's in Strategic Intelligence and attended the 35G SIGINT Course at Fort Huachuca, Arizona. She may be contacted at marilyn.saintlein@us.army.mil.

Captain Carolyn Bronson is the 1st MEB Assistant S2. She served as the S2 Plans Officer and Collection Manager for the 1st MEB in support of OEF. CPT Bronson holds a BA in Political Science from Norwich University. She may be contacted at carolyn.bronson@us.army.mil.

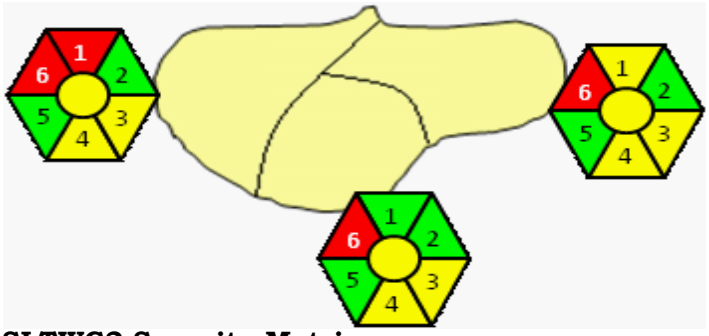
by Major Charles Assadourian

Introduction

The methods of measuring progress in any large endeavor are essential, yet often difficult to agree upon.[1] This is particularly true when the endeavor requires qualitative measures. Public debate regarding counterinsurgency (COIN) often raises this issue, but attention span in the news cycle does not permit complex answers to complex problems.[2] This complexity stems in part from the numerous entities involved which include external or foreign forces, host nation (HN) forces, HN government agencies, subsets of the population, and insurgent elements. Given this complexity, how can leaders translate the desired end state into specific tasks for Soldiers? Answering this question first requires clarification of desired outputs of the tasks.

Traditional measures of security in COIN often focus on the number of attacks executed or number of detainees captured.[3] While these are valid measures, a more holistic approach requires an examination of instances resulting in positive outcomes. In this, HN government and population activities are as important as enemy activities. Appropriate measures include events on the timeline in cases with successful outcomes. Such measures can shape priority intelligence requirements and reinforce or shape the commander's assessment of the environment.

Based on this, an examination of the "successful event" timeline or process, starting from the last event back to the beginning significant activity or incriminating act, produces measurable data points. Apart from a lack of casualties, the ideal situation ends in conviction of the insurgent. Prior to this, the security forces must capture the individual and exploit all available evidence at the point of capture or other relevant location. Prior to capture, the security forces must have a warrant or positive identification of incriminating activity. Prior to the warrant the security forces must receive tips or reporting of incriminating activity, such as the assembly of an improvised explosive device. Prior to the tips or reporting, the insurgent must attempt an attack or activity which would lead to a kinetic attack. Thus, six different metrics result from the timeline in case studies with positive outcomes. The acronym SLTWC2 captures these benchmarks for success.



SLTWC2 Security Metrics

1. SIGACTS.
2. Local security force networking.
3. Tips and reports.
4. Warrants.
5. Captures and sensitive site exploitation.
6. Convictions.

These metrics serve to evaluate the effects on the environment as well as those on the enemy.

In order of priority, desired effects on the enemy include reconciliation, capture, kill, marginalization, or exile. The criteria used to assess as green, amber, or red will vary based on local conditions and the desired end state. Each of the six metrics has unique linkages with each of these effects which can occur at any point in the SLTWC2 cycle. When tied to geographic areas, the six measures serve to indicate progress, stagnation, or regression and the boundaries between one or more of these assessments of the terrain. In all cases, HN buy-in dramatically increases the probability of success. What represents an external threat to the external force is a domestic threat to the HN.

A simple matrix captures the essential bits of information for each of these metrics. A workbook, such as the type typically used for SIGACTs, serves as an excellent tracking tool for the six components. An elaboration of each metric offers insight into the headings for each worksheet in the workbook, as well as their relationship to the five desired effects.

SIGACTS. While SIGACTs only provide a portion of the information necessary to effectively evaluate the environment,[4] they remain valid as one of a number of measures of effectiveness. SIGACTs and the events and resources which precede them are critical as incriminating evidence in the development of the rule of law. When combined with other information, SIGACT data can help explain the reasons for boundaries between permissive and non-permissive areas. SIGACTs also indicate threat group capabilities through the identification, elimination, or proliferation of new or signature tactics, techniques, and procedures.

Key to most successful SIGACT responses is the forensic exploitation of biometrics and ballistics. A qualified investigative officer must be part of this process from the beginning. Depending on the volume and nature of most SIGACTs, the type of crime qualifying as a SIGACT may be broadened or narrowed to include a meaningful yet manageable volume.

Local Security Force Networking. Local security forces are a critical component for evaluation.[5] Even when the actual perpetrator is captured or killed on sight, after a SIGACT occurs the counterinsurgent must know who to call to gain additional information or to explain the circumstances accurately before insurgents do. Security forces must establish roots in the community and fight to maintain them. This is true for both the foreign forces as well as the HN force. It takes a network to defeat a network, and nodal analysis is critical.[6] A key leader engagement with a local leader is good for a foreign force, but there is generally more value added between two or more HN elements. The frequency and outputs of HN key leader engagements allow opportunities for both qualitative and quantitative measures, the two categories of data points in determining success.[7]

In addition to engagements a number of other factors impact success. The existence of liaison officers, an active internal affairs, professionalization (consisting of expertise, corporateness, and responsibility),[8] clear roles and responsibilities (jurisdiction), the ability to gain biometric entries and intelligence, surveillance, and reconnaissance requests are some instances which provide opportunities to enhance COIN networking. All these organizations merit nodal diagrams which run vertically and horizontally and show informal relationships. Every driver of instability in a particular environment ties into one or more of the networks in the environment. Network challenges include vacant positions; the transition of former insurgents; the replacement of corrupt, complicit, or incompetent leaders, and political motivations.

Security force networking measures also include nonlethal aspects of COIN. The details of SWEAT-MTA (sewage, water, electricity, academics, trash, medical, transportation, and agriculture) and other elements of intelligence preparation of the environment offer inject points to enhance both the COIN and civil service networks. Hosting meetings to discuss various drivers of instability offers opportunities to increase interaction internal to local COIN and other environmental networks.

COIN leaders from all agencies should shape a common assessment of the enemy and intelligence preparation of the environment. Good networking helps prevent overreactions to significant events. Security forces and other community leaders such as essential service, social, and business leaders must be perceived as a consistently united front and key to a better future. This strengthens rule of law. The external security force must seek to be a catalyst for HN COIN efforts. Local security forces

must actually be in the lead, and not just appear to be in the lead. Networking effects are primarily reconciliation of insurgent elements and fence sitters but also lead to the other four effects.

Tips and Reporting. As networking begins, tips and reports will begin to flow in to the extent that support for COIN exists within the community. These can vary from mere rumors to incriminating physical evidence and come from initial contacts or historical relationships. It is important to get sworn statements, and when possible, testimony. Atmospherics, early warning, cache, or high value target locations are most meaningful in areas without significant prior reporting.

Counterinsurgents must be alert to filter false accusations or deceptive information. Tracking the volume, accuracy, tone, and geography of reporting yields key insights into both the enemy and the operational environment. An increase in tips and reporting often indicates an increase in reconciliation and can lead to other desired effects.

Warrants. Following a stream of reporting the counterinsurgent should seek a warrant. Critical to this are topics such as appropriate jurisdiction, judicial independence, and biometric matches. After obtaining a warrant, wanted posters and other targeting efforts possess a greater level of legitimacy. The ability to obtain a warrant depends upon available evidence and probable cause, judicial independence, resistance to corruption and political connections, and investigative and judicial competence.

Investigative officers must be able to analyze and summarize incriminating information as well as gather and present evidence. Warrants are also critical for the release of detainees into HN police custody from external force custody. The publishing of warrants generally results in one of three things: the insurgent is turned in (capture), flees (exile), or claims innocence (reconcile). In all three instances, case development does not end at this point, as the ideal case ends in successful prosecution.

Captures and Sensitive Site Exploitation. After obtaining a warrant, the counterinsurgent typically enjoys increased legitimacy to conduct detentions. Conversely, extra-legal actions reduce security force credibility and the perception of professionalism. Like SIGACTs, capture and search actions should include a trained and certified investigative officer to supervise biometric and forensic collection and processing of evidence. The capture must lead to initial and follow on judicial reviews. Proper chain of custody helps determine admissibility in court. This requires timely release of the details of the capture to HN authorities. Understanding HN investigative standards and any gap with desired standards aids the foreign force in providing assistance.

The significance of captures varies according to the detainee's place in the threat order of battle and the willingness to provide information in interrogation. Cache significance varies according to size and content. Detention orders following an unplanned detention reflect positively on the legal environment. Dry holes, indicators of early warning, or subsequent releases often reflect negatively. While a desired end state in itself, capture can often lead to the other four desired end states.

Convictions. True success following a capture includes a conviction in an HN court. This requires the political will to prosecute and knowledge of specific judicial preferences. Key aspects of conviction outcomes include judicial throughput, length of sentences, number of pardons, conviction/acquittal rate, specific roles of the defendants, and the details of testimony. It is important to consider that the need for judicial independence must have a significant impact on meetings with judges.

Failure to convict can result from complicity, incompetence, investigative or judicial corruption, or exposure of false accusations. While most prefer to think of courts as apolitical, courts often demonstrate a certain legal threshold which may or may not be met by available evidence. This requires significant HN administrative skill sets. Within this metric, convictions in cases of external force casualties weigh more heavily than HN victims, as the threshold is generally higher for the external force. Regardless, each conviction marginalizes or exiles a specific threat but can also lead to the other effects.

Conclusion

The use of SLTWC2 enhances planning to better define and apply resources to influence the environment. These metrics flow from the desired end states and the events which precede them. SLTWC2 offers opportunities in subordinate criteria to examine both quantitative and qualitative measures. It

also offers commanders opportunities to translate intent into specific tasks for subordinates.

I have successfully used these metrics to evaluate security in partnership with Iraqi forces. While the variables may not be entirely independent, a positive change in SLTWC2 data points coincided with anecdotal atmospheric evidence of success. This success resulted in the reconciliation, capture, killing, marginalization, or exile of significant threat elements. Organization of data collection efforts along these lines can increase the capture of appropriate information which better enables commanders to influence the environment.

Endnotes

1. David Kilcullen, *Testimony before the House Armed Services Committee Hearing on HR 1886, the Pakistan Enduring Assistance and Cooperation Enhancement (PEACE) Act 2009*, 23 April 2009. 3.

2. Eli J. Margolis, "How to Measure Insurgencies," *Small Wars Journal Posting*, 12 September 2007.

3. Jonathan J. Schroden, "Measures for Security in a Counterinsurgency," *Journal of Strategic Studies*, 32, 5 (October 2009): 715.

4. Tom Ricks, "Kilcullen (I): Here's what not to measure in a COIN campaign," *Foreign Policy*, 8 February 2010. Accessed at http://ricks.foreignpolicy.com/posts/2010/02/08/kilcullen_i_here_s_what_not_to_measure_in_a_coin_campaign.

5. Tom Ricks, "Kilcullen (IV): How to measure Afghan army and police units," *Foreign Policy*, 11 February 2010. Accessed at http://ricks.foreignpolicy.com/posts/2010/02/11/kilcullen_iv_how_to_measure_afghan_army_and_police_units.

6. John Arquilla and David Ronfeldt, *Networks and Netwars* (Santa Monica, CA: RAND, 2001), 15.

7. Jack D. Kem, "Assessment: Measures of Performance and Measures of Effectiveness," *Military Intelligence Professional Bulletin*, April-June 2009, 49.

8. Samuel Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations* (Cambridge, MA: Belknap Press, 1957), 8.

Major Charles L. Assadourian is currently the S2 for 2nd Brigade, 1st Calvary Division and recently returned from deployment in MND-N. His last assignment was as the S2X for 1st Brigade, 1st Cavalry Division where he served in MND-B from October 2006 to January 2008. He is a 1997 graduate of the U.S. Military Academy at West Point where he received a BA in Political Science. He is a graduate of the Air Assault School, FAOBC, MICCC, and the Signals Intelligence Officer Course. Major Assadourian can be reached at chuck.assadourian@us.army.mil.

Memetic Warfare: The Future of War

by First Lieutenant Brian J. Hancock

Introduction

The War on Terror pits the large conventional units of the U.S. against small, agile, and adaptable enemies around the world. The post modern world of warfare is characterized by a threat which can raise funds within the boundaries of the country it wishes to attack, train and acquire equipment within those same boundaries, and then ultimately execute its mission.

The response of the U.S. to this unprecedented challenge is embodied in the 2006 revision of FM 3-24 Counterinsurgency. This counterinsurgency (COIN) manual is a significant improvement over its predecessors. It recognizes how non-military aspects of the environment bear significantly on shaping insurgency and fueling terrorist movements. It devotes significant attention to recognizing these factors, and provides frameworks for analyzing and addressing them. Two such frameworks are ASCOPE (areas, structures, capabilities, organizations, people, and events) and PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, time).

While the revision of FM 3-24 is a significant improvement over its predecessors, it does have shortcomings. As insurgent movements continue to evolve, the most successful operate in complex urban terrain, receive indirect support from criminal activities and external agencies which reduces their need for popular support, and have an ideological appeal grounded in religious fundamentalism. The new manual devotes only a single paragraph to this environmental change indicating that urban insurgencies are "difficult to counter" because they require little or no popular support.[1] Even more significantly, the doctrine of breaking up the rich tapestry of a society into bite size pieces is an attempt to apply a reductionist mindset to a complex adaptive system. The predicable end result is that the symptoms of the insurgency are treated in the hopes that the insurgency will go away, while the actual root causes–pathogenic *memes*, or viruses of the mind–are never addressed. This leaves open the possibility that in time, the insurgency will reconstitute itself, requiring the U.S. to intervene once more at the cost of additional lives and other resources.

This article will explore how an emerging subfield of psychology known as *memetics* can be used to identify and target the specific root causes of insurgency and other challenging social problems such as youth gang violence, the welfare cycle, or the deterioration of the public school system.[2] Finally a practical model for constructing and propagating benevolent memes in theatre, at the brigade level, will be presented.

Memetics Defined

The Oxford English Dictionary defines a meme as "an element of culture that may be considered to be passed on by non-genetic means, especially imitation." In his landmark book, *The Selfish Gene*, author Richard Dawkins coined the word meme to describe cultural replicators which spread through the social body akin to how genes spread through the biological body.[3] Memes form the invisible but very real DNA of human society. A meme is essentially an idea, but not every idea is a meme. In order for an idea to become a meme it must be passed on—or *replicated* to another individual. Much like a virus moves from body to body, memes move from mind to mind. Just as genes organize themselves into DNA, cells, and chromosomes, so too do replicating elements of culture organize themselves into memes, and co-adaptive meme complexes or *"memeplexes."* The study of these replicating elements of culture is known as memetics.

Sample memes include "Look both ways before you cross the street," "Just say no," the first four notes of Beethoven's 5th symphony, or "If you martyr yourself you will receive 72 virgins in the afterlife." As illustrated by the last example it is important to note that memes do not necessarily have to be true in order to be successful at replicating themselves. The memes an individual possesses forms the basis of his artifacts and behaviors. Some memes replicate more successfully as a related set, or memeplex, than as individual elements. Sample memeplexes include the scientific method, communism, and radical Islam.

Genes are measured along three principal axes, specifically fidelity, fecundity, and longevity.[4] Genes

replicate digitally through the process of mitosis. Discounting occasional mutation, translocation, etc., the copy fidelity of DNA is very high. Memes however, aside from transmission via digital media, are often passed on through the asynchronous process of conversation which has a much lower copy fidelity. Anyone who has ever played the game of telephone or Chinese whispers knows that the message given at the beginning of the chain is often very different than what the last person in the chain receives. Fecundity of DNA is only moderate, as the organism has to grow to sexual maturity and then pass its genes on through sexual reproduction. This process is relatively slow, taking an entire generation to occur. By comparison, memetic evolution is extremely fast.[5] In the span of a couple of minutes several memes can be transmitted from one person to another. Memetic evolution is exponentially faster than genetic evolution, so it should be no surprise that memes have surpassed genes as the dominant driver in human behavior.[6]

Finally genes are measured in terms of their longevity–defined by the life of the individual who carries them and their existence within the larger gene pool. As memes exist in the minds of human hosts they possess similar constraints on their preservation–both within the individual–and within the meme pool which is comprised of books, recordings, and other storage devices. Just as genes with higher fidelity, fecundity, and longevity can overwrite and replace lesser genes, the same is true of memes as well.

Viruses of the Mind

While most memes are beneficial, or at least relatively harmless, some memes such as the Nazi master race meme or the Pol Pot communist mutation are responsible for many human deaths. When individuals are so consumed by a meme/memeplex that the entire purpose of their existence becomes to spread the meme, they have become *memeoids*. These individuals are willing to throw away their own genetic reproductive potential by strapping on bombs or flying airliners into buildings in order to promote the memeplex that consumes them. Pathogenic memes which have potentially disastrous effects on their hosts and their neighbors are termed "viruses of the mind."[7]

With this frame of reference it is possible to see the actual root cause of terrorism and insurgency. Terrorists and insurgents do not suffer from declining per capita income or an unstable government–such are merely shaping operations which allow the true problem, a disease of the mind, to sweep through the weakened body politic. It has been postulated that prior to armed military conflict, xenophobic war memes must reach a certain critical mass within the host population in order to support aggressive action.[8] The cure for war then, and the key to preventing future wars, is to identify, track, isolate, and eliminate the specific memes which form the basis for the conflict. This is a task for which the intelligence community (IC) is uniquely qualified. The extinction of certain pathogenic memes would have an effect as profound as the eradication of smallpox.

Memetic Cults

Certain organizations, such as al-Qaeda, utilize modern brainwashing techniques in order to turn otherwise ordinary people into memeoids with which they can then inflict upon their memetic opposition. The human brain, despite its large capacity, can only hold a finite number of memes. This forms the basis of memetic selection. Additionally, some memes are diametrically opposed. Xenophobic memes which espouse rigid control over society, and most especially its female members, are being challenged on a daily basis by western liberalism. The clash of these opposed memes and memeplexes leads to reactionary memetic cults such as al-Qaeda.

Al-Qaeda isolates its potential new members in order to expose them to a single meme set many times a day for months, or years, without contact from other memes. Exclusive exposure to one meme (also known as brainwashing) induces a "dependent mental state" in some people.[9] They also employ tested and true techniques of bypassing the human action-attention-reward (AAR) complex which is a fundamental part of the human psyche. Status among primates is defined by attention integrated over time. When human beings receive lots of attention, it elevates their status, and causes their brains to release dopamine and endorphins giving them a "high." [10] Cults like al-Qaeda heap large amounts of attention on prospective martyrs in order to bypass the natural AAR pathway and release pleasure chemicals in the brain of the recipient. The recipient then misconstrues this positive feeling with the meme set of the organization causing them to internalize the beliefs of the cult as the source of their pleasure. Al-Qaeda employs many other modern brainwashing techniques to propagate their narrative (memeplex).

The discovery of John Walker Lindh (The American Taliban) brought to light one of the critical shortcomings of modern COIN practice. As the U.S. does not practice COIN at home, it can neither predict nor defend against home grown extremists. John Walker was rushed to justice, and as a result very little intelligence was gained from him and a valuable opportunity to understand the extremist movement was lost.[11] The application of memetics affords the understanding that John Walker was in fact suffering from a disease of the mind. Had he been de-programmed, and inoculated against the cult memeplex, it would have been possible to re-insert him as a double agent and begin taking the Taliban apart from within.

Curing Insurgency and Terrorism

The ultimate long term cure for terrorism and insurgent movements is to attack them at the atomic level through a process of memetic warfare. By identifying, cataloguing, and tracing the pathogenic memes that lead to these behaviors it will be possible to predict when and where they will occur. When the IC perceives that a certain dangerous meme set is reaching critical levels within a community, it can trigger operations to quarantine the area and send in an expert team of educators to execute an inoculative and preventative education program on the tactics of mind control and destructive cults.

Memetic Warfare

The principle of memetic warfare is to displace, or overwrite dangerous pathogenic memes with more benign memes. Once a critical level of saturation of the new meme set is achieved in the target population, undesirable human artifacts and behaviors such as weapon caches and IED attacks will disappear. Ideally the virus of the mind being targeted will be overwritten with a higher fidelity, fecundity, and longevity memeplex in order to assure long term sustainability. When this is not practical, it is still possible to displace a dangerous memeplex, by creating a more contagious benign meme utilizing certain packaging, replication, and propagation tricks.

The process of offensive memetic operations down range should be sanctioned via a memetic annex in the Theatre level operations order. This annex will clearly articulate the commander's intent for the end state of the process. For instance, in order to facilitate stability and support operations, the commander may direct memetic operations to support democracy. While democracy is not a perfect form of government, it is more stable and peaceful than other forms of government. With the objective established the next step is to break down the individual components of the memeplex of democracy that will have to be propagated within the target audience. The Organization of American States has sub-divided democracy into six essential elements:

- Freedom
- Human Rights
- Rule of Law
- Free Regular Elections
- Pluralistic Political System
- Separation of Powers

These components happen to be memeplexes in their own right, and if this was an actual operation, they would have to be further sub-divided into their respective memes. In the interest of simplicity (and brevity) this step will be overlooked. The process of memetic component definition is summarized in Figure 1.

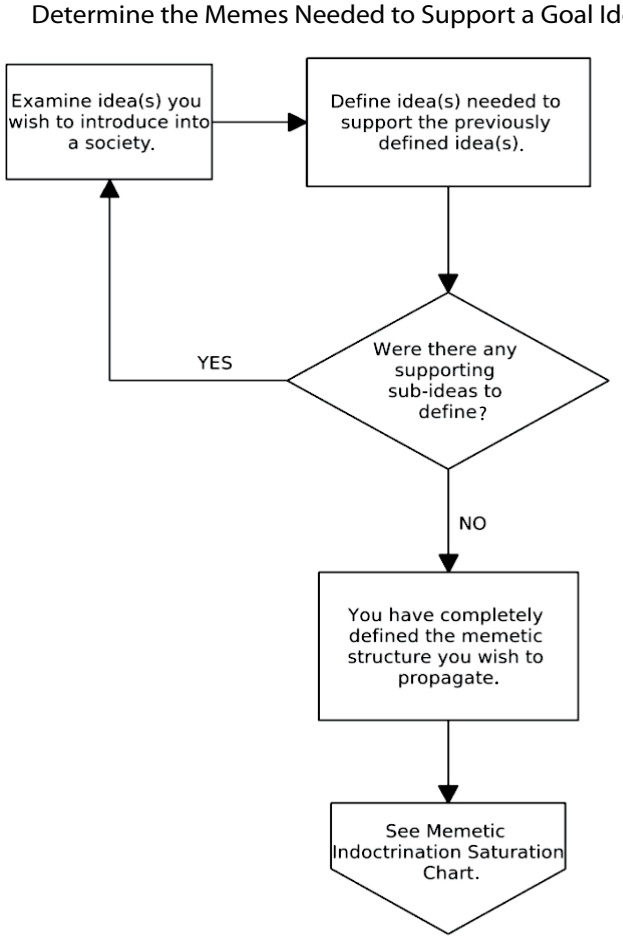


Figure 1. Memetic Component Definition.

With the specific memetic components defined, the next step is to incorporate packaging and replication tricks in order to make the message more attractive–and hence more likely to be passed on. Successful memetic packaging involves incorporating key elements that resonate with the human psyche, often on a very primitive level, within the context of the message. A list of primal and secondary human buttons can be found in Table 1.[12]

Table 1 Memetic packaging–primary and secondary behavioral hot buttons.

Primary Buttons	Secondary Buttons
• Anger	• Belonging
• Fear	• Distinguishing Yourself
• Hunger	• Caring
• Lust	• Approval
	• Obeying Authority

For example, when Richard Brodie wrote his book on memetics, he did not title it "Introduction to Memetics." He instead opted for the title "Virus of the Mind" because he knew that would tie into the human primal button of fear. Humans will go to great lengths to learn about and avoid perceived threats, and this fueled the sales of his book. While the primal and secondary buttons have universal appeal, there are differentiated male and female buttons, especially with regards to sexuality.[13] Judicious use of the buttons enumerated in Table 2 enables gender specific targeting of the memetic message.

Table 2 Memetic packaging–male buttons, female buttons, and repetition tricks.

Male Buttons	Female Buttons	Repetition Tricks
• Power	• Security	• Altruism
• Dominance	• Commitment	• Gifting
• Window of Opportunity	• Investment	• The Truth
		• Catchy
		• Mnemonics
		• Trojan Horse

Table 2 also lists a number of replication tricks which can further enhance the appeal of the message. Altruistic messages, for instance, are well received. Additionally altruistic individuals tend to have more friends and are held in higher regard, making it more likely that others will imitate them and spread their memes.[14] Gifting is a powerful technique as human beings are psychologically hard-wired to reciprocate when given something. The Hari Krishna cult took advantage of this by giving people a free flower, and in exchange people reciprocated by accepting their memes. The Trojan Horse technique is an insidious trick that involves proffering a very attractive meme such as sex, and having a less attractive meme such as beer sales ride on its coat tails. The target individual is effectively seduced into accepting the entire memetic package as a whole, including the less desirable elements.

Finally, there are a number of propagation techniques that can expedite the saturation of the target message. *Repetition* breeds familiarity, and when combined with *multiple media formats* appeals to a wide range of personality types. *Key leaders* can quickly influence their followers to accept a message; and gaining their endorsement should be an integral part of any propagation plan. Finally placing someone in a state of *cognitive dissonance* can open a window of opportunity for changing that individual's meme set. High pressure salesmen make extensive use of this technique.

When the memetic packaging, replication, and propagation strategy is complete, the next step is to begin the process of indoctrination of the target population in order to achieve the target level of message saturation. The initial focus should be on community leaders with influence networks. Through incorporation of a feedback loop, propagation measures are refined and continued until the desired end state has been achieved. This process is mapped in Figure 2.

Memetic operations in the military environment require the use of broad spectrum assets, both organic and inorganic. The central hub, or brain of the operation, is the intelligence staff. The theatre level commander's intent is filtered down through the Division Analysis and Control Element (ACE) to the Brigade S2 which is in charge of memetic construction, propagation oversight, and feedback analysis. Command level support will be required to coordinate non-organic assets such as the Air Force Commando Solo psychological operations platform, Cyber Warfare (CW), and Public Affairs (PAO).

High level support will also be required to synchronize and deconflict other aspects of state power which form additional propagation platforms such as non-governmental organizations (NGOs) and private volunteer organizations (PVOs) as well as the Office of the Secretary of State. The assets required

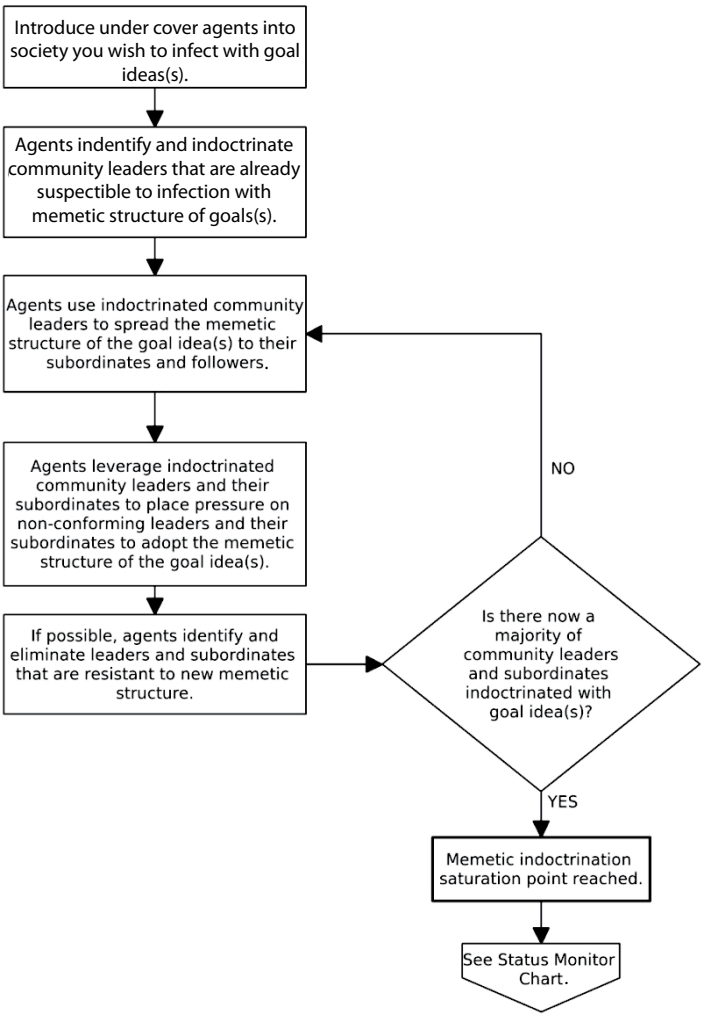


Figure 2. Memetic Indoctrination and Saturation Assessment.

to conduct brigade level memetic projection are summarized in Figure 3.

The same assets which are utilized to propagate the approved memetic message will also serve as

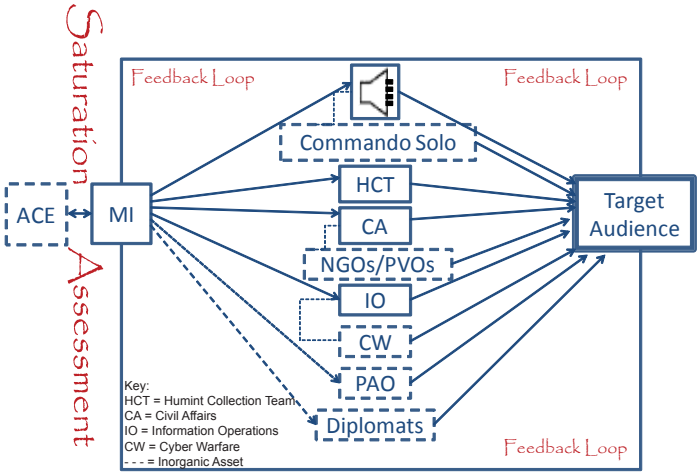


Figure 3. Brigade Level Memetic Propagation Model.

sensors within their specific areas of expertise to collect and channel feedback to the Military Intelligence (MI) control cell. The MI staff will make any necessary adjustments to the message to achieve the commander's intent, while mitigating second and third order effects, and then push the refined message through the appropriate propagation platforms once more.

Achieving the desired level of memetic saturation will result in the target population exhibiting the artifacts and behaviors that will support the ongoing coalition mission. It is important to note, that the memetic process does not end here. If a process of monitoring is not put in place to ensure that the memetic message maintains a critical mass, the target population may revert to previous undesirably artifacts and behaviors. For a relatively cheap ongoing investment, memetic monitoring can insure that unforeseen and/or emergent entities do not unravel the meme set and compromise future security. This critical process is detailed in Figure 4.

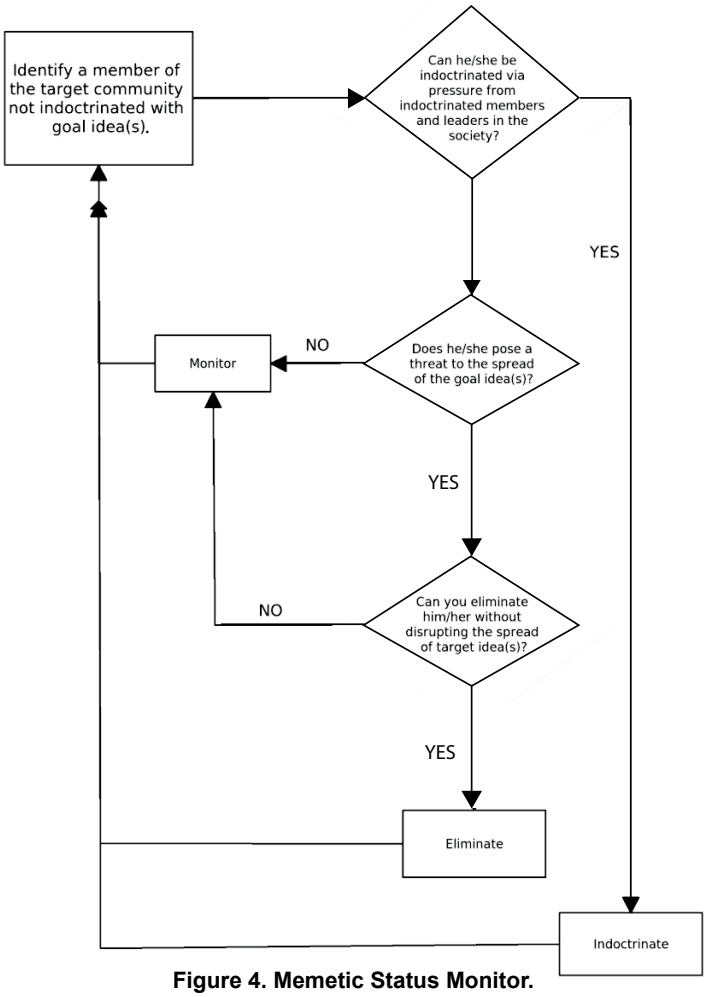


Figure 4. Memetic Status Monitor.

Conclusion–Implications of Memetics

Memetic theory provides a framework for dealing with the most troubling social and military problems at the root causal level. The relentless advance of technology will continue to make weapons of mass destruction (WMD) increasingly deadly, miniaturized, and available. Today memeoids are able to wreak considerable havoc by flying airliners into buildings or bombing key infrastructure. When these individuals are able to reliably obtain WMD, the survival of humanity will hinge on a preventative approach to terrorism and insurgency rather than a reactive response. Memetics provides the key to identifying, tracking, quarantining, and ultimately eradicating pathogenic memes before they result in deadly consequences. The IC is uniquely positioned to incorporate and exploit this new model to protect U.S. interests at home and abroad.

As society continues to become more competitive at every level, human beings are forced to evolve mentally and physically in order to be successful. These selection pressures will inevitably lead to genetic (and memetic) engineering. Future parents will do everything in their power to ensure that their progeny are able to successfully compete by supplying them with the best possible DNA and mental programming (memes). As high fidelity digital media technologies continue to proliferate, and with the expected debut of Artificial Intelligence capable of natural language recognition and common sense, the perfect tools to analyze, propagate, and engineer memes at the societal level will be within human reach.

While this raises profound moral implications, the reality is that this development is unavoidable. While the free thinking people of the U.S. may be loathe to utilize technologies which can be construed as mind control, its enemies have no such compunctions. It is vital to the interests of the U.S. and its people that memetic theory is fully explored, if for no other reason than to develop defenses against foreign memetic attack. Memetic operations do not require a presence in the target country. For a fraction of the cost of deploying troops on the ground, the enemies of the U.S. could conduct devastating memetic based information warfare against America. It is time for the IC to turn this threat into an opportunity. Memetics after all is only a tool, and tools when properly employed can be used to build peace, hope, prosperity, and a better way of life.

Endnotes

1. Frank G. Hoffman, "Neo-Classical Counterinsurgency?" *Parameters,* Summer 2007, 77.

2. Richard Brodie, *Virus of the Mind* (Seattle: Integral Press, 1996), Inside cover.

3. Susan Blackmore, *The Meme Machine* (New York: Oxford University Press, 1999), 6.

4. Ibid., 100.

5. Ibid., 59-62.

6. Ibid., 162.

7. Brodie, 57-64.

8. H. Keith Henson, "Evolutionary Psychology, Memes, and the Origin of War," *Kuro5hin*, 20 April 2006. 13.

9. H. Keith Henson, "Memetics and the Modular Mind," *Analog*. August 1987, 6.

10. H. Keith Henson, "Sex, Drugs, and Cults. An evolutionary psychology perspective on why and how cult memes get a drug-like hold on people, and what might be done to mitigate the effects," *The Human Nature Review*. Volume 2: August 23 2002, 343.

11. "John Walker and the fatal flaw in our war on terrorism!" *FACTNet Newsletter*, January 2002, 2-3.

12. Brodie, 90-93.

13. Brodie, 119-120.

14. Blackmore, 162-174.

1LT Brian Hancock was an Information Executive who joined the U.S. Army and completed basic training in 2006. He is the 2007 U.S. Army Reserve Soldier of the Year. He accepted a direct commission in October 2007. 1LT Hancock is currently the Executive Officer of the 7th Psychological Operations Group Headquarters Support Company.

Lethal Theory: Some Implications

by Claudia Baisini and James M. Nyce

Introduction

The conflicts in which our Armed Forces are engaged are increasingly characterized by large civilian presence and involvement, difficulties in identifying possible threats, high tempo, and dense terrain. The concept of the "three block war," introduced by General Krulak, reiterates the necessity of making a broad range of decisions in little or no time at the micro tactical level.[1] Far more complex than "shoot, don't shoot," the group leader has considerable responsibility in decisionmaking. In order for him to have the best possible situational awareness, he must have the necessary skills (not tools or rules). He must be provided with the capability of learning from the operational context, stretching his mental models and *transcending the obvious*.

Research suggests that visual orientation is an important ability for a group leader in urban combat; what one sees and how one interprets what is seen can be decisive. What has received less attention is the fact that the ability to make fast decisions in a critical situation depends also on the ability to make the right judgment of the situation; to perceive and understand context appropriately. Such ability requires sophisticated context-based training that gives the group leader the mindset to learn and understand the context appropriately while deployed.

This following discussion stems from a study conducted at the Swedish National Defense College in 2006 which focused on identifying the most relevant issues for conducting military operations in a built up area in a distributed operation.[2,3] In distributed operations a battalion's squads are generally autonomous and are spread throughout the operation area; thus, the squad leader has considerable decisionmaking power. The focus is on the squad leader's competence, judgment, and decisionmaking capabilities, which are highly dependent on his situational awareness. The study's premise was that a deeper understanding of the local culture is critical to the squad leader's reading of the operational situation due to the high density of civilian population in military operations in urban terrain.

The findings suggested the issue of *context* is the most relevant way to think about culture, with an emphasis on the visual dimension. In other words, to support the role of a unit's leader in populated settings–the three blocks, what he sees and reads in the social landscape turned out to be paramount. Furthermore, while it is possible to derive a generic system of values that reflect the structure of the local culture, it has to be kept in mind that countries such as Afghanistan are highly fragmented among diverse ethnic groups, tribes, and kinships. It is necessary to gain a deeper local understanding, one that cannot be easily extrapolated from more general statements about a culture. It is highly context-dependent.

U.S. Army and Marine Corps doctrines raise the issue of "learning" and, particularly, "learning while acting" as paramount in the complex counterinsurgency (COIN) operational environment. Both FM 3-07 Stability Operations and FM 3-24 Counterinsurgency also stress the "bottom up" nature of such operations. While orders come from above, it is only at the local tactical level that proper situational awareness can be achieved.[4]

If we look at the squad leader in a three block war environment, what is crucial to him is the context which culture, of course, informs. Whether he is leading his squad in patrolling (observation) or close quarter battle (CQB) or engaging against rebels or being ambushed, he needs to learn how to watch and interpret what he sees and he must refer to the *local context* (understand *what* he sees in relation to *where* he is) rather than interpreting it based on preconceived ideas or prior de-contextualized knowledge/information. Furthermore, he must do it fast,

which is why the visual dimension emerged as so critical. He must experience that *"Coup d'Oeil"* that was considered crucial by Napoleon and by many after him. He needs to develop that intuition that General Krulak considers the most important characteristic of young leaders. The question is: How?

Intuition and *Le Coup d'Oeil*

"The human mind's intuitive process is an irreplaceable determinant of combat success" [5]

According to Krulak, decisionmaking is a central human factor in warfare, the foremost means of lifting the "fog of war."[6] Usually, inexperienced leaders under extreme conditions wait until they have gained as much information as possible before making a decision, which leads to missed opportunities. "History has demonstrated that battles have been lost more often by a leader's failure to make a decision than by his making a poor one."[7] This is relevant in combat, but also to other aspects considered crucial in COIN operations, such as understanding and responding to local population(s).

Napoleon referred to the intuitive capability to rapidly assess a situation and make a fast decision as "C*oup d'Oeil*" or "strike of the eye" which he believed was a gift of nature.[8] In fact, behavioral psychologists have identified the creative-intuitive personality as being "alert, confident, foresighted, informal, spontaneous and independent. He is not afraid of his experiences, himself, or his world. He accepts challenges readily. He is unconventional, yet comfortable in this role. He can live with doubt and uncertainty. He is willing and able to create and is not afraid of exposing to criticism."[9]

Historically, militaries believed that although heredity and personality certainly play a role, intuition can be cultivated and developed. Prior to World War II the Japanese called it "sixth sense" and the Germans "character." They tried to identify this trait during recruitment and to cultivate it through stressful decisionmaking training under extreme conditions.[10]

Intuition has been defined as "*a developed mental faculty which involves the automatic retrieval and translation of subconsciously stored information into the conscious realm to make decisions and perform actions. Organized databases of knowledge gained through education–experiences, memorization, sensations and relationships–are the building blocks for intuitive thought.*"[11] From the many definitions of intuition three common traits can be identified:

- It is a phenomenon of subconscious thought.
- It relies heavily on experience-based knowledge.
- It is a comprehensive, unrestrained thought process.[12]

The traditional military decisionmaking process is mostly described as analytical and prescriptive. It is a systematic, methodical approach that breaks the situation down into manageable tasks. While such an approach is effective in long term planning, by its very nature it carries risks identified in the literature as "bounded rationality."[13] An alternate approach is the Intuitive (or Naturalistic) Theory of decisionmaking, based on the premise that people often use less formal, but much faster decisionmaking strategies in real time situations.[14]

When talking about military intuition many authors refer to Napoleon and his *Coup d'Oeil* or the instant, global understanding of a situation. This is particularly appropriate to the subject discussed here because it refers to what the eye seizes, both literally and metaphorically. It is the ability to see the whole and also to see what is not there, and act.

According to Klein, whose Recognition Primed Decision Model is a milestone in decisionmaking theory, the first source of power is intuition, which he defines as use of experience to recognize key patterns that indicate the dynamics of a situation.[15] This includes recognizing what is happening but also what *isn't* happening, as both can provide clues. This ability comes from experience, one is able to see the pieces of the event that are not perceptible to someone with less experience or expertise.[16]

Intuition as Socially Constructed

If we accept from Klein's definition of intuition as based on "experience to recognize key patterns that indicate the dynamic of a situation," a problem arises. If a Soldier has no experience of the local environment in which he is deployed, his intuition would be based on experiences, patterns and dynamics that generate from, and are applicable to, his own social context, but not necessarily applicable to the context in which he is deployed. Or even worse, they might be misleading when applied because the meaning is different. Such issues are the key to "understanding" and "learning" about the

operational environment. The way in which an individual sees the world is the product of the individual's personal history, experiences, upbringing, personality, and his social context. The interaction between the individual and the social context has the double effect of constructing how the individual sees the world (hence the way he acts) and, in turn, constructing his social context.[17] To put in Kurt Lewin's words behavior is a function of personality and context.[18]

The way we look at a situation defines (and limits) what approach we will have in relating to that particular situation. Everyday interaction tends to reconfirm and reinforce previous *habitus.* To illustrate how our intuition can mislead us when it comes to understanding a variety of local contexts—

This could be a main road to a rural community anywhere.

Now look at the next pictures.

These two images (below left and right), representing how a main road in Malawi looks, may seem unusual to most Westerners. What is unusual to us is that there is always someone walking aside the road, any time of the day or night. *Always*. If this is related and read through our Western experience, it would never be considered a main road. This is because according to what is normal for us on a main road there will be vehicular traffic and no pedestrians. We would suspect that something is wrong if we were driving on an interstate and saw many people walking along it.

Hence, if we found ourselves in Malawi and saw the road as illustrated in the first image, we would perceive the situation as normal. *The very fact that the road looks normal to us (no people) is the most relevant indicator for local people (or an intuitively skilled warfighter) that there is something wrong.*

Also, what may be seen as normal in Malawi may not be the case for a country road (Image 1) in Zimbabwe, a neighboring country to Malawi. This raises the question as to what extent we can generalize knowledge about local conditions. There is a tendency to either over generalize or over particularize knowledge especially when it comes to cultures other than own. This article will suggest a third, alternative path.

As Heuer[19] describes, we tend to see what we expect to see, but we would like to add that what we expect to see, what guides our attention, is a product of our social context.[20] Most attempts to take local context into account have taken the route of either learning basic content knowledge about others or attempting to memorize normative rules and principles that proscribe certain behavior. This approach to learning about local context has at least

two problems. One is whether the uptake of contextual knowledge in these forms balances out the economic costs. Second, and more importantly, can knowledge learned this way be readily and easily applied in tactical situations?[21] The temptation to rely on virtual simulations stems from the equation that close to reality experience and participation can result in a kind of direct "transmission" from what the simulation shows to what exists in an operational context itself. This finesses the question we address here of how to use one's intuition so that it is situationally appropriate and yields more directly understood tactical signals outside one's own country. To understand how this might occur takes us to the idea of visual cognition and cueing.

Contextual Cueing

The contextual cueing paradigm developed by Chun and Jiang states that "visual context can assist localization of individual objects via an implicit learning mechanism."[22] Several experiments have shown that invariant spatial context can cue the location of a target which happens unconsciously, leading to the conclusion that implicit memory of visual context can provide top-down guidance for attention and awareness. In other words, with repeated experience the visual system picks up on invariant spatial relationships and uses this information to guide attention, without the need for direct conscious intervention.[23, 24]

However, "objects can be recognized without context but when dealing with less familiar objects, complex scenes, or degraded information, the importance of context increases"[25] The same experiments have also demonstrated that there are constraints at work here–*"contextual cueing only occurs when the target was embedded within the predictive context."*[26] Visual context's function is that of guiding attention and facilitating recognition of objects within a scene; we are more likely to look for a breadbox than a drum when looking at the picture of a kitchen, which *guides* us to detect the breadbox much faster.[27]

Once again, it is worth mentioning that the predictive context is determined by what we are used to, what is obvious to us. A person who has grown up in a context where the laundry is done in the kitchen would more easily identify a clothes washer in the kitchen rather than a person whose laundry is done in the bathroom. In the latter case a clothes washer in the kitchen would not be part of this person's predictive context. Preconceived ideas, like what an interstate looks like, can bias not only how we make sense of what we see, but also what we actually see (and what we don't see or overlook.)

So how can warfighters both learn and respond to appropriate cultural cues? Further, how can we embed knowledge of this kind in such a format so that it can be available to them without the need for direct conscious intervention? Having to think rather than immediately react and respond appropriately as warfighters shift from context to context is what we are trying to address.

Change Blindness and Inattentional Blindness

Two other phenomena that relate to visual cognition and are highly relevant to our group leaders are change blindness and inattentional blindness. Change blindness, what Chun calls "the dark side of visual attention," is the failure to detect changes in the presence, identity or location of objects in scenes.[28] In experiments, over half of observers failed to note a change in the identity of a person that they were conversing with when changes (brief interruptions) occurred. The inattentional blindness phenomenon is closely related to this. Individuals failed to notice stimuli appearing in front of their eyes when they were preoccupied with an attention demanding task. In other words "*what you see is what you set.*"[29] Experiments demonstrated that people focused on observing players passing a ball to each other failed to notice a man in a gorilla costume who suddenly appeared on the scene. While inattentional blindness can be detectable often immediately, change blindness proved to be more difficult to detect even when the subject expects and actively searches for such changes.[30]

Research suggests that "our expectations and knowledge of a scene influence how we perceive objects associated with that scene. *Identification of objects is impaired when the given object is* ***incongruent*** *with the context of a paired scene.*"[31] The contextual cueing paradigm further shows how contextual information assists visual search and that implicit learning takes place, as observers during experiments learned which contexts were predictive and what markers were salient through implicit learning of repeated displays.[32] Finally, the change blindness paradigm refers to the difficulty of detect-

ing change, revealing that attention is crucial for the detection of change.

These results challenge traditional training and simulation paradigms that attempt to reproduce reality (the context) as perfectly as possible, to train the Soldier to a sort of automatic "internalized and reflexive response." We need to take these representations one step further. The role played by what the subject expects to see cannot be handled well in photorealistic simulations as presently implemented. These kinds of simulations do not help actors internalize the sort of reflex that guides quick response to certain stimuli. What is often crucial in operations in close interaction with civilian population is *to be able to see what we are not conditioned to see*. To achieve this, we need to move education, training, and simulation technology beyond a concern with detecting and reinforcing certain rules of behavior or by producing "better" reproductions of reality. The task should be to support staff capability to recognize what is salient in that reality, and to teach them to move beyond the paradigms of what is obvious to them in order to understand the context in which they are immersed, and act accordingly.

Transcending the Obvious: Lethal Theory

Eyal Weizman's Lethal Theory illustrates a way of thinking that *transcends the obvious*. In a 2002 operation in Nablus the IDF (Israel Defense Force) conducted a maneuver their commander described as "inverse geometry," the reorganization of the urban syntax by means of a series of micro-tactical actions."[33] By reinventing the way the topography of a whole town is regarded soldiers literally moved "through walls." They did not use any roads, streets, courtyards, etc. that constitute the logical, alleged common sense syntax of the city. They did not use windows or doors. Rather "they moved horizontally through walls and vertically through holes blasted in ceilings."[34] Walls are no longer barriers and streets are no longer ways through; all conventional geographic marks of a city were inverted or turned upside down. "Rather than submit to the authority of conventional spatial boundaries and logic, movement became constitutive of space. [...] The IDF strategy of "walking through walls" involved a conception of the city as not just the site, but the very *medium* of warfare–a flexible, almost liquid, medium that is forever contingent and in flux."[35]

The method was developed by necessity. Streets and alleys were often mined, entry points into buildings were watched or booby-trapped. An alternative to usual ways of exit and entrance had to be invented or discovered; this is where creative thinking came into the picture. Aviv Kokhavi, commander of the paratrooper brigade, had just returned from a leave during which he studied philosophy, social science, and architecture; subjects that influenced his way to envisage battle. As he explained:

> ***"This space that you look at, this room that you look at, is nothing but your interpretation of it. Now, you can stretch the boundaries of your interpretation, but not in an unlimited fashion, after all, it must be bound by physics, as it contains buildings and alleys. The question is how do you interpret the alley? Do you interpret the alley as a place, like every architect and town planner, to walk through, or do you interpret the alley as a place forbidden to walk through? This depends only on interpretation. We interpreted the alleys as places forbidden to walk through, and the door as a place forbidden to pass through, and the window as a place forbidden to look through, because a weapon awaits us in the alley, and a booby trap waits up behind the doors. This is because the enemy interprets space in a traditional, classical manner, and I do not want to obey this interpretation and fall into his traps. Not only do I not want to fall into his traps, I want to surprise him! This is the essence of war. I need to win. I need to emerge from an unexpected place. And this is what we tried to do."***[36]

Weizman's argument is that to become effective warfighters in urban contexts it is necessary to:

1. Realize what common sense representations are.
2. Use high order social theory to destabilize the "taken for granted" order of things.
3. Use the same theoretical set to identify strategic advantage.

In other words, the capability to visualize opportunities that otherwise would be masked by common sense. What is relevant is not so much that the end result is that the topography of an urban setting is exploited (that of course is the endpoint of any doctrine and strategy.) Rather it is to *deconstruct the natural order of things* as one's opponent understands it *and from this deconstruction gain operational advantage*. What Weizman does not discuss in detail is how this might be taught to frontline warfighters. It appears that he assumes that an adequate grasp of

the theoretical models he argues can immediately be translated into operational knowledge of this kind.

Charles Jennings (Chief of the Clinical Psychology function, School of Aerospace Medicine, Brooks Air Force Base) long ago spoke of the need for pilots to learn "*to transcend the obvious.*"[37] According to him "pilots are taught appropriate responses to problems that can be reasonably forecasted. However, these responses can become fixations. Pilots need to develop untested theories quickly, to enable them to "rise above the obvious," since many times they will encounter entirely unexpected challenges in flight to which there are no obvious solutions."[38] This kind of thinking applies as well to modern military operations, especially dispersed units operating in CQB or patrolling.

Learning Contextual Intuition

As we illustrated, intuition and perception are driven and informed by the predictive context which, in turn, is socially constructed. So, how do we manage to educate and train young leaders who can apply their intuition to a context other than their socially constructed one? We suggest an education and training method focused on:

1. Increased awareness of one's own framing. The way we see the world is a part of us, it is not something that can be taken off or put on as a pair of glasses. Increasing awareness of what such framing is made of, and in what way it guides our perception of the world, helps us recognize when we are interpreting other contexts according to frames we habitually use.
2. Exercises and drills based on experiential learning principles. Problem Based Learning (PBL) is aimed at *unfreezing* the dominant framing and developing the competences and skills necessary to learn from the context by engaging with it, and by exploiting our framing to detect relevant elements through "opposition."[39] In other words, this phase aims at teaching how to exploit differences in order to learn what the relevant categories and dynamics are at play in the operational context.
3. Exercises and drills based on Situated Learning. This will foster a mindset that *transcends the obvious* and enables warfighters to perform such cognitive and perceptual labor intuitively, automatically, and without much direct cognitive overhead.[40]

Problem Based Learning

PBL was developed for use in medical schools during the 1960s to help medical students learn to solve problems by *transcending the obvious*. Traditional basic knowledge is not taught through PBL, it is assumed to be already embedded in the curriculum. This method is based on presenting small groups of students with vaguely formulated sets of problems (real clinical cases). Critical to the method is *the formulation* of the problem and the acknowledgement that the students' prior formal knowledge is in itself insufficient for them to understand the problem in depth. Therefore they must train themselves to break down the problem in its components as well as look at it from all possible angles and then decide what additional information they need in order to solve it. *The method is about refocusing the learning around a scenario or trigger rather than upon the curriculum content itself.*[41] The students usually work in groups in order to *engage* with a particular scenario.

This method fosters:

- The ability to evaluate a situation, see what is wrong, and make decisions about appropriate actions based on the particular context.
- The acquisition, retention, and use of a variety of types of knowledge.
- Transfer. The ability to see similarities in apparently very different situations by "reading between the lines."
- Enhancement of *self-directed learning.* The individual acquires the capability to search for additional information appropriately.
- The development of inquiry skills and creativity. *There is strong evidence that heroes are in reality not so much rash brave beings rather highly creative men who perceive more than their comrades."*[42]
- Group cohesion and working towards a common goal. [43]

Traditional simulations might profit by embedding PBL, it would be useful as a design strategy because it is a method that does not look at the "learners" as empty jars that need to be filled with knowledge or information. On the contrary, it forces them to take charge of the problem at hand, think critically, creatively, and challenge their assumptions striving to *"transcend the obvious."*

Experiential and Situated Learning

Lave, contrasting with most traditional classroom learning activities that involve abstract, but not necessarily contextualized knowledge argues that learning is situated, *learning is embedded within activity, context, and culture.*[44] Knowledge needs to be presented in authentic contexts–settings and situations that would normally involve that knowledge.

Not only should it be presented in authentic contexts, we would argue, but the method should also combine such contextualization with active participation. Kolb developed the concept of Experiential Learning from the work of Kurt Lewin. According to Lewin little substantial learning takes place without the involvement of some or all of the following dimensions:

- Watching.
- Thinking.
- Feeling.
- Doing.[45]

Without engaging such dimensions we remain not much more than passive recipients and passive learning alone does not engage our higher brain functions or stimulate our senses to the point where we incorporate the lessons into our existing schemes.[46] We must put our knowledge into action.

Conclusion

Well designed education and training that aims at developing the necessary competencies and skills to learn about a new context (while engaging with it) is what is needed to prepare our Soldiers to meet the challenges of the complex operational enviroment. Such education would be one that forces them to take charge of the problem at hand, break it down, turn it, look at it from all angles, and decide what more information they need to make a decision about what to do next. This is what simulation technology might profitably be used for–to allow the staff to learn how to literally look through a building, break it down in pieces, turn it, rotate it, and consider a variety of options–some intuitive, some not so obvious.

It is not the simulator that should do this for them; nor is it necessary in order to achieve this kind of competence to reproduce a populated "village" for them. Rather the task here is to help them to play with what we think reality is, and go beyond it, in other words to *transcend the obvious*. In order to stimulate the development of more creative ways of thinking, one has to be less bound by what is perceived as obvious or passively learned such asas "typical behavior of the local culture," to being more receptive, agile, and prone to catch reality in its whole and its details: *le Coup d'Oeil.*

Endnotes

1. General Charles C. Krulak, "Cultivating Intuitive Decision Making," *Marine Corps Gazette,* May, 1999. Accessed at http://www.au.af.mil/au/awc/awcgate/usmc/cultivating_intuitive_d-m.htm

2, 3. Claudia Baisini and James M. Nyce, *"Mapping Culture (MAC),"* Concept Study Final Report, Swedish National Defense College, January 2007.

4. FM 3-24/USMC 3-33.5 Counterinsurgency, December 2006 and FM 3-07 Stability Operations, October 2008.

5. Major Brian R. Reinwald, "Tactical Intuition," *Military Review*, September-October 2000, 88.

6. Krulak.

7. Ibid.

8. Ibid.

9. Colonel James E. Mrazek, "Intuition: An Instantaneous Backup System?"*Air University Review*, January-February 1972. Accessed at http://www.airpower.au.af.mil/airchronicles/aureview/1972/jan-feb/mrazek.html.

10. Krulak.

11. Reinwald, 86.

12. Ibid., 80.

13. Lieutenant Colonel Kelly A. Wolgast, *"Command Decision Making: Experience Counts,"* USAWC Strategy Research Project, Carlisle Barracks, 2005, 2. Accessed at http://www.au.af.mil/au/awc/awcgate/army-usawc/cmd-decis-mkg.pdf.

14. David J. Bryant, PhD, Robert D.G. Webb, PhD, and Carol McCann, "Synthesizing Two Approaches to Decision-making in Command and Control," *Canadian Military Journal*, Spring 2003. Accessed at http://www.journal.forces.gc.ca/vo4/no1/command-ordre-01-eng.asp.

15. Gary A. Klein, *Sources of Power: How People Make Decisions* (Cambridge: MIT Press, 1998).

16. Wolgast, 7.

17. Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (Garden City: Anchor Books, 1966).

18. Kurt Lewin, *"Field Theory in Social Science: Selected Theoretical Papers,"* D. Cartwright, ed. (New York: Harper and Row, 1951).

19. Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Hauppauge: Nova Science Publishers Inc., 2006).

20. Social context that is generated by interactions among people, but also among people and things. For more about this see John Law and John Hassard, *"Actor Network Theory and After,"* Sociological Review Monographs (Oxford: Wiley-Blackwell, 1999).

21. And do we really believe that we can reproduce reality in all its facets and nuances?

22. Marvin M. Chun and Ingrid R. Olson, "Perceptual Constraints on Implicit Learning of Spatial Context," *Visual Cognition* 9 (3) (2002): 273-302.

23. Justin A. Junge, Brian J. Scholl, and Marvin M. Chun, "How is Spatial Context Learning Integrated over Signal Versus Noise? A Primacy Effect in Contextual Cueing," *Visual Cognition* 15 (1) (2007): 1-11.

24. Marvin M. Chun, "Scene Perception and Memory." Accessed at http://camplab.psych.yale.edu/articles/Chun_03PLM.pdf.

25. Ullman in Chun and Olson, "Perceptual Constraints on Implicit Learning of Spatial Context," *Visual Cognition* 9 (3) (2002): 273.

26. Ibid., 284.

27. Marvin M. Chun, "Contextual Cueing of Visual Attention," *Trends in Cognitive Sciences* 4 (5) (May 2000):170-177.

28. Marvin M. Chun and Rene Marois, "The Dark Side of Visual Attention," *Current Opinion in Neurobiology* 12 (2002), 184-189.

29. Steven B. Most, Brian J. Scholl, Erin R. Clifford, and Daniel J. Simons, "What you See is What You Set: Sustained Inattentional Blindness and the Capture of Awareness," *Psychological Review* 112 (1) (2005): 217-242.

30. Chun and Marois, "The Dark Side of Visual Attention."

31. Todd A. Kelley, Marvin M. Chun, and Kao-Ping Chua, "Effects of Scene Inversion on Change Detection of Targets Matched for Visual Salience," *Journal of Vision* 2 (2003), 1.

32. Ibid., 1-5.

33. Eyal Weizman, *Hollow Land: Israel's Architecture of Occupation* (London: Verso, 2007), 53.

34. Ibid.

35. Ibid.

36. Brigadier General Aviv Kokhavi in Eyal Weizman "Hollow Land: Israel's Architecture of Occupation" (London: Verso, 2007), 55-56.

37. Mrazek, 6.

38. Ibid.

49. Lewin.

40. As an example, for a micro-tactical exercise squad leaders might be given an operational task in a built up area that they must perform using a glass model (Glass-Box™) of the built up area. This model represents all the structural elements of small, multi-level Middle East urban area, is transparent on all sides, and can be assembled and reassembled (deconstructed) in many different ways. It is designed to support both visualization and decomposition of what both the problem and a solution might look like. The Glass-Box™ design also adds the very important tactile dimension to the drill. Soldiers could use the model, possibly divided into two competing teams, to find situationally appropriate solutions to the task, since an obvious common sense solution, (such as going through doors and windows) is forbidden by the exercise's rules. What Glass-Box™ methods and exercises are designed to support is the kind of intuitive, reflexive operational context specific awareness we have discussed and argued for here.

41. Andrew Roberts, "Problem Based Learning and the Design Studio," *CEBE Transactions* 1 (2) (December 2004).

42. Mrazek.

43. Geoffrey R. Norman and Henk G. Schmidt, "The Psychological Basis of Problem-based Learning: A Review of the Evidence," *Academic Medicine* 67 (9) (September 1992).

44. Jean Lave, *Cognition in Practice: Mind, Mathematics, and Culture in Everyday Life* (New York: Cambridge University Press, 1998).

45. David A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development* (Englewood Cliffs: Prentice Hall Inc., 1984).

46. Ibid.

Claudia Baisini, M.Sc. attended the University of Milan, and Aberdeen King's College completing studies in Organizational Studies, Cross Cultural Strategy, International Business, and Organizational Change and Learning. Following a term at Copenhagen Business School in Cross Cultural Marketing Strategy she took her M.Sc. in International Management at the Graduated Business School of the University of Gothenburg, Sweden. Her Master's Thesis was on "Knowledge in Knowledge Intensive Organizations: The Case of Crime Investigation and Consulting Firms." She joined the staff of the Swedish National Defense College in Stockholm 2004 where she participated in such projects as Planning under Time and Pressure in COIN (PUT) and squad leader Situational Awareness in MOUT. Her current focus is on the development of a method to understand the mindset of relevant actors in the area of operations, based on how our biases and categorizations influence our own understanding. She is also researching the development of education, training, and methods to enhance observation skills and foster meta-cognition and re-framing. The project is conducted in cooperation with the FBI Academy (Behavioral Science Unit, Terrorism Research and Analysis Project) and USJFCOM J9 within the framework of MNE6. Ms. Baisini is a PhD candidate in Neuroscience at Karolinska Institute, Stockholm Brain Institute. Her doctoral project combines her previous knowledge in Organizational Theories with Neuroscience in research on neurological implications of learning creativity (divergent thinking), re-framing and plasticity. She is an adjunct lecturer of Anthropology at Ball State University and may be reached at Claudia.baisini@fhs.se.

James M. Nyce, PhD is an associate professor in the Department of Anthropology, Ball State University. He is a visiting professor in military technology and war science at the National Defense College, Stockholm, Sweden from 1998 through 2000 and 2005 to the present. Since 2005, he has been scientific advisor to a research project that has focused on the military intelligence function, organizational/ technological change and professional development. He is also visiting professor in Lund University's Master's Program in Human Factors.

The Military Intelligence Corps 2010 Hall of Fame Inductees

Colonel Daniel Baker (U.S. Army, Retired)

Colonel Daniel Baker enlisted in the U.S. Army in 1970 and later commissioned in 1976 as a Second Lieutenant, Military Intelligence (MI), completing the MI Officer Basic Course at Fort Huachuca, Arizona. His first assignment as a 2LT was serving as the Deputy Officer in Charge (OIC), Detachment I, 201st Army Security Agency (ASA) Company, Wurzburg and then Detachment M, Stuttgart, Germany. He later moved to Augsburg and assumed duties as the Operations Officer of the 201st ASA Company. In February of 1981, Captain Baker returned to Fort Huachuca where he assumed duties as the Branch Chief/ Senior Instructor of the Advanced Individual Training Company, U.S. Army Intelligence Center. He was also the Commanding General's Aide-de Camp and Commander, Delta Company, 2nd Battalion, 1st School Brigade. It is here that he revitalized training and incorporated students in the Officer Basic Course as junior leaders.

In January 1985, he headed to Turkey where he would serve as the OIC of Space Operations (Hippodrome), Field Station Sinop, until January 1986. In February 1986, CPT Baker was assigned to the Pentagon as both Staff Action Officer and the Staff Action Control Officer. In June 1989, Major Baker returned to Germany as the Intelligence Officer to the 2nd Armored Calvary Regiment, Nurnburg Germany. In June 1990, he took command of 502nd MI Company and conducted intelligence operations in support of Operation Desert Storm. In November 1991, he assumed the duties of the Deputy Regimental Executive Officer, 2nd Armored Cavalry Regiment.

After three years in Germany, Lieutenant Colonel Baker took command of the 124th MI Battalion, 24th Infantry Division (Mech), Fort Stewart, Georgia. As Commander, he built and tested the first Analysis and Control Element in the Army. He pioneered this new MI concept and developed the tactics, techniques, and procedures that became the basis for subsequent Army doctrine.

He left command in June 1994 to attend the National War College at Fort McNair, Washington, D.C. LTC Baker returned to the Pentagon where he held the position of Intelligence Coordination Officer (Europe), J2 Joint Staff/Defense Intelligence Agency for two months before transitioning to the J2's Executive Officer. Fifteen months later he filled the role of J2 Special Assistant for seven months followed directly by the position of the Assistant J2.

In June 1998, Colonel Baker assumed command of the 513th MI Brigade, U.S. Army Intelligence and Security Command, Fort Gordon, Georgia. There he introduced new enduring operational constructs and capabilities, including the Army's first operations level Measurement and Signature Intelligence Exploitation. In July 2000, he became the Assistant Chief of Staff for Intelligence (G2),

3rd U.S. Army/Army Forces Central Command at Fort McPherson, Georgia.

His final assignment was as the Deputy Chief of Staff for Intelligence, Coalition/Joint Forces Land Component Command at Camp Doha, Kuwait for eight months. In December 2002, he retired from active duty after having served honorably for 32 years. He continued his intelligence career as a member of the Deputy Chief of Staff for Intelligence, G2.

COL Baker's civilian education includes a BS in Business Administration from Northwestern University, an MA in Management from Webster University, and an MS in National Security from the National Defense University. His military education includes the Defense Language Institute (Russian); MI Officer Basic and Advanced Courses; the Basic Electronic Warfare/Cryptologic Officer Course; the Combined Arms and Services Staff Course; the Command General Staff College, and the National War College.

COL Baker's awards and badges include the Distinguished Service Medal; Defense Superior Service Medal; Legion of Merit; Bronze Star Medal; Defense Meritorious Service Medal (8 OLCs); Army Commendation Medal; Army Achievement Medal; Joint Meritorious Unit Award (1 OLC); Valorous Unit Award; Army Good Conduct Medal; National Defense Service Medal (2 Bronze Service Stars); Armed Forces Expeditionary Medal; Southwest Asia Service Medal (3 Bronze Service Stars); Armed Forces Reserve Medal; Noncommissioned Officer's Professional Development Ribbon; Army Service Ribbon; Overseas Service Ribbon (4th Award); Kuwait Liberation Medal (SA); Kuwait Liberation medal (KU); Global War on Terrorism Service Medal; Global War on Terrorism Expeditionary Medal; Joint Chiefs of Staff Identification Badge, and Army Staff Identification Badge.

Command Sergeant Major Scott Chunn (U.S. Army, Retired)

Command Sergeant Major Scott Chunn enlisted in April 1971 and reported to Airborne Sensor Specialist Course at Fort Huachuca, Arizona. His first assignment was as a Specialist (SP5) serving in an Aerial Surveillance and Target Acquisition Platoon at Fort Wainwright, Alaska. In 1974 he was assigned as a Senior Data Terminal Operator, 9th MI Company, Fort Lewis, Washington, but due to lack

of equipment, he served as a Counterintelligence Coordinator. After two and an half years, SP5 Chunn assumed duties as an Aerial Sensor Specialist for the 73rd Combat Intelligence Company, Stuttgart, Germany.

In 1980, he left Germany and returned to Fort Huachuca where Staff Sergeant Chunn served as an Instructor, and later a Senior Instructor, for Bravo Company, 2d Battalion, 1st School Brigade. During his time as an Instructor, SSG Chunn was twice honored as Instructor of the Quarter. He also served as the First Sergeant for MI Officer Basic Course and as a project NCO for the New Systems Training Office.

In 1984, after four years at Fort Huachuca, Sergeant First Class Chunn returned to Germany and was assigned as the Battalion Operations Sergeant for the 1st MI Battalion, Wiesbaden. In July 1985, he became the 1SG for Alpha Company, 1st MI Battalion. In 1987, Master Sergeant Chunn was assigned to the 7th Infantry Division (Light), Fort Ord, California with duty as the Intelligence (G2) Operations Sergeant. In January 1988, MSG Chunn served as the G2 Sergeant Major for the 107th MI battalion. In 1989, he was selected for the U.S. Army Sergeants Major Course.

Upon graduating in January 1990, MSG Chunn was assigned as the I Corps Tactical Operations Center Support Element Sergeant Major at Fort Lewis. In March 1990, he deployed in support of Team Spirit, Republic of Korea, and while deployed was notified of his selection to Sergeant Major and appointment to Command Sergeant Major. Once he returned to Fort Lewis, he assumed duties as the CSM, 109th MI Battalion. After the inactivation of 109th in May 1991, CSM Chunn was assigned as the CSM of the 14th MI Battalion, 201st MI Brigade. He subsequently served as the Brigade CSM for the 201st MI Brigade before moving to the 524th MI Battalion, 501st MI Brigade in 1993. In March 1995, CSM Chunn assumed duties as the CSM of the 748th MI Battalion in San Antonio, Texas. After ten months, he was reassigned to Fort Meade, Maryland to serve as the CSM of the 704th MI Brigade from 1996 to 1998.

CSM Chunn's final assignment was as the CSM of the U.S. Army Intelligence School and Fort Huachuca. In this post, he initiated the Enlisted Assignment Council and a local chapter of the Sergeant Audie Murphy Club. He also established the Doctor Mary Walker Award Program, recognizing outstanding service for volunteers as well as the CSM (Retired) Doug Russell Award Program, recognizing junior MI enlisted soldiers. In January 2001, CSM Chunn retired from active duty after serving honorably for 30 years.

CSM Chunn's civilian education includes a BA in Liberal Arts from the University of the State of New York and an MA in Management from the University of Phoenix. His military education includes the Airborne Sensor Specialist Course; the Basic Leadership Course; the Advanced Noncommissioned Officer's Course; the Criminal Investigation Course; the Instructor System Development Course; and the Sergeants Major Academy.

His military awards and badges include the Distinguished Service Medal; the Meritorious Service Medal (7 OLCs); the Army Commendation Medal (3 OLCs); the Army Achievement Medal; the Good Conduct Medal (10th award); the Air Force Outstanding Unit Award; the Joint Meritorious Unit Award; the Army Service ribbon; the Overseas Service Ribbon; the Noncommissioned Officer Professional Development Ribbon; the National Defense Service Medal, and the Senior Aircraft Crewmember Badge.

Brigadier General Richard T. Ellis (U.S. Army, Deceased)

Brigadier General Richard T. Ellis was commissioned as a Second Lieutenant, Military Intelligence (MI) in 1978 and reported to MI Officer Basic Course at Fort Huachuca. His first assignment was serving as the Foreign Area Officer and later Intelligence Contingency Fund Class A Agent, 500th MI Group, Camp Zama, Japan. In August 1980, First Lieutenant Ellis became the Administration Officer of the 149th Military Detachment, 500th MI Group. In August 1981, he was assigned to the 500th MI Group as the Assistant Operations Officer/Team Chief of the Foreign Liaison Detachment.

Upon his return to the U.S. in 1982, 1LT Ellis attended the MI Officer Advanced Course at Fort Huachuca. In March 1983, after his promotion to Captain, he headed to Fort Bragg, North Carolina, where he assumed duties as the Counterintelligence (CI) Team Chief and later the Intelligence Officer of 1st Battalion, 7th Special Forces Group (Airborne), Joint Task Force-11, Honduras. After approximately two years, CPT Ellis became the Chief of Combined Security Element and Assistant Intelligence Officer of the 1st Special Forces Operational Detachment-Delta

(Airborne) at Fort Bragg. In January 1989, he took command of Charlie Company, 313th MI Battalion (Airborne), 82nd Airborne Division. From there he deployed to Panama to participate in Operation Just Cause. In January 1990, he took command of his second company, Area Operations Element, 1st Special Forces Operational Detachment-Delta (Airborne).

In August 1992 Major Ellis commanded Detachment K, U.S. Army Foreign Intelligence Activity, Korea and in December 1993 he took command of Detachment B, U.S. Army Foreign Intelligence Activity, Fort Meade, Maryland. After over two years of command, he became the Senior Instructor of the Special Training Center at the Defense Intelligence Agency, Washington, D.C. Less than three years later in 1997, Lieutenant Colonel Ellis again took a command position, this time as commander of the 319th MI Battalion, 525th MI Brigade, XVIII Airborne Corps, Fort Bragg.

In July 1999, LTC Ellis returned to Washington, D.C. to serve as the Director of Intelligence, Office of Military Support. During his year there he served as the Intelligence Officer (J2), U.S. Intelligence Cell, U.S. European Command, Supreme Allied Commander, Europe and for the Commander, Stabilization Force, Operation JOINT FORGE, Bosnia. Once LTC Ellis returned from deployment he attended the National War College, Fort McNair, Washington, D.C. After completion of the National War College, Colonel Ellis took his seventh command position, this time with the 650th MI Group (CI), U.S. Army Europe, SHAPE, Belgium.

In June 2004, COL Ellis returned to Fort Bragg to serve as the Assistant Chief of Staff for Intelligence, G2, XVIII Airborne Corps, and deployed as the J2, Multi-National Corps-Iraq. In August 2006, he became the Director of Intelligence, J2, U.S. Southern Command, Miami, Florida. As the J2, he led efforts to transform and improve the Human Intelligence (HUMINT) capabilities of our nation into a more relevant and integrated community in the fight on terrorism.

Brigadier General Ellis served at the National Counterterrorism Center for nearly a year before moving on to his final assignment. BG Ellis' final assignment was as Deputy Director, National Clandestine Service for Community HUMINT, Central Intelligence Agency, Washington, D.C. On 4 May 2009, BG Richard Ellis tragically died while on active duty, having served honorably for 31 years.

His civilian education included a BA in Criminal Justice and Political Science from the University of Nevada and an MS in National Security and Strategic Studies from the National War College. BG Ellis' military education included the Ranger Course; MI Officer Basic and Advanced Courses; Personnel Management Staff Officer Course; Military Operations Training Course; Special Forces Qualification Course; Combined Arms and Services Staff Course; Jumpmaster Course; the Command General Staff College, and the National War College.

BG Ellis' awards and badges include the Defense Superior Service Medal; the Legion of Merit; the Bronze Star Medal; the Defense Meritorious Service Medal (3 OLCs); the Meritorious Service Medal (2 OLCs); the Joint Service Commendation Medal (1 OLC); the Army Commendation Medal (2 OLCs); the Joint Service Achievement Medal; the Army Achievement Medal; the Armed Forces Expeditionary Medal (2 Bronze Service Stars); the Bronze Assault Arrowhead, and the NATO Medal. His badges included the Special Forces Tab; the Ranger Tab; Master Parachutist Badge (Combat Star), and the Honduran Parachute Badge. He was posthumously awarded the Distinguished Service Medal, and the National Intelligence Distinguished Service Medal, and the Distinguished Intelligence Medal.

Major General Barbara G. Fast (U.S. Army, Retired)

Major General Barbara G. Fast was one of the last members of the Women's Army Corps when she received her direct commission in January 1976 as a Second Lieutenant. She subsequently attended the MI Officer Basic Course and Tactical Surveillance Course at Fort Huachuca, Arizona. Her first assignment was as the Assistant Operations Officer for Training and Education, 66th MI Group, Munich, Germany. Soon thereafter she served as the Officer in Charge, Soviet Orientation Team, 5th MI Company. Before returning to the U.S., Captain Fast held positions as the Assistant S3 (Operations), 18th MI Battalion, as well as the Commander of the Headquarters, Headquarters Company, 18th MI Battalion, Munich, Germany.

In February 1982, CPT Fast reported to Fort Hood, Texas where she would serve as the Chief of

Intelligence Production Section, then Adjutant in the 303rd MI Battalion. In June 1983, she was selected over numerous combat arms nominees to become the first female Aide-de-Camp to the Deputy Commanding General, III Corps. In 1984, CPT Fast headed to Alexandria, Virginia where she served first as the MI Professional Development Officer, then as the Captain's Assignment Officer, MI Branch, and finally as the Special Operations Assignment Officer at the U.S. Army Military Personnel Center.

In July 1987, Major Fast was assigned as the Chief of the Advanced Systems Section, J2, U.S. European Command at Stuttgart, Germany. After two years, MAJ Fast became the Executive Officer of the 18th MI Battalion, Munich, Germany. While assigned to Munich she also served as Deputy, and then later, as the Chief of the Intelligence Division, 66th MI Brigade. In 1992, Lieutenant Colonel Fast assumed command of the 163rd MI Battalion, Fort Hood, Texas. Following command, LTC Fast became the first ever female Division G2, 2nd Armored Division at Fort Hood, Texas. In 1996, Colonel Fast took on a third command, this time the 66th MI Group (Provisional) in Augsburg, Germany. Returning to the U.S., Brigadier General Fast embarked upon a new position as the Associate Deputy Director for Operations/Deputy Chief, Central Security Service, then as the first S1, Signals Intelligence Directorate, National Security Agency at Fort Meade, Maryland.

In 2001, BG Fast assumed duties as the Director of Intelligence, J2, U.S. European Command in Stuttgart, Germany where she served with distinction for two years. Following her time in Germany, BG Fast returned to Fort Huachuca where she had begun her career 25 years earlier. There she served as the Assistant Commandant of the U.S. Army Intelligence Center and Fort Huachuca. While in this position she deployed to Iraq to become the first Director of Intelligence (C2) for Combined Joint Task Force-7, then Multi-National Forces-Iraq, Operation Iraqi Freedom. Upon returning from Iraq, Major General Fast served as the Senior Intelligence Officer before assuming command of the U.S. Army Intelligence Center and Fort Huachuca where she served as the Commanding General for over two years.

MG Fast's final assignment was the Deputy Director of the Army Capability Integration Center and G9 at the U.S. Training and Doctrine Command, Fort Monroe, Virginia. In July 2008, MG Fast retired from active duty in the U.S. Army after having served honorably for over 32 years.

She is a graduate of the MI Officer Basic and Advanced Courses; Intelligence Staff Officer Course; Tactical Surveillance Officer Course; Defense Sensor Interpretation and Application Training Course; the Armed Forces Staff College, and the U.S. Army War College. She holds BS in Education degrees in German and Spanish from the University of Missouri, an MS in Business Administration from Boston University, and an Honorary Doctorate of Laws from Central Missouri State University.

MG Fast's awards and badges include the Defense Superior Service Medal (1 OLC); the Legion of Merit; the Bronze Star Medal; the Defense Meritorious Service Medal; the Meritorious Service Medal (4 OLCs); the Joint Service Commendation Medal; the Army Commendation Medal; the Army Achievement Medal (1 OLC); the National Defense Service Medal with one Bronze Service Star; the Global War on Terrorism Expeditionary Medal; the Army Service Ribbon; the Overseas Service Ribbon; the Joint Meritorious Unit Award; the Meritorious Unit Commendation, and the Army Superior Unit Award.

Colonel John Lansdale, Jr. (U.S. Army, Deceased)

Colonel John Lansdale was commissioned as an Artillery Second Lieutenant in 1933 while serving as a member of the Army Reserves. After commissioning, 2LT Lansdale attended Harvard Law School and was later promoted to First Lieutenant in 1937. In May 1941, 1LT Lansdale received a letter from former roommate and future secretary to the Joint Chiefs of Staff, Frank McCarthy. McCarthy warned of the upcoming war and suggested he request a call to active duty serving in the Military Intelligence Division of the War Department General Staff. On 10 June 1941 1LT Lansdale reported for active duty to the Investigation Branch of the Office of the Assistant Chief of Staff, G2, War Department General Staff.

In February 1942, Captain Lansdale reported to Dr. James B. Conant who was, at the time, president of Harvard University and Chairman of the National Defense Research Committee. It was at this assignment that he learned of the efforts being made in a race to develop the atomic bomb. He was charged with safegurading the intelligence behind these efforts at the Radiation Laboratory at the University of California, Berkeley, California. In September of the same year General Leslie Groves recruited CPT Lansdale to aid in the atomic bomb project renamed the Manhattan Project now under the responsibility of the U.S. Army. He was charged with the mission of establishing a branch of military intelligence personnel. The Counter Intelligence Corps (CIC), or the "Silent Warriors," was charged with maintaining the secrecy and security of the Manhattan Project, under the support of the U.S. Army Corps of Engineers, Manhattan District. Lieutenant Colonel Lansdale's official title became Director of Intelligence and Security, Manhattan Project.

During his time as Director, Colonel Lansdale completed several other missions vital to the project's success. In June and July of 1945, COL Lansdale headed a small mission to Brazil aimed at negotiating the purchase of monazite sands. He led a subsequent mission to London and Sweden in order to obtain kolm deposits, a substance reportedly rich in uranium. COL Lansdale would also lead the Alsos Mission, which actively participated in the recovery of uranium ore in Germany and the capture of several prominent German scientists. By January 1946 approximately 325 CIC personnel still remained in the Manhattan Project Security and Intelligence Group commanded by COL Lansdale. His post-war duties included the establishment of a London based liaison office with British Intelligence, before returning to his civilian career as a lawyer at Squire, Sanders, and Dempsey, LLP in Cleveland, Ohio.

In the mid-fifties, COL Lansdale was a defense witness for the scientific director of the Los Alamos Laboratory, Manhattan Project, Dr. J. Robert Oppenheimer. Dr. Oppenheimer was accused of participation in Communist Party activities, and was charged with being a traitor and a spy. Years earlier, it was COL Lansdale, alongside General Groves, who had made the call to award Dr. Oppenheimer his security clearance. Later, many would recount his testimony as the most famous moment in the courtroom, and which became the basis for the Broadway play *"In the Matter of J. Robert Oppenheimer."* It is reported that during COL Lansdale's five years of active service from 1941 to 1946, he rarely took a single day of leave, showing his austere devotion to the project, the mission, and his country. He died on 22 August 2003.

COL Lansdale's civilian education includes a BA from the Virginia Military Institute and a law degree from Harvard Law School. His awards include the U.S. Legion of Merit, and the Order of the British Empire, CBE.

2011 Military Intelligence Corps Hall of Fame Nomination Criteria

All Commissioned Officers, Warrant Officers, Enlisted Soldiers or professional civilians who have served in a U.S. Army intelligence unit or in an intelligence position in the U.S. Army are eligible for nomination. Only nominations for individuals will be accepted. Individuals cannot be self-nominated. No unit or group nominations will be considered. The following criteria must be met by all nominees:

1. 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.

2. 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.

3. A nominee must have made a significant contribution to MI that reflects favorably on the MI 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 to the MI Corps Hall of Fame must be received by 30 September 2010 in order to be represented at the 2011 Nomination Board, which will meet in October.

Nominations should be sent to:

Command Historian, US Army Intelligence Center of Excellence,

ATTN: ATZS-HIS, 1903 Hatfield Street, Building 62711,

Fort Huachuca, Arizona 85613-7000

For additional information, email either **lori.tagg@us.army.mil** or **timothy.quinn@us.army.mil.**

eReader Technology at USAICoE

by Vee Herrington, PhD and Captain Ryan Gerner

This is the Digital Age! Why are we printing millions of pages per year?

—Major General John M. Custer III, Commanding General, USAICoE, March 2009

Introduction

The above statement from the Commanding General (CG) was the impetus kicking off the exploration of using eReader technology at the U.S. Army Intelligence Center of Excellence (USAICoE) instead of traditionally printing and distributing course materials to the hundreds of students attending classes. The CG was referring to the fact that the Training Materials Support Branch (TMSB) in 2009 printed almost 20 million pages of courseware for the classes at the Intelligence School. For example, the MI Captains Career Course alone issues 60 documents to 880 students in 27 classes during the year–many of these documents are Field Manuals and consist of hundreds of pages.

Instead of issuing a huge package of printed materials (Field Manuals, Army Regulations, student handouts, practical exercises, etc.), why not issue a small device which holds all of the documents? This device is called an eReader, which is a small hand-held digital reading device. It is lightweight, portable, and reads and feels like a book. Many are wireless, allow notetaking and some even read to you. The devices are searchable, so if you want to find information on a topic you can search hundreds of documents and books residing on the eReader in an instant.

Background

In June 2009, the CG asked Dr. Vee Herrington, the Chief of the Library Division, which also includes TMSB and the Virtual Footlocker, to investigate alternative ways to deliver the course materials. He asked, "If the future is wireless and digital, how do we get there—how can we cut down all of the printing we do?" The CG's 2010 Guidance calls for the MI Library division to seek innovative technologies to provide better training material access to our students. The Virtual Footlocker, had been launched a few years back, providing a searchable repository on the Intelligence Knowledge Network of the course materials. The next logical step in providing innovative technologies might just be eReader technology. This set the stage for launching a series of eReader trials throughout 1st and 2nd quarters of 2010.

It seemed timely to pursue this, since the U.S. Army Training and Doctrine Command had just sent a memorandum on 3 April 2009 supporting eReaders for reducing printing: "eReaders can provide one possible solution for the current practice of printing and physical distribution of courseware, training support materials and products." In addition, several universities throughout the country (University of Washington, Arizona State University, Princeton, Case Western Reserve University, and the University of Virginia) had jumped on the eReader bandwagon and were conducting trials. The focus of these university studies was mainly on environmental issues, cost savings, and the impact on learning.

Selecting an eReader for the Trials

eReaders were emerging technology in the summer of 2009 and few were on the market. The iPad was just a rumor and other devices such as the Plastic Logic Que were many months from hitting the market. As such, only four eReader devices were evaluated based on the prioritized requirements of the school. As Table 1 shows, the JetBook, the Amazon Kindle DX, the Sony and the iRex were all considered for the trials. The prioritized requirements were the following: the screen had to be large enough to read PDF documents; content had to be searchable; and the device had to have the capabilities for bookmarking and notetaking. Although more costly than

Table 1 eReader Requirements

Prioritized Requirements	JetBook 	Kindle DX 	Sony 	iRex 
Size/ Weight	6 x 4 7.4 oz.	10 x 7 18.9 oz. ✓	5 x 7 10 oz.	8.5 x 6 15.3 oz.
Search	Yes	Yes ✓	Yes	Yes
Bookmark	Yes	Yes ✓	Yes	Yes
Notetaking	No	Yes ✓	Yes	Yes
Color	No	No ✓	No	No
Price	$329	$489	$349	$699

Kindle DX meets prioritized requirements.

the Sony, the Kindle DX was selected because of the larger screen size.

eReader Trials and the Endstate Requirements

Prior to embracing an emerging technology, USAICoE needed to run trials to look at the impact on learning of using eReaders. Will the instructors and students find them an acceptable alternative to paper? Will eReaders be durable enough? Will they have the features and capabilities that students want in an eReader? Cost savings was also an issue–over the next five years, would eReader technology save money over printing costs?

An endstate is the set of required conditions that defines achievement of the commander's objectives. The eReader endstate is:

- ✦ USAICoE adopts eReader technology as the main training material source.
- ✦ Best eReader on the market, based on value, capabilities, and durability is selected.
- ✦ Students and instructors find the eReader an acceptable alternative to paper.
- ✦ eReader does not degrade learning.
- ✦ USAICoE saves money over printing costs and students read more books on the CG's Reading List with better availability.

Measures of Effectiveness

The Army uses measures of effectiveness (MOEs) to give insight into how effectively a unit is performing. For the eReader project the MOEs in Table 2 were developed so an informed decision regarding the future of eReader technology at the school could be made. Do trial results support continuing and expanding the eReader project to include future classes?

Table 2 Measures of Effectiveness

Condition	Measurement Type	Desired Outcome	Score WT
Learning not degraded	Structured interview/ survey instrument/AAR	Instructors & students report that 70% of the eReader class performed as well as previous classes, learning not degraded	5
eReader acceptable alternative to paper	Structured interview/ survey instrument	70% of students and instructors indicate that eReader technology an acceptable alternative to paper	4
eReader durable enough for soldiers / battery life sufficient / memory acceptable or SIM capable	% Return Rate for malfunction	No more than 10% of eReaders replaced during trial because of device failure	4
eReader has identified required capabilities	Checklist of desired capabilities	eReader meets 90% of the capabilities	4
eReader allows immediate access to the books on the CG's Reading List and students read more books.	# Books viewed on eReader	• Number of books viewed on eReader vs. number of books on Reading List checked out by non-eReader users • eReader users read 20% more books, as reported on survey instrument	3
Over period of three years, eReader drops in price and saves USAICoE money over printing.	Price per unit vs. printing costs	Price of eReader drops and there is a cost savings over printing	3

Five trials were conducted between September 2009 and March 2010. The Kindle DX was the main focus of the trials. However, a smaller trial of 20 students using the Sony Reader was conducted since preliminary Kindle trial results showed that the students liked the idea of eReader technology but felt that the Kindle lacked some of the capabilities. They wanted a touch screen and thought the Kindle was too slow and would often freeze up–especially during quizzes! The following classes were selected for the trials: Basic Officer Leaders Course (BOLC), Senior Leaders Course (SLC), Brigade Combat Team S2 Course (BCT S2) and the Warrant Officer Basic Course (WOBC).

Table 3 Conduct of eReader Trials

Class	eReader	Trial Period	Resources Loaded	Participants
BOLC	Kindle DX	15 Sep 09 - 15 Dec 09	• 260 PDF documents • 10 books from the CGs Reading List	• 50 students • 3 instructors
SLC	Kindle DX	23 Oct 09 – 09 Dec 09	• 17 PDF documents • 10 books from the CG's Reading List	• 17 students • 2 instructors
	Sony PRS600	17 Jan 10 – 26 Feb 10	• 42 PDF documents	• 17 students • 3 instructors
BCT S2	Kindle DX	27 Jan 10 – 19 Feb 10	• 22 PDF documents • 10 books from the CG's Reading List	• 18 students • 1 instructor
WOBC	Kindle DX	26 Jan 10 – 19 Mar 10	• 30 PDF documents • 10 books from the CG's Reading List	• 20 students • 2 instructors

Before each trial, class training was conducted on how to use the eReader. A survey instrument was created to measure behaviors and attitudes toward eReader technology. In addition to collecting demographic data, 17 survey questions focused on the ease of use of the eReader, the attitudes of using eReader technology instead of paper copies for class materials, reading and study habits, capabilities they desired in an eReader, and problems encountered during quizzes and tests using an eReader.

The instructors also were surveyed and asked questions related to instructional issues. For example, they were asked if they had to change the way they instructed because the students were using the eReader. Did the instructors give the students more time during quizzes and tests or did they teach at a slower pace? Also, the instructors were surveyed about whether they felt the class did as well academically as previous classes. In addition to the instructor survey questions, the grade point averages (GPAs) of previous classes were obtained.

Results

Besides the survey instrument questions, after action review comments were collected. Even though the majority of the participants agreed they would prefer eReader technology to carrying around a pile of books and documents, they felt that neither the Sony nor the Kindle DX was the perfect solution.

The participants commented that the Kindle DX was more difficult to navigate than the Sony, was too slow, and would often freeze during quizzes. The students also felt that the Kindle needed better capabilities such as touch screen, stylus and folders.

The majority provided feedback that they liked the Sony better than the Kindle DX, but it also has some flaws that were problematic. The participants indicated that the Sony screen is too small for viewing the PDF documents. They also complained that they could not view while charging the Sony and there were device delays while notetaking.

- 90% of the students like the idea of going to eReader technology, but don't feel the technology is there yet—they aren't satisfied with the Kindle or the Sony.
- Students want a large screen, a touch screen, wireless, and color.
- 90% would rather carry around an eReader than a pile of books.
- 95% of the instructors would not be opposed to teaching their next class with an eReader.
- No significant difference in overall GPA of the classes using an eReader.
- 82% of the students indicate they would read more books from the reading list if the books were available on an eReader.

Summary of Results

Table 4 eReader Advantages/Disadvantages

eReader	Pros	Cons	MOE Score
Sony PRS600 	• Touch screen • Stylist • Searchable capability • Highlight and save features • PDF format feature • Folder capability • Wireless • Built in dictionary • Cheaper	• Screen is too small (7") • No color • No password protection feature • Screen glare makes reading difficult	16
Kindle DX 	• Large screen (9.7") • Searchable capability • Text to speech ability • Easy on the eyes • Wireless • Built in dictionary	• Poor durability and freezes often • No touch screen • No Stylist • No color • No password protection feature • Poor highlighting • Only handles Kindle format files well • No folders • More expensive • Too slow • Hard to navigate	10.5

Conclusion

Since starting these trials, the eReader market has more than tripled and Forrester Research predicts that 2010 will see many more devices hitting the market with great new features, applications, and lower prices. The Apple iPad was released to stores in April 2010 and is expected to challenge Amazon's Kindle. The iPad does much more than just read ebooks. It has hundreds of applications, plays music, video and games and browses the web. The eReaders are moving from being just a book reader to being more like a small, hand-held full service computer. Forrester Research[1] reports that 2009 was a breakout year for eReaders and ebooks, device sales tripled and content sales were up 176 percent for 2009. The company predicts that eInk will be replaced with other technology and new applications will make non-eReaders (i.e., computers, mobile phones) more eBook friendly. Why purchase a single-function reading device, when you can purchase a dual purpose device? Unlike the Amazon Kindle DX which mainly does a good job of just reading books, future eReaders will come with thousands of applications. Forrester says, "As anyone with an iPhone knows, apps are where the magic happens." A color map application for the Military Intelligence students might be very beneficial!

With more devices coming out in the next few years with better features at lower prices, the school is not ready yet to commit to a course of action regarding the mass purchasing of a particular eReader or other hand-held learning device. More trials with more devices are needed. The trials are encouraging, however, and indicate that the students and instructors are very favorable towards eReader technology–they just don't feel that the optimal device has been found yet. The adoption of this kind of technology will be another step towards focusing on the student centered approach to learning and the adult learning model.

Endnote

1. Sarah Rotman Epps and James McQuivey, "*Ten Predictions for the E-Reader/E-Book Market in 2010,*" Forrester Research, 1 December 2009, accessed at http://paidcontent.org/article/419-ten-predictions-for-the-e-book-market-in-2010

Dr. Herrington received a PhD in Education from Arizona State University and a Master's degree in School Psychology from the University of Cincinnati. After 15 years as a school psychologist and school administrator, she re-careered and obtained a Master's in Information/Library Science from the University of Tennessee at Knoxville. In 2003, she became the Chief of the U.S. Army MI Library at Fort Huachuca, Arizona. Within two years the MI Library won the 2005 Library of Congress Federal Information Center of the Year Award. Much of the success of the library was due to the non-traditional approach to library services–with its "Barnes and Noble" atmosphere. The library environment is relaxed and very customer centered. In 2008, the MI Library Division was expanded to include TMSB and the Virtual Footlocker. Dr. Herrington won the 2008 Federal Librarian of the Year Award and accepted the award with the CG at the Library of Congress in October 2009. She may be reached at vee.herrington@us.army.mil or at (520) 533-8631.

Captain Ryan Gerner was commissioned as a Second Lieutenant from Johns Hopkins University and completed the Infantry Officer Basic Course and Ranger School. He deployed to OIF with the 1BCT, 82nd Airborne Division and served as a Scout Platoon Leader in the 3rd Squadron, 73rd Calvary.

TES SIGINT:

A Conventional Warfare ELINT System Supporting an Unconventional COMINT Fight

by Chief Warrant Officer Two Raul Negron, Jr.

Yesterday, Today, and Tomorrow: Facts and Misconceptions

The Tactical Exploitation System-Forward (TES-FWD) is an integrated Tactical Exploitation of National Capabilities (TENCAP) System, the lineage of which can be traced back to the Modernized Imagery Exploitation System (MIES), the Enhanced Tactical Radar Correlator (ETRAC), and the Advanced Electronic Processing and Dissemination System (AEPDS). The MIES received and processed National imagery data. The ETRAC system processed Advanced Synthetic Aperture Radar data from theater intelligence, surveillance, reconnaissance platforms, while the AEPDS was responsible for receiving and processing theater and nationally derived Signals Intelligence (SIGINT) data. All three were stand-alone systems, serving as pre-processors for the All Source Analysis System.

CW2 Raul Negron in Baghdad, Iraq. Next to him is the TES-FWD's Advanced Miniaturized Data Acquisition System antenna, which provides access to SIGINT data.

The Army began fielding the TES-FWD during the early part of this decade, as a Corps and Echelons above Corps system used to support Corps and Theater Commander's priority intelligence requirements (PIR). The TES-FWD was built to merge the functions of the MIES, ETRAC, and AEPDS into a single system. The system reduced tactical footprints and improved the ability to leverage National and theater level Imagery Intelligence (IMINT) and SIGINT data in support of warfighting capabilities.

The TES-FWD is recognized for its Electronic Intelligence (ELINT) capabilities. Providing ELINT support to commanders is critically important, as it provides details of adversary radar and Electronic, Missile, and Ground Orders of Battle. ELINT continues to provide the U.S. and its allies with situational awareness and indications and warnings (I&W) regarding threat countries' radar, missile, and ground force postures and intentions. ELINT supported conflicts such as the Cold War, Operations Desert Storm/Desert Shield, and will continue to support major conflicts of the future. The threat of a high intensity conflict still exists, and as in the planning and execution coordinated by Coalition Forces in support of the initial phase of Operation Iraqi Freedom (OIF), ELINT will always be one of the primary intelligence disciplines used to support major combat operations of the future.

Often overlooked are the TES' Communications Intelligence (COMINT) capabilities. Understanding the TES' full capabilities also allows commanders to leverage COMINT data. Today's conflicts–OIF, Operation Enduring Freedom (OEF), the Horn of Africa, the Philippines, and other theaters of interest–are COMINT orientated fights. Fully utilizing the TES' COMINT ca-

pabilities ensures commanders receive relevant and timely SIGINT in support of current conflicts.

Combat Support via Multiple Links, Comms Paths, and Accesses

The TES-FWD's ability to interface with a myriad of National, theater, and tactical systems and its direct access to raw intelligence make it truly unique. When fully utilized, the TES-FWD can function as a stand-alone SIGINT and IMINT system.

In its first deployment, I Corps' TES-FWD Soldiers have capitalized on the opportunity to fully employ the system's unique SIGINT capabilities. The TES-FWD's strength resides in its versatile communications architecture. SIGINT data is retrieved from a multitude of worldwide intelligence agencies and support sites. Intelligence dissemination to higher headquarters and major subordinate command commanders is seamless because of its robust communication paths.

The TES' data sharing capabilities are transmitted and received through satellite communications (SATCOM) access. With this connectivity, the TES-FWD can perform its doctrinal functions by providing indications of enemy radar and missile activity. Additionally, its ability to receive and display Blue Force Tracking data complements the commander's common operating picture. Improvised explosive device intelligence data can also be analyzed with the TES-FWD. All of these capabilities are processed and received by the TES-FWD in near-real time (NRT) basis, providing situational awareness for the Corps Commander and staff requirements. The TES-FWD's network-to-network interface and the system's VSat capabilities relay data to subordinate units.

I Corps' TES-FWD vehicles in convoy formation, in preparation for re-deployment to Fort Lewis, WA. I Corps' TES-FWD completed its first deployment while in support of OIF 09-11.

Connectivity to supported echelons and reach-back to the National intelligence community is possible through the TES-FWD's ability to interface with the TROJAN Special Purpose Integrated Remote Intelligence (SPIRIT) communications system. TROJAN SPIRIT systems provide Secret Internet Protocol Router Network and Joint Worldwide Intelligence Communications Systems (JWICS) connectivity to the TES-FWD.

The TES-FWD's Tactical Communications Support Processor (TCSP) transmits and receives NRT high-priority COMINT message traffic and intelligence reporting. Messages are routed to the TCSP via the TROJAN SPIRIT's JWICS connectivity from multiple sources, ranging from tactical messages to National level reports. These reports provide immediate situational awareness to commanders during events of high interest as they occur throughout the battlespace.

TROJAN SPIRIT JWICS connectivity allows database COMINT information exchange between the TES-FWD's internal databases and National intelligence repositories. TES' graphic display and analysis software allow analysts to directly query National agency databases. The results are displayed within the analysts' workstations. The database information exchange is also arranged so that the TES-FWD's databases automatically refresh every ten to fifteen minutes without user interaction. This ensures data redundancy should a National database be inaccessible, such as during database maintenance. Over the past year, retrieved COMINT data was used to assess threat activity in support of counter-smuggling operations, as well as other MultiNational Corps-Iraq (MNC-I) PIR.

The TES' JWICS capability allows TES analysts to remotely log into Sensitive Compartmented Information (SCI) databases. The TES' SCI connectivity is the primary gateway used to provide in-depth and detailed COMINT data for analysis. As a result, TES-FWD SIGINT analysts in Iraq supplied commanders with intelligence that facilitated security operations and counterterrorism operations. Additionally, NRT JWICS network feeds are received through the TES-FWD's TROJAN SPIRIT connectiv-

ity. The TES' JWICS network feeds are similar to the SATCOM feeds. However, unlike the SATCOM feeds, the network feeds contain intelligence data of a higher classification. This intelligence data enhances the Secret level data received via the TES' SATCOM broadcasts, which results in increased situational awareness across the battlefield.

Combat support takes place on the TES' Secret level network. This level of intelligence is relayed to units supporting numerous types of operations. In Iraq, units based their Electronic Warfare (EW) support on the intelligence exploited and analyzed by TES analysts. TES SIGINT analysts monitored historic and immediate intelligence reporting, and when required, disseminated NRT I&W to convoys within their areas of responsibility. TES analysts also cross-cued simultaneously with National, theater ISR, and EW assets to refine threat reporting. High interest tippers were relayed over chat channels to EW personnel, who relayed threat reporting to ground units and EW support. The cross-cueing results undoubtedly saved Coalition Force lives during convoy operations.

The TES-FWD's ability to interoperate and cross-cue with National systems is what truly makes the system distinct. It receives real-time downlinks from select National systems. The downlinks are received and processed within the system's internal servers and processors and are used to conduct SIGINT analysis. The results were used to provide EW analytical support to special operations units during time-sensitive targeting missions. Throughout the course of their deployment, I Corps TES SIGINT analysts helped facilitate the detainment of persons of interest. The downlinked data was also used to conduct COMINT searches. Typically, the COMINT searches were used to provide situational awareness in support of counter-smuggling and counterinsurgency requirements.

Conclusion

Over the last 20 years, TENCAP SIGINT support systems have provided direct access to intelligence for commanders. The capabilities of these systems improved as technological advancements made the gathering, processing, and exploitation of intelligence data more accessible and timely. Their migration from many stand-alone and large footprint systems to a single multi-purpose and minimized footprint system has been consistent with the Army's force modularization process.

The threat of conventional warfare against the U.S. remains a reality. The TES-FWD is ready and able to support such a conflict. Its various ELINT processing capabilities will ensure commanders and their forces are provided the most timely and accurate enemy missile, radar, and ground dispositions. Today, however, the TES-FWD is also able to support the OIF and OEF unconventional COMINT fights. The TES-FWD's multiple receive and transmit paths and its inherent ability to interface with communications enabling systems and National systems has proven to be the TES-FWD's strength. As an integral part of MNC-I, the I Corps TES-FWD has supported elements that range from logistics and support units, to special operations units, and to Corps and above customers.

Courage!

The misconception that TES only provides ELINT support and is only suited for conventional warfare nearly resulted in leaders overlooking the SIGINT capabilities organic to it. TES is equally capable of providing SIGINT support to the unconventional fight, as clearly demonstrated by the I Corps TES team during OIF 09-11.

As the War on Terror continues, the TES-FWD's design makes it configurable and tailorable to support large scale or smaller conflicts. Its deployability is based on the intelligence requirements necessary for commanders to accomplish their missions and offers commanders an expeditionary capability. OIF requirements have called for the full employment of

the TES-FWD's SIGINT and IMINT capabilities, and the system and its analysts have more than met the challenges.

Within the near future, much of the TES-FWD's capabilities will be encompassed under the Distributed Common Ground System-Army architecture. Until that migration process is complete, however, the TES-FWD will continue to support commanders with its unique IMINT *and* SIGINT (ELINT *and* COMINT) capabilities.

The TES-FWD has always had dynamic organic SIGINT capabilities. I Corps' TES-FWD warrant officers, noncommissioned officers, and Soldiers, teamed with the Army Special Program Office engineers, technical advisors, civilians, and contractors demonstrated that a conventional warfare system can support an unconventional fight.

Acknowledgements

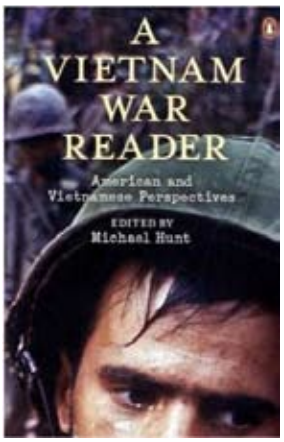
Special thanks to the I Corps TES SIGINT team, SFC Robert D. Hoffstetter, SSG Erica J. Fuchs, SGT Ryan J. Fuhrmann, SGT Iain A. Evans, SPC Kimberly M. Pine, SPC Jason T. Linton, SPC David Cundiff, wingman CW2 Kevin Rinehart, and longtime mentor CW4 (Ret.) Robert D. Rounds (congratulations, buddy).

CW2 Raul Negron currently serves as TES SIGINT OIC, I Corps G2 ACE, Fort Lewis, Washington. He may be contacted at raul.negron@us.army.mil.

Current UMI Courses

- Cryptologic Linguist Reclassification-Phase 1
- Dari Familiarization Course
- Defense Strategic Debriefing Course
- Division Electronic Interceptor Analyst Course
- Every Soldier a Sensor Leader
- Garrison S2 Coordinating Staff
- Imagery Analyst Course
- Information Security
- Intelligence Analyst Military Decision-Making Process
- Intelligence in Combating Terrorism
- Intelligence in Combating Terrorism-Analytical Methods
- Intelligence in Combating Terrorism-Anti-Terrorism
- Intelligence in Combating Terrorism-Terrorist Threat Assess
- Intelligence Oversight
- Intelligence Support to Garrison Operations
- Iraqi Language Training
- ISR Synchronization
- MI Anthropology: Afghanistan
- MI Anthropology: Iraq
- Pashto Familiarization Course
- Pashto Headstart
- Pashto Headstart-Font Downloads and Instructions
- Stability Operations & Support Operations (v.2)
- Tactical Questioning

Professional Reader



A Vietnam War Reader: A Documentary History from American and Vietnamese Perspectives
by Michael H. Hunt, Ed.,

(The North Carolina Press, Chapel Hill, NC, 2010)
256 pages, $59.95, ISBN 978-08078-5991-9

One of the characteristics of a good book is the presentation of both sides to a story. This is what the author has done in providing a masterful commentary of the Vietnam War and the American involvement in it. He has gathered a wide variety of viewpoints and sources of information about one of America's most controversial wars showing the reader how it affected many different individuals. The uniqueness of the book is that we as Americans and others get important insights into how the North Vietnamese viewed the war, what they did, and how it affected them. However, there is also considerable coverage of how it affected the Americans who served in that controversial war.

The book, however, is not just about America's relation to the war or Vietnamese participation in it. For example, the author begins the work with a basic chronology of events affecting Vietnam and ends it with American diplomatic relations being established with Vietnam in 1995. The amount of information found in the book before the huge American military presence comes about is quite interesting and valuable because it helps to understand the motivation and characteristics of the Vietnamese people. What we see is a country dominated for a long time by foreigners and exploited in various ways by outsiders. We also see a strong sense of unity among the people, coupled with a feeling of nationalism, and a desire for independence. For generations, indigenous leaders had sprung up in Vietnam to improve the country, but were often made ineffective by outside political interests. After the Vietnam War and the Americans depart the country once becomes unified with a hope for improvements.

However, the gist of the book is really about the Vietnam War period and American involvement in it through a Vietnamese perspective. It is in this time frame that readers are exposed to a series of communications made by a wide variety of individuals on both sides who were affected by the Vietnam War or who felt a need to comment on it. These communications contain comments made all the way from low ranking soldiers on both sides of the conflict to major world leaders such as the president of the U.S. and the leader of North Vietnam. For example, a private first class who fought for North Vietnam in the Tet Offensive and who was later captured, notes that he wanted to liberate the country from the American imperialist. (155) On the other hand, a young American army soldier wrote to his Mom and Dad that "Everything is just fine—in fact it's better than I thought it would be," even though he was later killed. (127) Contrasting views of one's involvement, perceptions, and experiences of individuals on both sides of the war are what make this book so interesting and different from other books about the Vietnam War which generally give just one side's view. The North Vietnamese are pictured as being motivated in the war by a strong sense of patriotism and a desire to unite Vietnam into one country, while the U.S. is pictured as fighting to stop the spread of communism. A need recognized by the North Vietnamese to enlist the popular support of ordinary peasants is also contrasted with the My Lai Massacre where a large number of unarmed peasants were killed by the American soldiers.

Although the book does contain reflections of military personnel on both sides, there is plenty of com-

mentary about politicians and prominent citizens in terms of their views regarding the war. For example, Ho Chi Minh's comments to the Politburo about the need to be able to fight a protracted war against the Americans are interesting, and so are those of Senator Stennis made to the American Legion National Convention where he calls for a more aggressive war policy toward North Vietnam.

It's also interesting to see the author's comparison of the North Vietnamese fighters to American servicemen. They had a cause in which most could believe. The multiple personal reasons to fight were reinforced by a steady, systematic party-directed effort at keeping morale high. But these same fighters had to confront a much greater likelihood of death than Americans ever did. They were in the struggle for the duration, not just twelve months, and they faced a foe with an overwhelming advantage in weaponry. They had to absorb the punishment the far more powerful Americans could throw at them and then line up and take the punishment again. (124)

Of course, the struggle in Vietnam did not just involve combat between various military individuals. There were other effects on the domestic scene as well. Large numbers of civilians were killed, property was destroyed, and normal social functions such as family matters were interrupted in both parts of Vietnam. In the U.S. domestic dissent and opposition to the war became major events of the time. It is in this type of environment that the author has chosen to seek out information about how individuals were affected by the war.

The book itself is not very long. It can easily be read in a couple of evenings, perhaps even sooner because of the human interest brought to it by focusing on some of the personal recollections of individuals associated with the war. It should be of interest to anyone today who has been affected by the war, and that means many of us. Special interest in the book will probably be taken by those who served in that war. Its reliance on primary sources of information such as documents and speeches lifts it to a level of scholarship that will also be appreciated by academics who are either interested in various views of the war or who are looking for a valuable supplement to be used in a university course dealing with it.

For many reasons, the Vietnam War will remain of interest to us for a very long time. Perhaps one reason is that it was a controversial war which means that individuals have different views about it. This book will be a substantial contribution to knowledge about the Vietnam War from different and varying personal accounts, and perhaps lead to a better understanding of it.

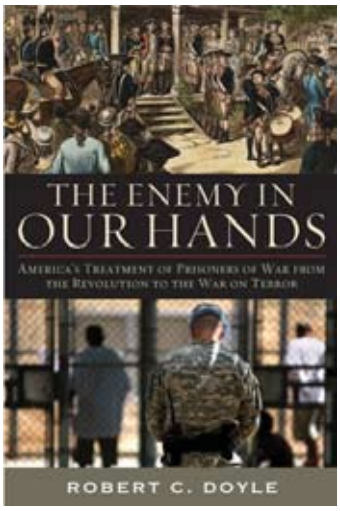
Reviewed by William E. Kelly, PhD, Auburn University

Read any good books lately?

We welcome reviews of books related to Intelligence or Military History. Please review our list of available books and book review submission standards under the Professional Reader Program at https://icon.army.mil/apps/mipb_mag/.

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

Professional Reader



The Enemy in Our Hands by Robert C. Doyle,

(The University Press of Kentucky, Lexington, KY, 2010)
496 pages, $34.95, ISBN: 978-0-8131-2589-3

This book is about the treatment of enemy prisoners of war (EPWs) held by the Americans. Its author, Robert C. Doyle, has published two other works dealing with the subject of POW status. He has also been a consultant for a number of documentary film projects and has made presentations regarding his professional interests at various prestigious institutions such as the U.S. Air Force Academy. Hence, he is quite capable of writing on the subject of POWs. The author notes that "the objective of this work is to contribute to filling in some blanks left hazy, and in many cases, empty in the many studies of the American experience of war." (xvii)

The scope of the book is quite large since it covers the period from the Revolutionary War to the current War on Terror. One of questions researched by Doyle was how the U.S. treated its enemy EPWs. The answers depended on a number of factors such as what wars, what times, and who the enemy was at the time of the war. Other factors could also explain the treatment toward EPWs such as their behavior while imprisoned, the attitudes of their captors, the Geneva Convention, and the culture of a particular country which holds POWs.

Upon reading the book one learns that during a major war against a nation state like Germany and Japan, soldiers who became prisoners of the Americans and incarcerated in the U.S. were generally treated in a humane manner. This was also true during the American Revolutionary War with the exception perhaps of the Loyalists who sided with England during the conflict. However, during the Civil War humane treatment of captured soldiers by both sides at times seemed to be lacking as exemplified by events present at the Union POW camp in Elmira, New York and the Confederate POW camp at Andersonville, Georgia.

As mentioned above, a country's culture also affected the way EPWs were treated. Japan (during World War II) is cited as an example. Examples of Japanese culture of the times that may have influenced how Americans treated Japanese prisoners are illustrated in the following quotes: "Because they believed that surrender was an act of shame and disgrace to all soldiers of all nations, the white flag of surrender meant little to the Japanese. Regardless of how deceitful it may have seemed, Japanese soldiers often lured their enemies into open death traps where, instead of surrendering honorably, they waited in ambush. Wounded men kept hand grenades for use against unsuspecting enemy soldiers who attempted to help them." (206)

Another part of the book quotes an individual who served Japan when the Americans invaded Saipan. "In those days, Japanese soldiers really accepted the idea that they must die. If you were taken alive as a prisoner you could never face your own family. Those unable to move were told to die by a hand grenade or by taking cyanide. …Ones like me, who from the beginning were thinking about how to become prisoners, were real exceptions."(209)

The time frame of World War II is viewed as a commendable period in American treatment of the EPWs incarcerated in the U.S. Perhaps the reasons for this type of favorable treatment by the Americans was the Geneva Convention of 1929 which man-

dated humane treatment toward prisoners of war, as well as a hope that the enemy would reciprocate in its treatment of our prisoners. The book cites several examples of where EPWs held in the U.S. actually benefitted from their incarceration experience. The author notes: "World War II was, without doubt America's finest hour in terms of its treatment of EPWs." (342)

When one reads this book it is interesting to note that the status of a captured person could affect the treatment of the individual by the Americans. For example, the author seems to suggest that generally those individuals who were readily identified as captured soldiers in the uniform of an opposing nation were generally treated well by the Americans. When it comes to other individuals who were not clearly identified as soldiers of an opposing nation involved in war with the U.S., the treatment of them could be harsh. An indication of this is in the author's description of American military treatment of detainees at the infamous Abu Ghraib prison during the Iraq War. The book makes it quite clear that having an identified military status with a country does make a difference in terms of treatment by the Americans.

The author also seems to advocate a view that it is in everyone's best interest to treat EPWs fairly and humanely. This is understandable for a number of reasons. For example, the idea of reciprocity is advantageous to both sides in a conflict. This implies that if the Americans treat their EPWs humanely, there might be more of a chance that their own soldiers will be treated in a similar fashion upon capture. Secondly, the treatment of EPWs in a humane manner projects a favorable image of a country which is advantageous in international affairs. In addition, there is the possibility that today's POW may become tomorrow's ally as demonstrated by those German World War II prisoners of war held by the Americans who later became allies with their American captors against the former Soviet Union.

Reviewed by William E. Kelly, PhD, Auburn University

Captain Charles R. Bailey

2010 Recipient
Lieutenant General Sidney T. Weinstein Award for Excellence in Military Intelligence

In honor of LTG Weinstein, the Military Intelligence (MI) Corps created the *LTG Sidney T. Weinstein Award for Excellence in Military Intelligence* in 2008. Each year the award recognizes one outstanding MI Captain who, through his or her actions, demonstrates the values and ideals for which LTG Weinstein stood: *Duty, Honor, and Country.*

Captain Charles Bailey enlisted in the U.S. Army as a Counterintelligence (CI) Agent following graduation from Keene State College with a BA in History. Upon completion of his initial training, he was assigned to a CI team with the 202nd MI Battalion, Fort Gordon, Georgia.

Selected to attend Officer Candidate School, CPT Bailey earned his commission as an Infantry Officer in January 2003, and subsequently attended and graduated from Airborne and Ranger schools. His first assignment was as a Rifle Platoon Leader with the 1-17 Infantry Regiment, 172nd Stryker Brigade Combat Team. He was then selected to lead the reconnaissance platoon, both in garrison and in Mosul, Iraq in support of Operation Iraqi Freedom. CPT Bailey led numerous offensive operations resulting in the death or capture of more than 100 armed insurgents. In June 2006, he was wounded in a suicide vehicle borne improvised explosive device attack and assigned to Walter Reed Army Medical Center. Determined to continue to serve his country, he re-branched into MI.

Following attendance of the MI Captains Career Course, CPT Bailey was assigned to the 66th MI Brigade where he briefly served as Assistant Battalion S3 before being selected to lead the Headquarters and Operations Company of the 105th MI Battalion. Following the inactivation of the 105th, he was selected to command the Stuttgart MI Detachment and the Communications and Technology Detachment-Europe, 2nd MI Battalion in June 2008. During his command, he provided vital CI and force protection support to one of the more critically important garrisons in Europe and to senior leaders in European Command and Africa Command.

Captain Bailey's awards and decorations include the Bronze Star Medal, Purple Heart, Army Commendation Medal (1 OLC), Army Achievement Medal (1 OLC), Valorous Unit Award, Iraq Campaign Medal, Global War on Terrorism Service Medal, Combat Infantryman Badge, Ranger Tab, and Airborne Badge.

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

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

PIN:100114-000