MI Professional Bulletin

January - March 2014
PB 34-14-1

Emerging Intelligence Capabilities

Subscriptions: Free unit subscriptions are available by emailing the Editor at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. Include the complete mailing address (unit name, street address, and building number) and the number of copies per issue.

Don’t forget to email the Editor when your unit moves, deploys, or redeploys to insure continual receipt of the Bulletin.

Reprints: Material in this bulletin in not copyrighted (except where indicated). Content may be reprinted if the MI Professional Bulletin and the authors are credited.

Our mailing address: MIPB, USAICoE, Box 2001, Bldg. 51005, Ft. Huachuca, AZ, 85613

Issue photographs and graphics: Courtesy of the U.S. Army and issue authors.

Commanding General
MG Robert P. Ashley

Chief of Staff
COL Jeffrey E. Jennings

Chief Warrant Officer, MI Corps
CW5 Joe D. Okabayashi

Command Sergeant Major, MI Corps
CSM Jeffery L. Fairley

STAFF:

Editor
Sterilla A. Smith

Design and Layout
Gary V. Morris

Cover Design
Gary V. Morris

Military Staff
MAJ Antonio Crucet III
SFC Rebekah L. James

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

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

By order of the Secretary of the Army:
Official:

GERALD B. O’KEEFE
Administrative Assistant to the
to the Secretary of the Army
1401401

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

From The Editor

Important Notice: As directed by the CG, ICoE MIPB is undergoing some changes that will improve this professional bulletin over the course of the upcoming year. We identified some aspects of this bulletin that will be improved to ensure we discuss the topics most important to our Army MI force, broadcast the most important intelligence strategic messages, and use MIPB as a driver for training and force modernization developments.

Some of the changes are: reintroducing MIPB themes, soliciting specific articles from senior leadership and across the MI Corps, changing some of our recurring departments and adding new ones. You will also see a change in the current MIPB format for easier reading and added visual appeal.

Articles from the field will always be very important to the success of MIPB as a professional bulletin. Please continue to submit them. Even though the topic of your article may not coincide with an issue’s theme do not hesitate to send it to me. Most issues will contain theme articles as well as articles on other topics. Your thoughts and lessons learned (from the field) are invaluable.

The following themes and suspenses are established for:

April-June 2014, *Intelligence Training and Leader Development,* deadline for article submissions is 14 March 2014.

July-September 2014, *TRADOC Culture Center*, deadline for article submissions is 21 May 2014.

October December 2014, *INSCOM*, deadline for article submissions is 21 August 2014.

Due to a lack of articles and in order to reenergize our publication and implement this new method of operation to begin with this issue, we did not publish the October-December 2013 issue. For those who submitted articles for the October–December issue, you can expect to see them in the January-March or April-June issues.

Please call or email me with any questions regarding your article or upcoming issues. We appreciate your cooperation as we undertake this exciting new effort to upgrade MIPB and serve you better.

Sterilla Smith
Editor

MI Professional Bulletin

January - March 2014
PB 34-14-1
Volume 40 Number 1

7

16

FEATURES

DEPARTMENTS

Always Out Front

by Major General Robert P. Ashley
Commanding General
U.S. Army Intelligence Center of Excellence

> ***"We need to clearly distinguish our thinking in terms of near, mid and far term. Many audiences have written off the deep future. We cannot afford to do that. It's not a series of simple modifications of what we currently have. We need to be both technology takers and makers; take now, make for the future. There are over 90 countries that can buy advanced items off the commercial shelves right now; we need to keep our technological overmatch. What keeps me awake at night is not thinking about breakthroughs that other nations are already working on. We need to focus and balance our portfolios accordingly."***
>
> ***–General Cone, Commanding General, TRADOC, November, 2013***

Rapid technology developments in response to urgent wartime requirements have brought the intelligence community (IC) some tremendous new capabilities. Advancement in the areas of biometrics, battlefield forensics, miniaturization, SIGINT terminal guidance, DCGS-A, and distributed processing have been vital to the success of Military Intelligence (MI) and the Army. This issue of MIPB looks at several of these capabilities and their integration into our formations. To the greatest extent possible, we must leverage these wartime investments to help us mitigate fiscal and force reductions. As leaders and professionals, you must understand how these technologies support our mission; and that means first-hand experience. I encourage you to embrace and promote, as well as challenge these technological developments.

Here at the Intelligence Center of Excellence we are pursuing a short-term and mid-term strategy that includes selecting the best of these capabilities, identifying areas for potential development, and integrating them into current programs. Some promising areas for short-term and mid-term development include a multifunction tablet, a sensor common operational picture, augmented analytics, and a smart sensor capability. Development of these capabilities will enhance intelligence operations, provide leaders with higher fidelity situational awareness, and support the Army's goals of reducing our support footprint and providing more effective expeditionary forces.

The long-term outlook, however, identifies many new and significant challenges. Recently, Department of Defense and IC leaders warned Congress that our current incremental capability development and investment strategy is unlikely to sustain a competitive advantage past 2030. Over the past several years, our competitors have invested and continue to invest in fundamental research and promising emerging technologies. For us to maintain our competitive advantage, our research and development community must focus on breakout, leap-ahead technologies, as opposed to evolutionary, incremental gains.

Despite difficult fiscal constraints a number of operational realities will drive this paradigm shift. These realities include:

- ✦ An interactive and complex operational environment with continuously changing threat networks and regional/local perceptions, and an intense competition for local support.
- ✦ A continued trend towards urbanization that will challenge our ability to distinguish between friendly, neutral, and threat personnel and to identify, track, and target threat forces and personnel.
- ✦ An increased operational tempo that will challenge our ability to process information quickly enough to be useful to leaders and staffs.
- ✦ Enemy anti-access and area denial capabilities that will challenge our Global Positioning System technologies and our ability to collect from stand-off distances.

In spite of these realities, I'm convinced that our MI core competencies–collection, analysis, and intelligence synchronization–remain enduring and central to assessing our future technological needs. The Intelligence and National Security Alliance has identified several emerging technologies that illustrate the potential to significantly improve performance of our core competencies.

Collection. Emerging technologies will produce a new generation of sensors that are able to answer a broad range of future collection requirements. The new generation of sensors must be capable of collecting from stand-off distances and in urban environments and they must sense a variety of threat signatures. These sensors must be able to operate effectively in spite of denial and deception tactics and techniques and must perform reliably in the harshest environments. Opportunities exist in:

- Social media and mobile network exploitation to offer insight into rapidly emerging hot spots in near real time.
- Energy harvesting to solve issues with sensor battery life. In this context energy harvesting is the process of collecting energy from the surrounding environment and converting it into electricity or another useful form.
- Big data capture, exploitation, and analysis to support intelligence operations.
- Behavioral biometrics–unique behavioral and psychological characteristics to aid in identity resolution or detection of deceptive intent.

Analysis. New technologies will enable intelligence analysts to rapidly process data and information from a wide variety of sources into specific intelligence products that provide tactical, operational, and strategic situational understanding. Opportunities exist in:

- Context-based data-mining using advanced algorithms and pattern detection to process all sources of data into meaningful intelligence.
- Natural language processing (automated text and voice translation), semantic metadata generation (automated tagging of time, location, and context of collection), and context-based reasoning to significantly improve the entire information inference chain.
- Bio-inspired computing (study of life to improve the usage of computers) and human-inspired big data coping strategies (multi-level, human reasoning inspired approach to automated problem solving) to help a limited number of analysts make sense of a vast volume of data more quickly and accurately.
- Holistic knowledge management schemas that facilitate and guide the art of intelligence analysis.

Intelligence Synchronization. Emerging technologies will allow Soldiers at all echelons easy, secure, and reliable access to intelligence. Additionally, technology will provide access to and collaboration with collection managers that will facilitate quick adjustments to our collection in order to react to changing situations. Opportunities exist in:

- Swarm technologies and communications that enable large numbers of inexpensive, simple, and controllable collection devices to collaborate on difficult urban terrain collection tasks.
- Holographic, 3D display of all available collection assets and resources in real time or near-real time at whatever scale the commander requires.
- Carbon-based electronics to achieve computing power beyond the limits of silicon.

Over the course of my career, I have witnessed a radical transformation in intelligence capabilities and intelligence missions. We have gone from acetate to Google Earth and from the ability to track major combat formations to the ability and need to track single individuals. The future operational environment will require us to cover all the aforementioned areas. Technology has made our job both easier and more complex. Technology has mandated that our intelligence professionals be better educated, better trained, and more versatile than ever before. As we move forward, I have faith that our MI Corps will continue to lead in the identification and exploitation of new and innovative technologies that will provide critical intelligence to operational commanders.

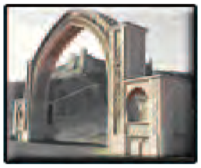
Always Out Front!

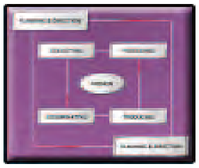
What is the UMI? Where is it? How do I use it?

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

UMI
Powered by
USAICoE





CSM FORUM

by Command Sergeant Major Jeffery L. Fairley
U.S. Army Intelligence Center of Excellence

Team,

Happy New Year to all of you!

I hope each and every one of you had a safe and wonderful Holiday Season.

2014 promises to be a great year for the MI Corps. This year will also present numerous challenges and hurdles as we continue to restructure and shape our force for future contingency operations with limited resources and many competing requirements.

Over the past few months the Deputy Chief of Staff (DCS), G3/5/7 provided detailed guidance on how the Army would go about implementing the One Army School System (OASS). The DCS further outlined his vision of what “centralized missioning” is, as well as how units should proceed in streamlining their individual efforts and optimizing institutional training to come on line with that vision. I can share with you MI Professionals that the implementation of the OASS will prove to have great benefits for our young MI Professionals in the future.

In order to meet and optimize efforts within the Intelligence training structure and in accordance with Headquarters, Department of the Army (HQDA) guidance, your Senior Intelligence Leadership began immediate evaluation of the current curriculum and courseware being taught within our MI Noncommissioned Officer Academy (NCOA) system. The goal of the evaluation was two-fold in nature. One, the evaluation was to ensure that the courseware met the equivalency standards needed to come “on-line” with the DCS’s guidance and two, that the curriculum met the parameters of that vision. I can promise you MI Professionals that your Senior Leadership is meeting the demands coming out of HQDA and is working tirelessly to ensure that you stay relevant and current in the fight.

In light of the above challenges I have every confidence that we as a Corps will continue to be out front as we shape the Army of 2020. This month’s MI Corps CSM newsletter (See website at the end of this column) reiterates the importance of getting our young Service Members to NCOES. I realize that units are facing a tough challenge of getting their Soldiers into positions where they can take advantage of these valuable educational opportunities, but I am confident that they will get it done and take care of our Soldiers.

During 2014 I would like to encourage all of the many Intelligence professionals in the Force to continue pushing towards the mark of excellence. With the start of the New Year it will be important that we as leaders focus on re-emphasizing the importance of the Army Profession, getting back to basics as it pertains to Soldiering, and creating a more ready and resilient force structure. I am glad to report that our current overall personnel strengths continue to increase and we are recruiting and retaining quality Soldiers and future MI leaders. As always I thank each of you for your efforts and I am truly honored to be part of this team.

Always Out Front!
Army Strong!

MI Corps CSM Website:
https://ikn.army.mil/apps/IKNWMS/Default.aspx?webId=2360

Check out the Fort Huachuca Museum website at
http://huachucamuseum.com

Technical Perspective

Chief Warrant Officer Five Joe D. Okabayashi
U.S. Army Intelligence Center of Excellence

I want to highlight the changes we are making to our Military Intelligence Warrant Officer Basic Course and Military Intelligence Warrant Officer Advanced Course. To inform you of these updates I defer to CW4 Matt Martin (Chief, Warrant Officer Training Branch) in his recent article published in the MI Senior Mentor Symposium last August. In the coming days, in this publication and in other forums, we will update you on our U.S. Army Training and Doctrine Command approved efforts to implement MI Branch Technical Training Phases to be added to our Army's Warrant Officer Staff Course and Warrant Officer Senior Staff Course.

We look forward to your feedback on the evolution and needs of our warrant officer leader development and training. Your participation in surveys and in critical task site selection boards is essential to shaping our leader development and training.

As you read Matt's article below, know that I thank all of you for your selfless service, your dedication and commitment to our Army and our Nation. I thank your families for their generous and giving support to you–please, take the time to thank them!

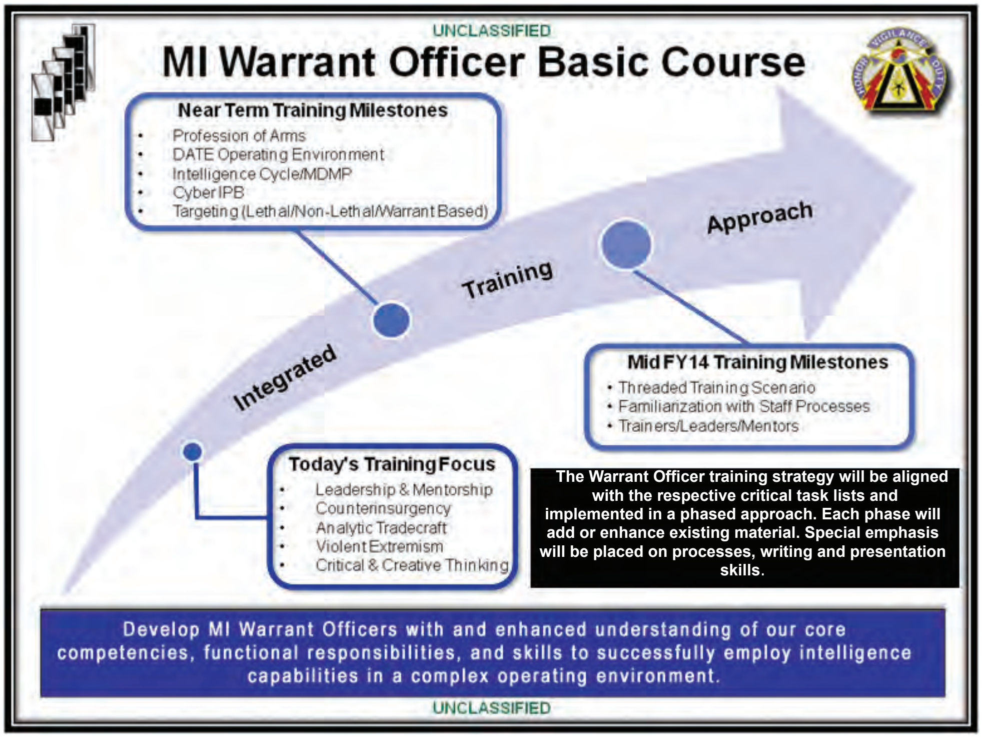
–CW5 Okabayashi, Chief Warrant Officer of the MI Corps
Always out Front!
Army Strong!

Warrant Officer Training Branch–Getting Back to the Basics

by Chief Warrant Officer Four Matthew R. Martin

The evolution of conflict in Iraq and Afghanistan provided Soldiers with an unprecedented amount of practical experience and knowledge. Leveraging the acquired experience, while adapting the training environment beyond the current fight, is necessary in the development of the Army's next generation warrant officers (WOs). Therefore, as the Army transitions from Afghanistan, it is paramount that leaders establish a balance between applying counterinsurgency lessons learned while revisiting our foundational intelligence competencies that have largely remained dormant.

The U.S. Army Intelligence Center of Excellence–Warrant Officer Training Branch (WOTB) recognizes the need to "get back to the basics" by focusing training on leadership skills and technical proficiency. The Soldiers' education and training experience will be centered on the core competencies of the Intelligence Warfighting Functions. Special attention will be directed towards the intelligence cycle and the Military Decision Making Process (MDMP).



UNCLASSIFIED

MI Warrant Officer Basic Course

Near Term Training Milestones
- Profession of Arms
- DATE Operating Environment
- Intelligence Cycle/MDMP
- Cyber IPB
- Targeting (Lethal/Non-Lethal/Warrant Based)

Mid FY14 Training Milestones
- Threaded Training Scenario
- Familiarization with Staff Processes
- Trainers/Leaders/Mentors

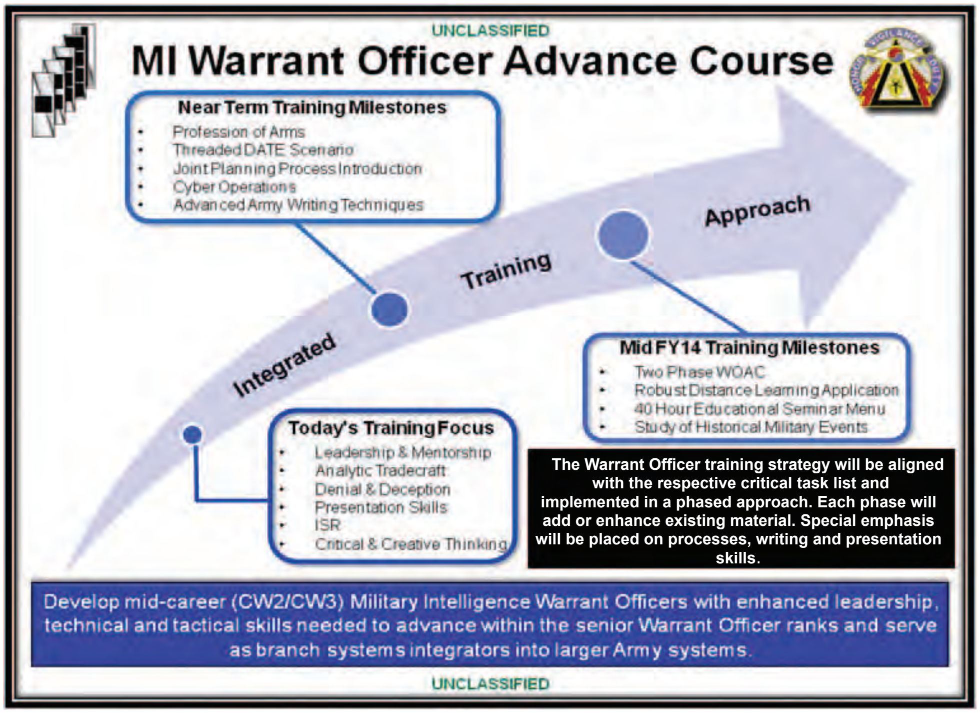
Today's Training Focus
- Leadership & Mentorship
- Counterinsurgency
- Analytic Tradecraft
- Violent Extremism
- Critical & Creative Thinking

The Warrant Officer training strategy will be aligned with the respective critical task lists and implemented in a phased approach. Each phase will add or enhance existing material. Special emphasis will be placed on processes, writing and presentation skills.

Develop MI Warrant Officers with and enhanced understanding of our core competencies, functional responsibilities, and skills to successfully employ intelligence capabilities in a complex operating environment.

UNCLASSIFIED

The Military Intelligence (MI) WO Basic Course is an 11-week course that certifies seven MI WO specialties. The first four weeks focus on integrated or common core curriculum. During the remaining seven weeks, each respective Military Occupational Specialty (MOS) transitions to specific technical training. To meet the demands of the future operational environment, the WOTB is developing a collaborative program of instruction that streamlines the existing curriculum by bridging the gap between integrated and technical training. The intent is to enhance the Soldiers' understanding of the intelligence disciplines, while fostering communication across all intelligence specialties. This will be accomplished through the implementation of a seven-week threaded Decisive Action Training Environment scenario during which Soldiers will serve in multifunctional teams. These teams will gather at predetermined periods throughout the course to collaborate and deliver Distributed Common Ground System-Army enabled intelligence products within the framework of the intelligence cycle and MDMP.


UNCLASSIFIED

MI Warrant Officer Advance Course

Near Term Training Milestones
- Profession of Arms
- Threaded DATE Scenario
- Joint Planning Process Introduction
- Cyber Operations
- Advanced Army Writing Techniques

Mid FY14 Training Milestones
- Two Phase WOAC
- Robust Distance Learning Application
- 40 Hour Educational Seminar Menu
- Study of Historical Military Events

Today's Training Focus
- Leadership & Mentorship
- Analytic Tradecraft
- Denial & Deception
- Presentation Skills
- ISR
- Critical & Creative Thinking

The Warrant Officer training strategy will be aligned with the respective critical task list and implemented in a phased approach. Each phase will add or enhance existing material. Special emphasis will be placed on processes, writing and presentation skills.

Develop mid-career (CW2/CW3) Military Intelligence Warrant Officers with enhanced leadership, technical and tactical skills needed to advance within the senior Warrant Officer ranks and serve as branch systems integrators into larger Army systems.

UNCLASSIFIED

The MI WO Advanced Course (MIWOAC) is a six-week course that provides CW2/CW3 WOs with additional leadership and technical skills needed to advance within the senior WO ranks. The curriculum centers on MOS-related topics from a variety of subject matter experts. This affords Soldiers the opportunity to share their experiences with fellow warrant officers in a learner-centric environment. Additionally, Soldiers are challenged with leadership and mentorship responsibilities associated with the senior WO positions in which they will soon serve.

In the future, the WOTB seeks to transition the MIWOAC into two phases. Phase One will integrate learning technologies to deliver distance learning modules including Army effective writing, leadership development, and knowledge management. This phase will also enhance the Soldiers' knowledge of the joint operating environment via the phases of war. Phase Two of the MIWOAC is a resident course that will continue to expand the Soldiers' knowledge of the operational environment through the application of the joint planning process, critical and creating thinking, collection management, lethal and non-lethal targeting, and the examination of significant historical events that have shaped today's operational environment. WOTB also wants to afford Soldiers the opportunity to construct their desired training outcome. WOTB will allow Soldiers to choose from a selection of seminars, each no longer than 40 hours in length. The Soldiers will select a seminar based on a self-evaluation and guidance provided by the MIWOAC cadre. WOTB will host these select seminars which will be taught by local instructors.

Today's MI WOs are proven leaders equipped with exceptional knowledge and skills. As the operational landscape shifts, WOTB will continue the process of improving educational design to produce highly adaptive and technically proficient WOs. In turn, these WOs will serve as organizational innovators and leaders able to provide operationally relevant support to mission command.

CW4 Matthew Martin is an All Source Intelligence Technician with 20 years experience as an intelligence professional. He is presently serving as the Chief of Warrant Officer Training Branch for the 111th Military Intelligence Brigade, U.S. Army Intelligence Center of Excellence at Fort Huachuca, Arizona.

IROC: Redefining Army Intelligence

by Captain Patrick C. Mulloy

"The commitment of Soldiers to the fight is no longer a matter of proximity."
–Colonel Todd A. Megill, FORSCOM G2

Introduction

In this era of political uncertainty and fiscal austerity, the demand for tailored intelligence from commanders operating in complex environments has exponentially increased. Formidable challenges await the U.S. Army in current conflicts, such as Afghanistan, and future conflicts likely to involve hybrid threats, possibly in the Levant or the Maghreb. To meet these challenges, Army Military Intelligence (MI) is developing an innovative concept, the Intelligence Readiness and Operational Capability or IROC.[1]

The 2d Cavalry Regiment (2 CR) is among the few tactical brigades in the Army and the first brigade in U.S. Army Europe (USAREUR) to operate under the IROC concept. This article describes the IROC design as part of Army 2020 and subsequently addresses how 2 CR is currently leveraging the IROC concept to support combat operations in Kandahar Province, Afghanistan.

"No Cold Starts, No MI Soldier at Rest" [2]

It became apparent early on in the campaigns in both Iraq and Afghanistan that intelligence analysts at the tactical level were unprepared to satisfy commander's requirements. The multitude of surveillance reports and subsequent requirements to process and analyze collected information overwhelmed tactical intelligence sections. To address these concerns, the U.S. Army Intelligence and Security Command (INSCOM) established Project Foundry in 2006.

Foundry was a visionary concept. It was initially designed to be a training program in which Soldiers could train individual and collective tasks specific to the Intelligence War Fighting Function (IWFF) prior to a deployment. It allowed intelligence professionals to have a specialized platform where they could improve analytical and technical skills and ensure that the tactical intelligence shortcomings experienced in Iraq and Afghanistan would never recur. Since its establishment, it has been widely reported that Foundry has trained nearly 100,000 intelligence professionals on topics ranging from foreign language enhancement to interrogation skills. The European Foundry Platform (EFP) Director, Mr. Tod Stimpson, summarizes it best when he stated that, "Foundry gives Soldiers a means to enhance and focus their MI skills before the unit deploys."

The Army's vision for "Army Intelligence 2020 and Beyond" expounds on Foundry's foundational idea of a training capability, known as Foundry 2.0.[3] Foundry sites are now evolving to become Tactical Overwatch and Intelligence Reach facilities or IROC-enabled locations.

IROC aggressively increases intelligence readiness and prepares Regionally Aligned Forces (RAF) to defeat threats with a *reduced* forward deployed force while *increasing* the use of established, internal, intelligence capabilities at a home station. IROC strives to improve the tactical and operational flexibility of Army commanders, ensures the IWFF's relevance in decisive action and optimizes existing intelligence architecture.

IROC Activities

- Home Station Training
- Individual and Collective Tasks
- Support Mission Command
- Support RAF Construct
- Intelligence Reach

In order to increase readiness, MI Soldiers need to be actively and continuously engaged in relevant global security affairs so they are better prepared to provide valuable intelligence to their commanders. By establishing an IROC-enabled location, commanders can train their MI units and Soldiers to support their intelligence requirements by developing training objectives that are either a current applicable operation or regional security threat. These objectives would be nested within the unit's mission responsibilities, such as an upcoming deployment in support of Operation Enduring Freedom or the unit's regional mission as part of a RAF.

Regional alignment allows a commander to simultaneously train MI units collectively, MI Soldiers individually, and more importantly develop an in-depth understanding of the dynamic environment and potential threats before deploying. If required, a commander could gain immediate insight for planning from his intelligence staff if his unit is to deploy in support of a regionally aligned operation. Colonel Todd Megill, U.S. Army Forces Command G2, explains, "IROC not only allows the IWFF to be ready, improve, and remain continuously engaged, but it also allows the mission commander to train his subordinate commanders and staff on critical intelligence operations and fusion functions."

As the Army's fundamental deployable maneuver organization, the brigade combat team (BCT) is the optimal echelon for implementing the IROC design. Unlike other Army echelons, the BCT possesses the all-source and analytical capabilities required to perform substantial intelligence driven missions. BCTs are the combat power for combatant commanders' RAF. RAF is the Army Chief of Staff's, General Ray Odierno, initiative to align BCTs with specific regions in the world so they become resident experts and therefore better prepared for contingency operations in their area of responsibility. RAF supports operational missions, bilateral and multilateral military exercises, and theater security cooperation activities. IROC considerably improves situational awareness for the BCT commander charged with a RAF mission. Along with tactical BCTs, Theater Intelligence Brigades, as part of INSCOM, will also be regionally aligned to support the combatant commanders' requirements.

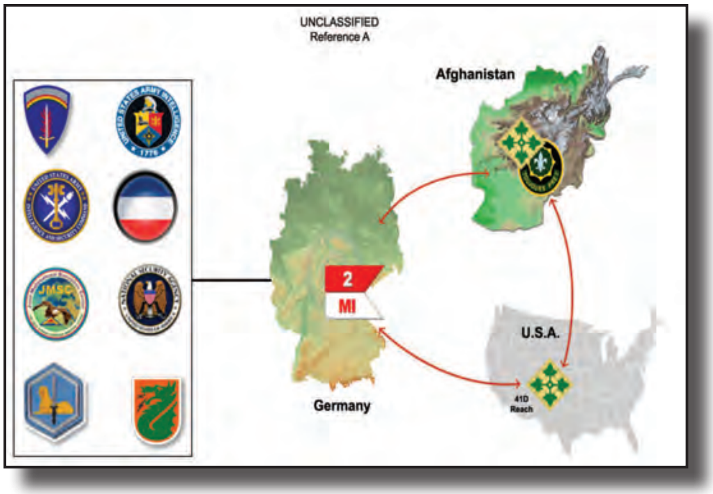
MI Soldiers are best utilized when positioned with the commander, personifying the "Always Out Front" MI branch motto. However, in current conflicts and likely in future ones, deploying an entire BCT worth of combat power is counterproductive and likely unfeasible. Intelligence reach allows BCTs to accomplish their mission without deploying the entire brigade and is a key component to IROC. It allows deployed units to conduct direct collaboration and information sharing with other units, unconstrained by geographic proximity, echelon, or command. At the tactical level, IROC's intelligence reach is specifically designed to provide the commander an organic, home station based unit which provides tailored intelligence specifically for the BCT commander.

An advocate of intelligence reach, Foundry 2.0, and implementing IROC across the Army, is the Army Deputy Chief of Staff for Intelligence, Lieutenant General Mary A. Legere. According to LTG Legere,

> ***"...in order to support our Army Intelligence 2020 goal of 'no MI Soldier at rest,' Foundry is now employing MI Soldiers in dwell against live theater collection or production requirements, providing expert support to our Army forces forward ... our goal is to ensure that every MI Soldier is actively engaged in the fight against a complex and adaptive enemy, whether deployed or at home. In the years ahead, as the regional alignment of Army units increases, our Foundry platforms will provide countless opportunities for our Soldiers to contribute, assisting Army 2020's rotational forces with the execution of their regional missions, while sustaining a corps of Army Intelligence professionals who are better prepared for deployment, possess greater functional and regional expertise, and are more closely linked to the broader intelligence community."*** [4]

IROC–The Dragoon Way

> ***It is impossible to overstate the importance of the DISE's work. Their ability to fuse various sources of intelligence, out-of-contact, and provide a weekly assessment of critical information requirements is simply phenomenal. The first report I received from the DISE I assumed came from the intelligence team in theater. I had no idea the real work was accomplished 2,000 miles away.***
>
> ***Colonel D.A. Sims, 77th Colonel of the Regiment***



As 2 CR was preparing for deployment under a stringent force cap in late 2012, it became evident early on that the Regiment could not deploy its full complement of combat arms Soldiers and enablers. Although the Regimental staff had to plan to operate with limited enablers, because of IROC, the IWFF could continue to provide in-depth threat analysis, support to situational understanding, and support to targeting, in two geographically separated locations–Bavaria, Germany and Kandahar, Afghanistan.

In accordance with both a Regiment and USAREUR directive, 2 CR's MI Troop, also known as Maverick Troop, initiated plans to execute intelligence reach. Based on the IROC design and with the assistance of USAREUR, the EFP, and the Joint Multinational Training Command, Maverick Troop established the Dragoon Intelligence Support Element, known as the DISE, which would operate out of the IROC-enabled EFP in Grafenwoehr, Germany.

Task organizing MI Troop to meet mission requirements was the first priority. Nearly 40 Maverick Soldiers were reassigned to the Regimental intelligence section (and select infantry squadrons) in order to support operations forward. These Soldiers included a platoon to fly and maintain the RQ-7 Shadow Unmanned Aerial Systems, two Human Intelligence Collection Teams (HCTs), Signals Intelligence (SIGINT) Soldiers to augment the Cryptologic Support Team, a select number of intelligence analysts to work in the Brigade Intelligence Support Element, and a team of geospatial intelligence analysts.

Current MI Troop Capabilities:

- Commander's Intel Update Brief
- White & Red Targeting
- VHF Analysis and Production
- Imagery Analysis
- Source Production Review
- HUMINT Report Management
- Dragoon Ready Reserve Intel Support
- Afghan Governance Analysis
- Data Analysis and Research

The DISE was initially established during the Regiment's Mission Readiness Exercise (MRE) in March 2013, operating out of the Regiment's Sensitive Compartmented Information Facility. Testing the intelligence reach concept during a training event allowed the Troop to develop standard operating procedures, test networks, and more importantly identify the systems, networks, and hardware needed to become IROC-enabled.

Incorporating lessons learned from the 4th Stryker BCT, 2nd Infantry Division and from the Regiment's MRE, Maverick Troop worked with Mr. Stimpson and his staff to transform the already robust Foundry Platform into an IROC-enabled facility.[5] Network infrastructure was considerably expanded to include Combined Enterprise Regional Information Exchange, secure video teleconference (SVTC), multiple Distributed Common Ground Systems, and other secure networks needed for various intelligence disciplines. Mr. Stimpson described the effort as, "leveraging equipment organic to the Troop and tailoring the Foundry Platform to meet the needs of 2 CR in order to best support the deployed Soldiers."

Photo by WO1 Jamie Garcia, MI TRP, 2 CR

Camp Aachen, Tower Barracks, Germany

Concurrent with the transformation of the EFP into an IROC-enabled facility, DISE Soldiers increased the Regimental Commander and staff's situational awareness regarding the operational environment well before the scheduled Transfer of Authority. Assessments included intelligence estimates on threats, the fluid political environment, and likely enemy reactions to Relief in Place operations. This facilitated the squadron commanders and their staffs to further refine their own intelligence estimates regarding their unit's area of operations.

Maverick Troop assumed the intelligence reach mission in the summer of 2013 with four intelligence disciplines: All-Source, HUMINT, SIGINT, and GEOINT. The mission:

> ***"MI Troop, 2 CR, in direct support to Combined Task Force (CTF) Dragoon, establishes the Dragoon Intelligence Support Element (DISE) and MI Ready Reserve consisting of Multi-Discipline Intelligence capable of processing, exploiting and disseminating intelligence from the European Foundry Platform until mission complete in order to support CTF Dragoon's mission."***

The DISE serves as a fusion/analytical center and provides the Regimental Commander detailed Intelligence Preparation of the Battlefield products and intelligence estimates which primarily support the planning of future operations. These products are often "sanitized" by trained foreign disclosure officers in order to release them to the

Afghan National Security Forces (ANSF). This supports the Regimental mission to "advise and assist" ANSF and to increase their operational effectiveness by sharing intelligence. Conversely, the deployed Regimental intelligence section focuses on the immediate threat and current operations; plans and directs intelligence collection efforts, and publishes daily and weekly intelligence summaries. MAJ Patrick Miller, 2 CR's Intelligence Officer, explains it best when he stated, "the DISE augments our deployed force by taking on recurring intelligence production requirements allowing our forward intelligence Soldiers the flexibility to handle our current enemy situation and threat."

DISE Functional Capability:

✦ Access to coalition networks
✦ Multidiscipline Intelligence
✦ Live Collection/Fusion Capability
✦ Near real time Situational Awareness

DISE all-source analysts use information from all disciplines and available sources to create an intelligence estimate for the Commander. All-source analysts comprise the majority of the Soldiers in the DISE and are divided into four groups: Enemy Networks and Diagrams, Lines of Communication, Governance, and Situational Templates, each led by an experienced noncommissioned officer. These groups are primarily responsible for leveraging the single-source disciplines to create a weekly multi-intelligence layered product, called the Commander's Intelligence Update Brief (CIUB). The CIUB is a comprehensive intelligence estimate briefed directly to the Regimental Commander once a week, and is designed to answer the Commander's Priority Intelligence Requirements.

Out of the four disciplines in the DISE, HUMINT Soldiers perform their Operational Management Team (OMT) duties far from their comfort zones and in a radically different way than doctrine dictates. Maverick Troop deployed two HCTs, trained to extract information from human sources and subsequently write Intelligence Information Reports. Doctrinally, the OMT is designed to provide operational and technical control and guidance to the deployed HCT. It is also designed to be located where it can provide oversight of team operations and best support the dissemination of tasking, reports, and technical data between the unit and the deployed collection assets. The OMT relies on continuous communication with the deployed HCTs in order to ensure all administrative and operational reports are accurate and adhere to strict regulations.

More than any other intelligence discipline in the DISE, the SIGINT section is just as capable, if not more capable, of producing intelligence in an IROC construct, unconstrained by geographic proximity. This is primarily because SIGINT relies exclusively on technology, automations, and U.S. based servers, allowing SIGINT collection and analysis to take place virtually anywhere with adequate systems and networks. This makes a permanent facility with secure, robust, and reliable connectivity an ideal location to conduct SIGINT operations.

SIGINT Soldiers in the DISE maintain the same capabilities as SIGINT Soldiers deployed, with few exceptions. In the DISE, SIGINT concentrates on report publishing while SIGINT forward concentrates more on targeting and current operations. In the DISE, SIGINT Soldiers are armed with the Joint Worldwide Intelligence Communications System as well as National Security Agency access, all with the respective programs to perform their mission. Forward deployed SIGINT Soldiers have further access to various programs and with the necessary adjustment, SIGINT could exclusively perform their mission geographically separated from the operational environment.

GEOINT, similar to SIGINT, is another ideal intelligence discipline for an IROC construct. GEOINT relies entirely on internal systems and programs in order to adequately exploit and analyze imagery and geospatial information; therefore, GEOINT is capable of performing its mission unconstrained by geographic boundaries. The DISE currently leverages GEOINT for terrain analysis, base defense products, moving target indicator, and forensic analysis.

Regardless of the DISE's ability to provide intelligence in an IROC construct, it is important to understand that while intelligence reach augments a forward deployed intelligence section, it does not replace it. In 2 CR's experience there are two significant limitations that hinder the DISE's capabilities and effectiveness.

First, because of the DISE's considerable geographic separation from the Regimental headquarters, direct collab-

Photo by WO1 Jamie Garcia, MI TRP, 2 CR

Camp Aachen, Tower Barracks, Germany

Photo by WO1 Jamie Garcia, MI TRP, 2 CR

Camp Aachen, Tower Barracks, Germany

orative intelligence sharing between the DISE and forward elements is exponentially more difficult than if the DISE was in close proximity. A more holistic understanding of the environment and threats therein is achieved though both formal and informal meetings between staff officers and commanders, maneuver units (to include Special Operations Forces), and civilians, who are experts in various fields. This is most apparent with enemy network analysis. By not having a direct collaborative effort with other analysts, the DISE's ability to analyze elaborate, fluid enemy networks is not as effective.

Secondly, the DISE is heavily reliant upon dependable communications connectivity, along with the proper and necessary automations support. Ensuring that sufficient communications technology has been obtained to enable constant information flow between two separate domains, USAREUR and Afghanistan, remains a critical challenge to overcome. Using Secret Internet Protocol Router Network, online portals, Voice over Internet Protocol, and SVTC, are the most effective use of communications.

Despite these limitations, 2 CR's DISE has been an enormous success and continues to exceed initial expectations. 2 CR's intelligence team is paving the way for the future application of tactical intelligence support. Within the next year, 2 CR's Foundry 2.0 based mission will be the foundation for the Multi-National IROC in Europe where various intelligence professionals from allied nations will collectively work to provide intelligence in support of North Atlantic Treaty Organization (NATO) missions.· Colonel Jim Lee, USAREUR G2, explains, "In developing 2 CR's IROC, we have created a capability that will be used by United States and NATO forces alike in training and increasing intelligence capabilities in a post-International Security Assistance Force environment. USAREUR is on the leading edge of training multinational forces capabilities and this intelligence innovation will allow us to continue improving our intelligence interoperability and capacity in live environment training venues well into the future."

Going Forward

As the Army prepares to defeat hybrid threats, IROC and Foundry 2.0 will be critical components for mission success. The future operational environment will be diverse, complex, and demanding, testing the intelligence expertise of the U.S. military. The Army MI Corps is prepared for the future with IROC, ensuring our commanders are armed with the best available intelligence before and during combat operations. With IROC, MI Soldiers and units across the Army will have a direct and profound influence on combat operations no matter where they are located. As Colonel Megill so aptly stated, "the commitment of Soldiers to the fight is no longer a matter of proximity." That is an exceptionally powerful statement for Army Intelligence.

Endnotes

[1] IROC is an emerging concept currently being developed by FORSCOM. This article only discusses select portions of IROC. The Army is still validating the requirements for IROC and the concept is pending publication in key regulations and policy.

[2] LTG Mary A. Legere, *"Army Intelligence in Support of a Regionally Aligned Army: No Cold Starts and No MI Soldier at Rest,"* Association of the United States Army (AUSA) Army Greenbook, October 2013, 1.

[3] Brigadier General Robert L. Walter Jr., *"Overview Briefing for National Defense Industrial Association (NDIA)"*, April 2013. This was a presentation delivered to the NDIA and discussed the future of intelligence.

[4] Legere, "Army Intelligence 2020: Enabling Decisive Operations While Transforming in the Breach," *Army Magazine*, October 2012, 169.

[5] 2 CR relieved 4-2 SBCT in Kandahar Province in the summer of 2013. Simultaneously, MI Troop conducted a Relief in Place with 4-2 SBCT's intelligence reach who conducted operations from Joint Base Lewis-McChord.

[6] The USAREUR goal is to establish the Multi-National IROC by spring 2014 and fully operational by winter 2015.

References

U.S. Army Forces Command IROC Concept of the Operation, Deputy Chief of Staff, G-2, December 2012.

ADP 2-0, Intelligence, August 2012.

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

FM 3-22, Army Support to Security Cooperation, January 2013.

AR 350-32, Army Foundry Intelligence Training Program, June 2010.

TC 7-100, Hybrid Threat, October 2010.

"Army Intelligence 2020 and Beyond," Department of the Army, Military Intelligence (DAMI) website at http://www.dami.army.pentagon.mil/g2Docs/StratComms/2013%2003%2012%20Intel%202020%20Releasable%20to%20Website.pdf.

AUSA Torchbearer National Security Report, July 2007.

Captain Patrick C. Mulloy, U.S. Army, is currently serving as the Commander of the MI Troop, 2d Cavalry Regiment at Rose Barracks, Germany. During his career, CPT Mulloy served in the 4th Infantry Division at Fort Carson as a Scout Platoon Leader and Troop Executive Officer where he deployed to Baghdad, Iraq. CPT Mulloy also served as a Squadron Intelligence Officer in 2 CR in southern Afghanistan. He holds a BS from Longwood University in Virginia.

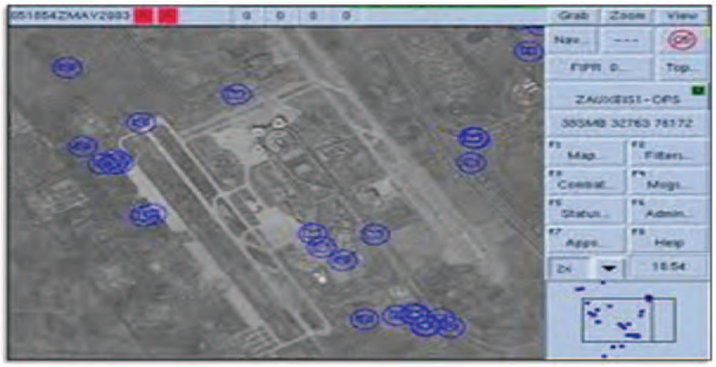
by Captains Luis Mendoza and Jinsuk Yum, First Lieutenant Daniel Jernigan, and Staff Sergeant Phillip Dontje

Modernizing and Streamlining ABCS through Integration of Google Earth

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

Introduction

Recently, the U.S. Army has transitioned from primarily training to conduct counterinsurgency operations to conducting decisive action operations. Decisive action operations encompass offensive, defensive, and stability operations, sometimes conducted simultaneously. In order to plan and execute decisive action operations, units require systems that are easily accessible, user friendly, and compatible with one another. The Army developed the Army Battle Command System (ABCS) which included Command Post of the Future (CPOF), Distributed Common Ground System-Army (DCGS-A), and Force XXI Battle Command Brigade and Below (FBCB2), in an attempt to provide tools which would allow units to plan and execute missions, while providing a common operational picture for the force.



FBCB2 graphics.

The reality is that these systems were either designed for counterinsurgency (CPOF and DCGS-A) or were never modernized (FBCB2). These systems were also complicated and required days and weeks or training just to use them, not to mention the significant contractor support to setup and maintain. Within decisive action, units must be able to move a command post within a few hours rather than establish them for an entire year in the same location. Battle tracking may also have to occur on the move, many times with no connectivity.

Aside from FBCB2, the current systems cannot provide this capability without robust bandwidths. Graphics on FBCB2 have low resolutions, poor quality imagery, and maps that are difficult to read. Many of today's Soldiers have either grown up with or adapted to new technology and have the ability to visualize space and time in a three-dimensional environment on a screen. Three-dimensional visualization allows for better analysis and situational awareness. With fiscal resources becoming more constrained, the Army needs to move towards utilizing what is already available with current hardware and change its software. If the Army were to move towards making Google Earth the primary means of portraying maps, graphics, enemy situations, and plans, it would be a significant improvement on the force's capabilities, without the need for significant research and development.

CPOF

The CPOF was introduced to provide units with a command operational picture and tools to conduct digital mission analysis. There have been several glaring shortfalls for the system however. Units have stated that CPOF is rarely utilized to its full extent due to lack of training. CPOF requires 80 hours of formal training to be able to utilize it to its full potential. For its intended purpose, the end user would likely be a Battle Captain/NCO, Planner, S3, or S2, all of whom rarely have the time to attend a two week course. What normally ends up occurring is that a PFC or SPC is sent to the course and expected to use the system as an RTO, but is immediately removed from the system to man a radio.

CPOF is also designed to allow a commander and the staff to make decisions via rapid dissemination of real-time information in their battlespace. This immediate exchange of information is inhibited due to limited bandwidth in the field. During decisive action operations bandwidth is only available when connectivity can be established, which may be only for a few hours at a time. Another bandwidth issue is the inability to save overlays when the system is offline or disconnected from a CPOF server. When a connection is re-established the data is lost as the system synchronizes.

Commands choose not to use CPOF because it tends to get overloaded fairly frequently, which then causes the system to crash and can affect all CPOFs on the network. The commander and the staff are not making decisions based on the information contained on the CPOF system. Rather they use it to take a snapshot of a map and build products using PowerPoint, essentially making the system a glorified map producer. Decisions are usually made from ordinary SIPRNet systems and PowerPoint slides or maps with acetate.

The system was also designed to provide three-dimensional visualization, however this feature only runs when the network is connected and takes up so much bandwidth that most units prefer not to employ it. The Army has a computer system that is not being properly utilized because of minimal bandwidth and lack of training. Commanders, staffs, and operators are not fully trained on this system because it is not very easy to use. Limited bandwidth has not only limited the CPOF to being a map picture producer, it has also limited DCGS-A, the system developed specifically for intelligence analysts.

DCGS-A

DCGS-A was designed to allow intelligence analysts to build databases and for the computer to build graphs, charts, and overlays, saving the analyst valuable time to conduct analysis. Issues with the system become evident from the moment analysts are trained. Training consists of a 40 to 80 hour course. Upon completion, most participants do not fully comprehend the detailed instructions that were taught during the training. Advance knowledge of the system requires additional time one-on-one with a certified instructor. Outside of the classroom the system is not easy to establish and maintain. DCGS-A relies on its own servers, which only a few qualified personnel in a given unit can setup, maintain, and support. Due to the lack of constant support and maintenance the system frequently freezes and crashes, making its use, particularly in decisive action operations, impractical for intelligence personnel to utilize.

To combat these issues, units have to rely heavily on external contractor support to maintain their systems. Relying on contractor support presents several challenges, particularly in decisive action environments. These challenges include, but are not limited to, coordinating transportation and security for the contractor. While contractor support at the strategic level may be tolerable, it is impractical and a hindrance at the brigade and battalion level. Even when the system is operational, there are still significant issues that arise, including the loss of products and data on servers that seem to occur almost randomly, slow map interface which makes working on the system nearly intolerable, and the need to constantly monitor and setup network interface.

Many analysts in Operations Iraqi Freedom/Enduring Freedom (OIF/OEF) would utilize Google Earth or the Tactical Ground Reporting System for mapping and analysis as their interface, speed, and ease of use significantly outperformed the Multifunction Workstation interface that the DCGS-A utilizes. When it comes to compatibility, DCGS-A was supposed to be able to send overlays to CPOF. The intricacies in establishing a network that would allow this has required significant support from contractors for both systems working side by side for weeks at a time.

FBCB2

In order to create a method for commanders to track their forces in real time, the Army developed FBCB2. Though it is a system that is still useful, it has significant drawbacks. FBCB2 requires users to undergo a 40 hour course that instructs the basics of operating the system over nine modules of training. The system was first used in military operations in 1998. While the system was advanced for the time, it is now outdated and rarely serves its purpose. Fifteen years after its introduction, the system has not been significantly updated, even with over ten of those years in counterinsurgency operations. Maps and graphics on FBCB2 are of poor quality and low resolution, making terrain difficult to see. Due to its dated interface, creating operations graphics can be extremely time consuming.

User interface is also known to be confusing, even for those who attend the 40 hour course. This is partly due to the majority of training taking place in a "white box" environment. White box training is conducted on a commercial computer that has the FBCB2 software loaded into it to replicate the functions of an FBCB2 "green box" system. Once Soldiers transition to using the system in a field environment or "green box," they struggle to adapt to the clunky interface in a track or wheeled vehicle platform. FBCB2 can also have GPS lag times of up to five minutes, which results in units utilizing it as a text messaging platform, not a force tracking tool. While FBCB2 has had success in the Army, operations in Afghanistan and Iraq have highlighted several of the system's limitations when employed in tactical environments.

The first was the system's interoperability with similar systems utilized by other armed forces of the military. This was evident in Iraq, especially during the initial push for Baghdad as both Army and Marine Corps elements were involved in combat operations in the city. As the Army was pushing north on the west side of the Tigris/Euphrates River Valley the FBCB2 failed to identify and exchange digital information with Marine Corp elements pushing north on the east side.

Internally within the Army, different units task organized under other units can also pose challenges for the system as each unit may have different configurations for the system's setup, such as its hard drive. This in itself requires additional time and planning for a unit to ensure the systems can communicate with each other. Furthermore, several units still rely on SINCGARS or EPLRS to share data with other users on the system. This reliance restricts the unit's capability to receive and transmit information over long distances due to constraints of terrain and line of sight communication. These FBCB2 systems can support platoon and company operations on flat land but fail to account for terrain and distance.

Google Earth

Overall there is no base line or common operating procedure for every system to operate so that each system communicates effortlessly with other systems. Although CPOF, DCGS-A, and FBCB2 were all developed for different reasons and developed separately with the intention of making them compatible at some point, the Army missed its mark. The software for these systems, which was written exclusively for the Army's use, was poorly designed and built. The fix then is software, the software is Google Earth.

Google Earth is a virtual globe, map, and geographical information program that was originally called EarthViewer 3D. It was created by Keyhole, Inc., a company partially funded by the Central Intelligence Agency and acquired by Google in 2004. One of the primary benefits of using a program such as Google Earth is the commercial availability of the product and the development process inherent in software that is so widely available to a mass audience. When software is subject to the widest possible user base, the requirements leveraged on the software are numerous and varied.

In Google Earth's case, map and imagery data effectively combines with GPS latitude and longitude data. That is then presented to the user in an aesthetic manner while constantly maintaining program metadata and map updates, regardless of whether the computers is connected to the Internet or not. Live streams of situational overlay data can then combine with vehicle movement information and provide a near-real-time picture of a given environment. The streamlining comes from having to make the software do many tasks with a finite set of resources.

The efficiency comes from the need to have the components of the program integrate well internally and externally through effective and compartmentalized source code and simplified data-basing interfaces. When computers have only a certain amount of battery life, CPU processing power, Random Access Memory (RAM) space, graphics processing power, and Internet bandwidth, this is a daunting task, but one that Google Earth performs very well.

Furthermore, all of these resource constraints are what Army units are subject to on a regular basis. Automations hardware is consistently outdated and lacking processing power. Bandwidth is often limited in remote sites. But the need to collect, compile, and share information with a unit and among friendly forces is a basic need for battle tracking in a fast-paced operational environment. Google Earth's ability to do this better than any current program of record system is its inherent origin as publicly available and usable software.

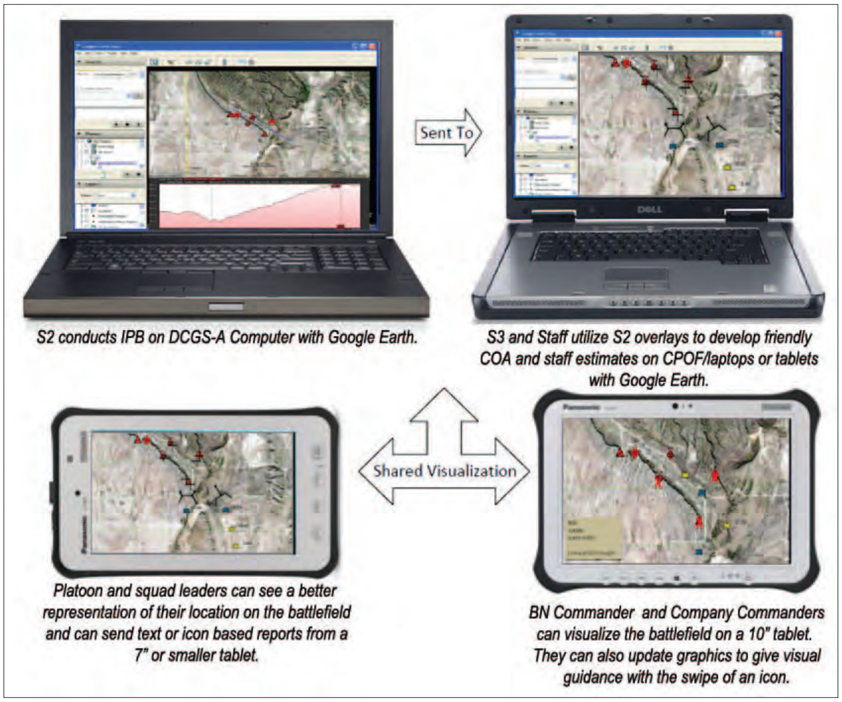
Such a program quickly evolves through the mechanisms stated above, to reach a level of effectiveness that cannot be achieved by software and hardware combinations that are isolated and used only by limited segments of the government and DOD. A good example of this is the current inability of all the ABCS to consistently and effectively interface with each other without an exorbitant amount of resources, as well as civilian contractor support. Google Earth works on a 7 year old laptop with only 2 gigabyte of RAM.

Google Earth is available on all levels of classified systems. The program does not require any special equipment; just about any computer in the Army can have Google Earth installed in minutes. The program is compatible with all Windows based operating systems currently being used by the Army from Windows 2000 to Windows 7 and even Linux. Users do not requiremore than 8 hours of training to understand advanced functions of Google Earth. Its

Google Earth integrated into GPS unit of 2011 Audi A8.

user interface is also easy enough that just about anyone can learn to use it just by trying its different functions and features. Users will quickly find that the interface in Google Earth is similar to PowerPoint, thus it is familiar. Several units utilized Google Earth during OIF and OEF. Nearly all of the functions performed by CPOF and DCGS-A can be provided by Google Earth at this point.

The possibilities with a Google Earth based mobile platform can take the workings of battlefield command to a new level. Current commercial vehicles like the Audi A8 have built in Google Earth functionality in the place of a typical GPS. With new phone and handheld GPS technology, the mobile capabilities can be given down to the squad and even team leader level as seen in Figure 1. What is key to this concept is that an overlay, with enemy and friendly graphics, which was originally what FBCB2 would provide, would now be available to all leaders on the battlefield. Off the shelf units can provide the visual capabilities, while modifications to the hardware can make the systems secure.



S2 conducts IPB on DCGS-A Computer with Google Earth.

S3 and Staff utilize S2 overlays to develop friendly COA and staff estimates on CPOF/laptops or tablets with Google Earth.

Platoon and squad leaders can see a better representation of their location on the battlefield and can send text or icon based reports from a 7" or smaller tablet.

BN Commander and Company Commanders can visualize the battlefield on a 10" tablet. They can also update graphics to give visual guidance with the swipe of an icon.

Figure 1. Visual representation of Google Earth architecture on the battlefield.

Conclusion

The Army has attempted to develop the best systems for providing tools that would give a commander and the staff the best visual representation of the battlefield. The lack of easy to use and reliable software that came with the equipment has made it mostly ineffective. Google Earth is easy to use, easy to train, and does not require always on broadband or specialized equipment to function properly. It is for these reasons that the Army should seriously consider revising the current systems and maneuver towards further developing Google Earth for military use.

Raider University Project III, Tier III, Group III
1st Battalion, 22nd Infantry Regiment
1st Armored Brigade Combat Team, 4th Infantry Division

Raider University is a comprehensive professional development program created within 1ABCT, 4ID, focusing on building operational adaptability in Soldiers.

CPT Luis Mendoza was commissioned in 2007 as a 35D All Source Intelligence Officer and graduated from the MI BOLC and the MICCC. He served as the Battalion S2X and is currently the Battalion S2.

CPT Jinsuk Yum enlisted 1999 as 31S-1C (now 25S) Satellite Network Controller and was commissioned through the U.S. Military Academy. He graduated from Signal BOLC and has held positions as the Brigade Automations Management Officer and Brigade Information Systems Management Officer. He currently serves as the Battalion S6.

1LT Jernigan enlisted in 2008 as an Intelligence Analyst. He attended the Warrior Leader Course, Officer Candidate School Graduate 2010 (Branched MI, Branch Detail IN), Infantry BOLC, and the Mechanized Leader's Course. He has served as a Rifle Platoon Leader and is currently the battalion's Assistant S2.

SSG Phillip Dontje enlisted in 2006. He attended the Warrior Leader and Advance Leader Courses, as well as the CPOF and DCGS-A courses. He has served as a Geospatial Intelligence Analyst, and in the Area Support Group-Kuwait as Information Security NCOIC; Alternate KU Security Manager; Strategic and Tactical KU Intelligence Analyst; Intelligence Sergeant, and Intelligence CUOPS NCOIC. He is a Raven Master Trainer.

Interface and display capabilities of a modern handheld GPS unit (Earthmate GPS PN-40).

Army Aerial Intelligence, Surveillance, and Reconnaissance 2020

by Captain Mark A. Swiney

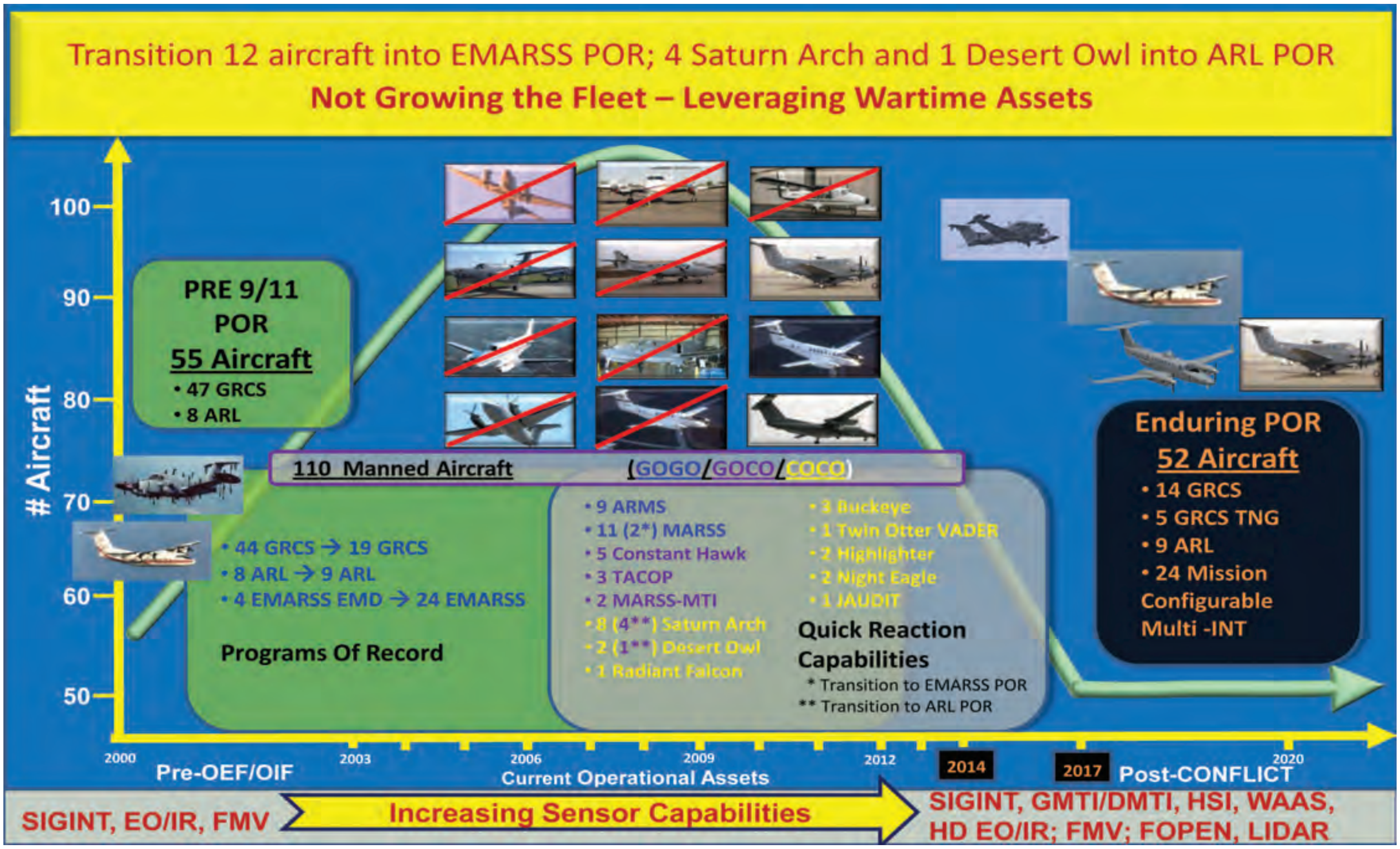
Introduction

The Army's manned and unmanned Aerial Intelligence, Surveillance, and Reconnaissance (AISR) fleet has historically consisted of a mix of unique single-discipline capabilities that process, exploit, and disseminate the intelligence collected. These legacy systems have been highly effective in a variety of worldwide deployments, but are not adequately adaptable with analytical elements for changing operational environments. Current and emerging threats have demonstrated an ability to take advantage of expanded communications technology, enhanced cover and concealment techniques, and vulnerabilities in traditional sensing capabilities.

Future AISR capabilities must expand on lessons learned in recent conflicts and deliver mobility, endurance, persistent coverage and advanced sensing capabilities while providing tailored and dynamically responsive support to ground maneuver commanders. The Army's AISR strategy through 2020 is designed to ensure mission success by having the ability to rapidly adapt to changing tactical conditions, while still providing maximum value in a fiscally constrained environment.

AISR Foundational Requirements

Geographic Combatant Commander Urgent Operational Needs in Afghanistan and Iraq resulted in deployment of more than 40 quick reaction capability (QRC) ISR systems that were rapidly acquired or built and deployed as quickly as feasible. These systems included new sophisticated sensors which provided an exponential increase in total collection coverage and demonstrated the value of multi-sensor systems with onboard processing, exploitation, and dissemination (PED) for rapid sensor cross-cue and target confirmation. With the drawdown of forces in U.S. Central Command's (USCENTCOM) Iraq and Afghanistan areas of responsibility, the Army will divest the majority of those QRC systems, but harvest the investment made in technology in order to transition their unique capabilities into the base force and avoid the cost of procurement of new production systems (See Figure 1).



Transition 12 aircraft into EMARSS POR; 4 Saturn Arch and 1 Desert Owl into ARL POR

Not Growing the Fleet – Leveraging Wartime Assets

PRE 9/11
POR
55 Aircraft
- 47 GRCS
- 8 ARL

110 Manned Aircraft (GOGO/GOCO/COCO)

- 44 GRCS → 19 GRCS
- 8 ARL → 9 ARL
- 4 EMARSS EMD → 24 EMARSS

Programs Of Record

- 9 ARMS
- 11 (2*) MARSS
- 5 Constant Hawk
- 3 TACOP
- 2 MARSS-MTI
- 8 (4**) Saturn Arch
- 2 (1**) Desert Owl
- 1 Radiant Falcon
- 3 Buckeye
- 1 Twin Otter VADER
- 2 Highlighter
- 2 Night Eagle
- 1 JAUDIT

Quick Reaction Capabilities

* Transition to EMARSS POR
** Transition to ARL POR

Enduring POR
52 Aircraft
- 14 GRCS
- 5 GRCS TNG
- 9 ARL
- 24 Mission Configurable Multi -INT

SIGINT, EO/IR, FMV
Increasing Sensor Capabilities
SIGINT, GMTI/DMTI, HSI, WAAS, HD EO/IR; FMV; FOPEN, LIDAR

Figure 1. Manned Aerial ISR Surge.

The QRC systems were able to help identify gaps documented in the Joint Direct-Support Airborne Intelligence, Surveillance, and Reconnaissance (JDSAISR) Initial Capability Document (ICD) and the Counter-Concealment Sensing (C-CS) ICD, documents designed to focus the Army on acquiring the capabilities needed for the future. These ICDs are the foundational documents for the Joint Capabilities Integration Development System (JCIDS), the formal U.S. Department of Defense (DoD) procedure which defines acquisition requirements and evaluation criteria for future defense programs. They underpin the overall AISR 2020 strategy (illustrated in Figure 2), which is synchronized with current Defense Planning Guidance and optimized to mitigate operational gaps not satisified by other joint ISR systems.

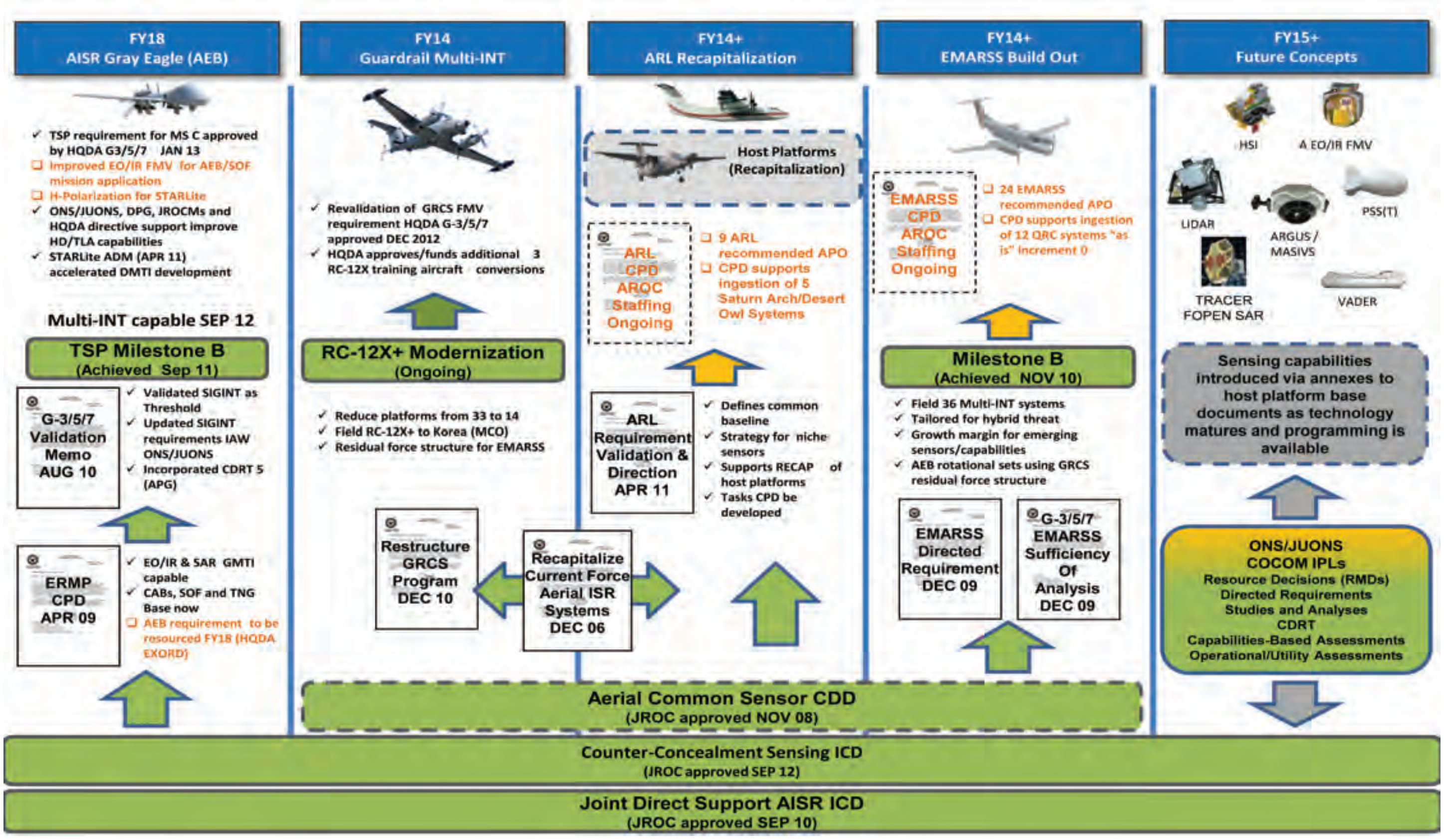

FY18
AISR Gray Eagle (AEB)
✓ TSP requirement for MS C approved by HQDA G3/5/7 JAN 13
□ Improved EO/IR FMV for AEB/SOF mission application
□ H-Polarization for STARLite
✓ ONS/JUONS, DPG, JROCMs and HQDA directive support improve HD/TLA capabilities
✓ STARLite ADM (APR 11) accelerated DMTI development
Multi-INT capable SEP 12
TSP Milestone B
(Achieved Sep 11)
G-3/5/7 Validation Memo AUG 10
✓ Validated SIGINT as Threshold
✓ Updated SIGINT requirements IAW ONS/JUONS
✓ Incorporated CDRT 5 (APG)
ERMP CPD APR 09
✓ EO/IR & SAR GMTI capable
✓ CABs, SOF and TNG Base now
□ AEB requirement to be resourced FY18 (HQDA EXORD)
FY14
Guardrail Multi-INT
✓ Revalidation of GRCS FMV requirement HQDA G-3/5/7 approved DEC 2012
✓ HQDA approves/funds additional 3 RC-12X training aircraft conversions
RC-12X+ Modernization
(Ongoing)
✓ Reduce platforms from 33 to 14
✓ Field RC-12X+ to Korea (MCO)
✓ Residual force structure for EMARSS
Restructure GRCS Program DEC 10
Recapitalize Current Force Aerial ISR Systems DEC 06
FY14+
ARL Recapitalization
Host Platforms
(Recapitalization)
ARL CPD AROC Staffing Ongoing
□ 9 ARL recommended APO
□ CPD supports ingestion of 5 Saturn Arch/Desert Owl Systems
ARL Requirement Validation & Direction APR 11
✓ Defines common baseline
✓ Strategy for niche sensors
✓ Supports RECAP of host platforms
✓ Tasks CPD be developed
FY14+
EMARSS Build Out
EMARSS CPD AROC Staffing Ongoing
□ 24 EMARSS recommended APO
□ CPD supports ingestion of 12 QRC systems "as is" increment 0
Milestone B
(Achieved NOV 10)
✓ Field 36 Multi-INT systems
✓ Tailored for hybrid threat
✓ Growth margin for emerging sensors/capabilities
✓ AEB rotational sets using GRCS residual force structure
EMARSS Directed Requirement DEC 09
G-3/5/7 EMARSS Sufficiency Of Analysis DEC 09
FY15+
Future Concepts
HSI
A EO/IR FMV
LIDAR
ARGUS / MASIVS
PSS(T)
TRACER FOPEN SAR
VADER
Sensing capabilities introduced via annexes to host platform base documents as technology matures and programming is available
ONS/JUONS
COCOM IPLs
Resource Decisions (RMDs)
Directed Requirements
Studies and Analyses
CDRT
Capabilities-Based Assessments
Operational/Utility Assessments
Aerial Common Sensor CDD
(JROC approved NOV 08)
Counter-Concealment Sensing ICD
(JROC approved SEP 12)
Joint Direct Support AISR ICD
(JROC approved SEP 10)

Figure 2. Roadmap to AISR 2020.

AISR System Capabilities

Current and future AISR sensing capabilities include:

- Full Motion Video (FMV) camera with High-Definition (HD) Electro-Optic/Infra-Red (EO/IR).
- Wide Area Aerial Surveillance (WAAS) imaging.
- Radar-based Ground and Dismount Moving Target Indicator (GMTI and DMTI).
- Ground and Foliage Penetrating (GPEN and FOPEN) radars.
- Synthetic Aperture Radars (SAR) for high-resolution imaging.
- Light Detection and Ranging (LIDAR) using light waves instead of radar waves.
- Hyper-Spectral Imaging (HSI) that analyzes spectral data reflected or emitted along the electromagnetic spectrum.
- Communications Intelligence (COMINT) intercepts targeting communications.
- Electronic Intelligence (ELINT) collection of radio frequency emanations.
- High-resolution color mapping sensors.

This family of interoperable sensors will be hosted on a variety of AISR platforms, including:

- Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS).
- Airborne Reconnaissance Low–Enhanced (ARL-E).
- Guardrail Common Sensor (GRCS).
- MQ-1C Gray Eagle.

All sensors will be fully integrated with the "all encompassing" Defense Intelligence Information Enterprise (DI2E) framework. The PED process is facilitated by Distributed Common Ground System-Army (DCGS-A) which provides common software and tools. DCGS-A is the Army's primary system that enables rapid sharing and dissemination of data, information, and processed intelligence to all echelons.

AISR Platforms

EMARSS. EMARSS is a worldwide self-deployable AISR system designed for timely, accurate, assured support to tactical forces over the full spectrum of operations. The MC-12S EMARSS is a new program that evolved from the QRC systems fielded in support of Operations Iraqi Freedom and Enduring Freedom. The MC-12S includes two onboard DCGS-A compliant workstations with sensor operators that communicate through direct downlink to tactical units/commanders while the aircraft detects, identifies, tracks, and reports high value targets (HVTs) and high value individuals (HVIs). The first four systems are currently in developmental testing at Aberdeen Proving Ground, MD and will be fielded to an Aerial Exploitation Battalion (AEB) in 4QFY14.

The EMARSS strategy includes a total of twenty-four systems which are a mix of new-build EMARSS and transitioned QRC systems including five Constant Hawk systems, three TACOPS systems with LIDAR sensors, and four MARSS with EO/IR and COMINT sensors. Two of the MARSS platforms will also be equipped with the Vehicle and Dismount Exploitation Radar (VADER). These QRC systems will retain their unique sensing capabilities and configurations until upgrades are performed to meet EMARSS Key Performance Parameters (KPPs) and other system requirements.

EMARSS is intended to provide previously unachievable levels of situational awareness directly to tactical commanders at the lowest levels where forces are in direct contact. As an example, EMARSS can transmit FMV and other system-collected intelligence directly to supported units via Remotely Operated Video Enhanced Receiver/One System Remote Video Terminal (ROVER/OSRVT), while simultaneously conducting tactical radio communications down to the squad level with Soldiers executing finishing operations as part of the Find, Fix, Finish, Exploit, Analyze, and Disseminate process.

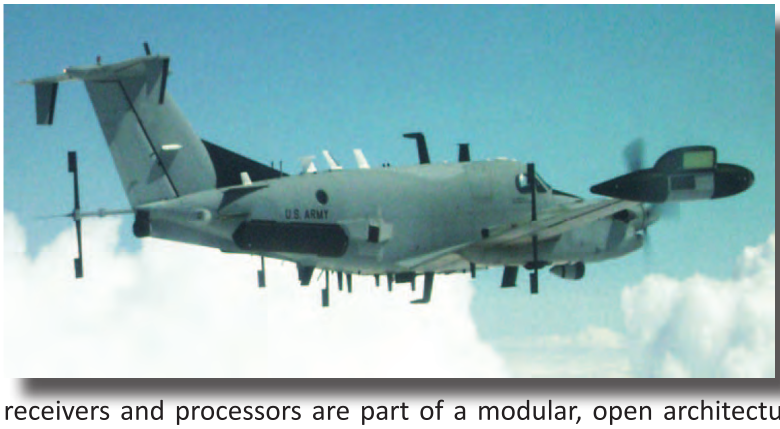
EMARSS will leverage DCGS-A developments in common software for its sensor operator interface and intelligence processing/fusion capabilities via SIPRNET and NSANet networks. Connectivity to the global PED enterprise will be provided by the DoD standard Common Datalink for line of sight (LOS) links to the DCGS-A Operational Ground Station, or via wideband Ka/Ku-band SATCOM when beyond line of sight (BLOS) links are required. The Battlefield Information Collection and Exploitation Systems will similarly be leveraged via DCGS-A to provide for multinational intelligence sharing. The EMARSS modular open-system architecture will leverage investments and developments in other programs for future upgrades to its COMINT and Imagery Intelligence (IMINT) sensor and PED capabilities

EMARSS will be assigned to AEBs within the U.S. Army Intelligence and Security Command (INSCOM), which will provide command and control, mission planning, sustainment support, and tailored EMARSS deployment packages in support of worldwide missions in accordance with standard joint and Army tasking processes. EMARSS will support collection requirements of brigade combat teams (BCT) and other echelons across the full range of military operations (ROMO).

ARL-E. The ARL-E program is an evolution of the current ARL system that was first fielded in 1991. The ARL-E is a multi-INT system that provides the capability to detect, locate, classify, and track surface targets in day/night, near-all-weather conditions with a high degree of timeliness and accuracy. The current ARL program is based on the De Havilland DHC-7 platform and includes 4 onboard operator positions with EO/IR, COMINT and SAR/GMTI sensors. The ARL-E program will include the transition of five more modern DHC-8 300 series QRC platforms and their associated sensors into the program. These QRC systems will be modified to meet ARL KPPs and other requirements, with delivery beginning in FY17. The ARL-E Capability Production Document, now in Army Requirements Oversight Council staffing, also calls for the acquisition of four additional DHC-8 platforms and sensors that will allow retirement of all current DHC-7 ARL systems by 2021.

The ARL-E provides broad-area surveillance and/or focused stare on targeted areas of interest while providing multi-sensor tactical overwatch of ongoing operations. Baseline ARL-E sensor capabilities include dual high-definition EO/IR with laser illumination/range finding and target designation, a tactical COMINT sensor, and a SAR/GMTI sensor. Additional sensing capabilities will include DMTI radar, LIDAR, wide area aerial sensor, penetrating radar (PENRAD), and high-resolution color mapping sensors. Individual platforms will share data via wideband LOS and BLOS data-links through the DCGS enterprise in order to maximize PED efficiency and effectiveness. The ARL-E platforms will also contain four embedded DCGS-A workstations and standard DCGS-A software applications. ARL-E onboard operators ensure responsive support to tactical commanders through a robust tactical communications suite. This allows direct broadcast of situational awareness and targeting data, with finished products to customers as low as the squad level to provide them with the information required to conduct tactical operations.

ARL-E will be assigned to Aerial Reconnaissance Battalions (ARBs) within INSCOM, which will provide command and control, mission planning, sustainment support, and ARL-E deployment packages configured with the ideal sensor for a particular region. Like EMARSS, ARL-E will support collection requirements of BCTs and other echelons across the full ROMO.



GRCS. Guardrail has been the Army's aerial COMINT and ELINT collection workhorse for more than 40 years. Over the last 10 years, fourteen of the GRCS systems were completely rebuilt and received a significantly upgraded Signals Intelligence (SIGINT) capability. The new COMINT subsystems maintain Guardrail's status as the Army's premier SIGINT collection system and include the baseline Enhanced Situational Awareness, the Communications High Accuracy Location System–Compact, as well as a variety of specialized components for advanced processing. These new airborne receivers and processors are part of a modular, open architecture that provides advanced processing and targeting of modern signals; it is easily upgradeable to keep the GRCS system relevant well beyond 2020.

In December 2012, the Army G3 validated a requirement to further upgrade these fourteen RC-12X systems with a high-definition EO/IR capability based on reduction of the number of EMARSS systems planned for fielding. Initial deliveries of the RC-12X with EO/IR capability will occur in late FY15, with all systems being upgraded by the end of FY17. This capability will enable a single RC-12X system tasked by the DCGS-A enterprise to rapidly cross-cue SIGINT geo-location to EO/IR imagery for target confirmation. The new necessity for cross-cueing will require training of flight profiles that differ from the singular COMINT approach employed in the past. These RC-12X systems will remain in the force while the older RC-12H, RC-12K, and RC-12N systems are replaced by EMARSS and retired. Like EMARSS, the GRCS systems are assigned to the INSCOM AEBs where they support collection requirements at BCTs and other echelons across the full ROMO.

MQ-1C Gray Eagle UAS. The MQ-1C, Gray Eagle UAS is the Army's medium altitude endurance (MAE) multi-INT information collection system. Originally designed as a replacement for the Hunter UAS, Gray Eagle fielding to the Army's AEBs has been delayed while those units were deployed in support of operations in Iraq and Afghanistan. Initial fieldings are now underway in the Army's combat aviation brigades and the 160th Special Operations Aviation Regiment (SOAR); Gray

Eagle is scheduled for AEB integration beginning in FY16 (replacing the Hunter UAS). Compared to the Hunter, the Grey Eagle provides increased on-station times, greater range capabilities, a larger sensor payload mix and increased targeting accuracy/timeliness. The MQ-1C was designed to deploy, communicate, survive, deliver effects, and remain responsive in real time to meet the commander's changing tactical requirements.

The Gray Eagle companies in the AEBs will be similar to the Hunter UAS companies they replace, though smaller than the Gray Eagle companies in the combat aviation brigades (CAB) and Army Special Operations. The MQ-1C payloads include an Electro Optical /Infrared/Laser Designator (EO/IR/LD) sensor and a SAR/GMTI radar. The AEB and SOAR variants will also host the Tactical SIGINT Payload (TSP); the CAB and SOAR versions can employ Hellfire missiles. Additionally, the Warfighter Information Network-Tactical (WIN-T) Communications Payload is planned for integration on all Gray Eagle aircraft. The combination of these payloads will provide the MQ-1C with a sensor/weapons package capable of supporting reconnaissance, surveillance, security, attack, and command and control missions. Future payloads envisioned for the MQ-1C include FOPEN, HSI, LIDAR and WAAS. The modular payload capability will enable tailoring of close-in and deep look sensors, with persistent surveillance across multiple disciplines while improving the commander's ability to build and enhance situational awareness and rapidly engage high-value/high priority targets.

Distributed PED Enterprise

All future aerial layer systems will be fully integrated into Army and Joint PED networks and share common analyst software tools across the distributed PED enterprise. This network-centric approach allows direct sharing of intelligence products with tactical commanders via SIPRNET, and provides analysts within the supported unit with the ability to query sensor databases directly in near-real time. The sensor data will be accessible through the global intelligence enterprise to enable analysts in Army and Joint PED centers to augment the onboard sensor operators with additional analysis and reporting.

The use of common networks facilitates cross-cueing of off-board sensors from other Army and Joint platforms and correlation of off-board and onboard collected data. In addition to this global network connectivity that ensures timely, accurate, and assured intelligence correlation and fusion, AISR systems are also equipped with the capability for secure voice communications and FMV broadcasts directly to the supported unit. This assures that Indications and Warnings, Force Protection (FP) and target information are provided directly to the supported unit to support time-critical operations. Collectively, these capabilities provide the supported commander with the intelligence required to shape the environment and win decisively.

Aerial Intelligence Brigade

Until 2006, most Army aerial layer assets were assigned to Corps AEBs. In December 2006, the Vice-Chief of Staff approved realignment of all Corps AEBs under INSCOM's regionally-focused Military Intelligence (MI) Brigades. This consolidation increased readiness of linguists and analysts (with INSCOM-funded training) and leveraged improvements in the PED enterprise to increase intelligence throughput. Although this realignment allowed more efficient employment of these low-density, high-demand assets, the INSCOM staff was not augmented with the requisite additional command and control structure required to most efficiently manage and employ those formations. In September 2013, INSCOM formed a provisional Aerial Intelligence Brigade (AIB) in order to realize further refinement of this concept and increase efficiency through unity of command at the lowest possible level.

The mission of the AIB is to conduct multidiscipline aerial intelligence operations, which complement organic intelligence operations of the supported unit and integrate with other elements of the intelligence enterprise. This provisional structure was formed in conjunction with an on-going Force Design Update (FDU) that is projected to inactivate the 1st MI Battalion (Aerial Exploitation) Headquarters in Wiesbaden, Germany, and use that structure to form an enduring AIB structure. The FDU is now in the final stages of staffing and anticipated to be approved in 2QFY14 with the publishing of an AIB organizational structure; its effective date is likely to be October 2016.

The AIB includes a separate PED company to address the need for multi-discipline intelligence capabilities to meet supported commander requirements. The ability of the threat to evolve rapidly in response to U.S. forces, and the ubiquitous availability of modern technology that rapidly changes in response to commercial demands, presents a challenge to traditional PED techniques and capabilities. The traditional approach to multi-disciplined intelligence (i.e., multiple phased analyses of single discipline intelligence products followed by multiple phases of fused product analyses to determine enemy intent) is too cumbersome and lacks the agility to quickly adapt to the emerging threat.

The AIB PED Company is designed to consolidate the analytical capabilities of the AIB to gain these efficiencies and reduce the PED cycle timeline. It is resourced to sustain dynamically adaptive production of relevant, time sensitive reporting to meet Warfighter demands in this new threat terrain. The AIB can forward deploy small, expeditionary PED elements from the PED Company to augment organic AEB PED elements. These elements can support expeditionary operations, ensuring an initial 24/7 PED support capability forward for both mature and immature theaters of operation. The PED Company can also be augmented by the battalions' PED Sections when forward ground-based PED requirements must be reduced for operational reasons. Finally, the PED Company serves as a focal point for coordination of AIB analytical efforts with other Army or joint partners within the PED enterprise.

Conclusion

Defense Planning Guidance and projections of the future operational environment demand that U.S. forces must be prepared to address a full range of threats, and counter enemy methods of operation that focus on opportunity and asymmetric advantage. The aerial layer of the Army ISR 2020 strategy capitalizes on the initiatives and lessons learned from a decade of asymmetric conflict; it provides a modular set of platform, sensor and PED tools. It features a revised structure that will provide flexible, multi-INT, and persistent ISR coverage to meet the needs of tactical commanders in Army 2020 without exclusive dependence on joint, strategic or national systems.

CPT Swiney is currently a Deputy Chief of the Manned Systems Division, TCM Intelligence Sensors at Fort Huachuca, Arizona. He has served multiple tours in Iraq and Afghanistan and is an Army Aviator qualified in the OH-58, CH-47, C-12, and RC-12 Guardrail Aircraft with 800 combat flight hours. He is a graduate of the MICCC and holds a Masters of Aeronautics from Embry-Riddle University.

Glossary of Acronyms

ADM	***acquisition decision memorandum***
ARGUS	***Autonomous Real-Time Ground Ubiquitous Surveillance (Imaging system)***
ARMS	***Aerial Reconnaissance Multi-Sensor System***
AROC	***Army Requirements Oversight Council***
CDD	***capability development document***
CDRT	***capabilities development for rapid transition***
COCO	***contractor owned, contractor operated***
COCOM	***combatant commander(s)***
CPD	***capability production document***
DPG	***defense planning guidance***
EMD	***engineering and manufacturing development***
ERMP	***extended range multi-purpose***
EXORD	***executive order***
FY	***fiscal year***
GOCO	***government owned, contractor operated***
GOGO	***government owned, government operated***
HQDA	***Headquarters, Department of the Army***
IPL	***intelligence priority lists***
JAUDIT	***a USSOCOM QRC LIDAR sensor program***
JROC	***Joint Requirements Oversight Council***
JROCM	***JROC memorandum***
JUONS	***joint urgent needs statement***
MAMI	***medium altitude, multi-intelligence (C-12 based QRC aircraft systems)***
MASIVS	***Multi-Aperture Sparse Imager Video System***
Milestone B	***Established by DoDI 5000.02, Milestone B designates entry into acquisition program***

MTI	*moving target indicator*
OEF/OIF	*Operations Enduring Freedom/Iraqi Freedom*
ONS	*operational needs statement*
POR	*program of record*
PSS(T)	*persistent surveillance system (tethered)*
SIPRNET	*Secure Internet Protocol Router Network*
SOF	*Special Operations Forces*
TACOPS	*a QRC tactical aerial LIDAR sensing aircraft capability*
TLA	*target location accuracy*
TNG	*training*
TSP	*tactical SIGINT payload*
USSOCOM	*U.S. Special Operations Command*

TRADOC CULTURE CENTER
ONE STOP SHOP
FOR ALL THINGS CULTURE

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

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

Why is Culture Important?

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

OVER 160,000 SERVICE MEMBERS TRAINED

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

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

REQUEST TRAINING NOW!

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

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

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

The TCC produces cargo pocket-sized training products to include smart books and smart cards, as well as digital downloads for smart devices. Areas covered include Iraq, Afghanistan, North Korea, Democratic Republic of Congo, and more. Let us know what we can produce for you. For a complete list of materials, see:
https://ikn.army.mil/apps/tccv2/.

Relevant Intelligence, Surveillance, and Reconnaissance to the Edge (RITE): A New Conceptual Framework and Requirements Strategy

**by Robert M. Wilkinson, Nicholas A. Green,
Robert D. Nelson, Thomas P. McDermott**

> ***"The priority for modernization efforts must remain focused on the Soldier, the squad, the network, mobility, and survivability."***
> ***TRADOC PAM 525-3-0, U.S. Army Capstone Concept*** [1]

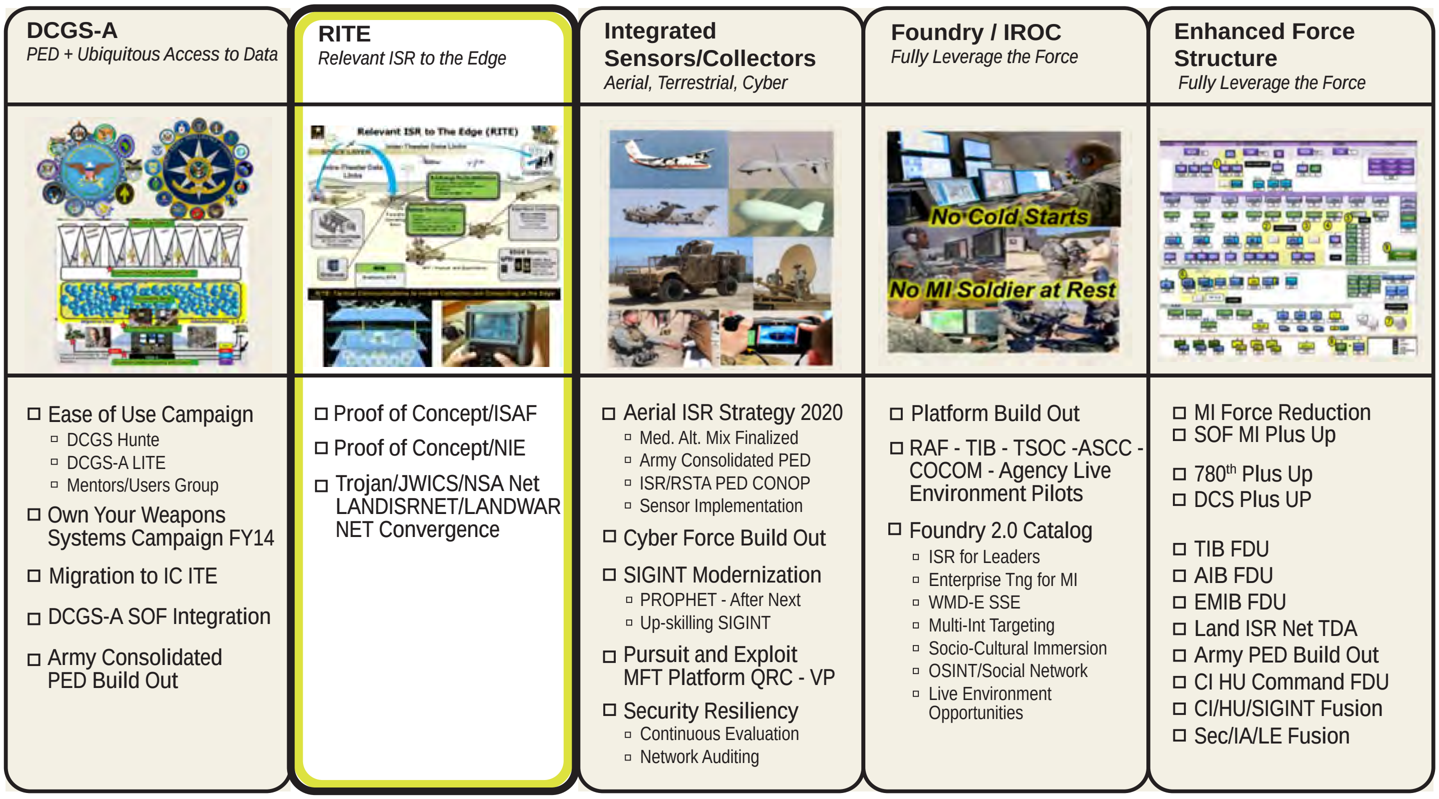
Introduction

The quote above from the Army's Capstone Concept, December 2012, indicates the importance the Army places on connecting the Soldier and the squad to Intelligence, surveillance, and reconnaissance (ISR) information on network while they are disadvantaged, dismounted, and mobile. Relevant ISR to the Edge (RITE) is a concept and requirements strategy to address four of the priorities listed in the Army Capstone Concept (Soldier, squad, the network, and mobility). To address these priorities, RITE improves the collaboration between the network, sensors, processors, and dissemination paths for combat information. If you have heard of the acronym RITE, chances are you have been exposed to several quick reaction capabilities (QRCs), including RITE 3G (R3G). Or perhaps you have seen it as a line of effort (pillar) in the Army G2's INTEL 2020 strategy (See Figure 1). Until now, RITE has been widely used, but not well defined in the Army Military Intelligence (MI) lexicon.

The U.S. Army Intelligence Center of Excellence (USAICoE) and Deputy Chief of Staff for Intelligence (DCSINT, G2) set out to better define RITE in August 2012. Over the course of the next 13 months, USAICoE produced a comprehensive study of approved capability gaps and required capabilities that trace directly to the five capability areas that make up the RITE conceptual framework. USAICoE, in coordination with the other U.S. Army Training and Doctrine Command (TRADOC) CoEs and the U.S. Army Special Operations Command, published the *RITE Concept and Requirements Strategy* in November 2013 to codify RITE in support of unified land operations and to develop recommendations for the many requirements needed to achieve RITE as a modernization priority for the future force. In this article, we will describe both the RITE conceptual framework and review the recommendations for the future. INTEL 2020 is described in further detail in a companion article in this same issue.

Terms of Reference

In order to define RITE, we must first define its components "Relevant," "ISR," and "the Edge". Let's start with



DCGS-A
PED + Ubiquitous Access to Data

- □ Ease of Use Campaign
  - ▫ DCGS Hunte
  - ▫ DCGS-A LITE
  - ▫ Mentors/Users Group
- □ Own Your Weapons Systems Campaign FY14
- □ Migration to IC ITE
- □ DCGS-A SOF Integration
- □ Army Consolidated PED Build Out

RITE
Relevant ISR to the Edge

- □ Proof of Concept/ISAF
- □ Proof of Concept/NIE
- □ Trojan/JWICS/NSA Net LANDISRNET/LANDWAR NET Convergence

Integrated Sensors/Collectors
Aerial, Terrestrial, Cyber

- □ Aerial ISR Strategy 2020
  - ▫ Med. Alt. Mix Finalized
  - ▫ Army Consolidated PED
  - ▫ ISR/RSTA PED CONOP
  - ▫ Sensor Implementation
- □ Cyber Force Build Out
- □ SIGINT Modernization
  - ▫ PROPHET - After Next
  - ▫ Up-skilling SIGINT
- □ Pursuit and Exploit MFT Platform QRC - VP
- □ Security Resiliency
  - ▫ Continuous Evaluation
  - ▫ Network Auditing

Foundry / IROC
Fully Leverage the Force

- □ Platform Build Out
- □ RAF - TIB - TSOC -ASCC - COCOM - Agency Live Environment Pilots
- □ Foundry 2.0 Catalog
  - ▫ ISR for Leaders
  - ▫ Enterprise Tng for MI
  - ▫ WMD-E SSE
  - ▫ Multi-Int Targeting
  - ▫ Socio-Cultural Immersion
  - ▫ OSINT/Social Network
  - ▫ Live Environment Opportunities

Enhanced Force Structure
Fully Leverage the Force

- □ MI Force Reduction
- □ SOF MI Plus Up
- □ 780th Plus Up
- □ DCS Plus UP
- □ TIB FDU
- □ AIB FDU
- □ EMIB FDU
- □ Land ISR Net TDA
- □ Army PED Build Out
- □ CI HU Command FDU
- □ CI/HU/SIGINT Fusion
- □ Sec/IA/LE Fusion

Figure 1. RITE and the INTEL 2020 Strategy.

the term "relevant." The common usage for the word can be found in any dictionary as referring to information having significant and demonstrable bearing on the matter at hand or information closely connected or appropriate to the matter at hand. ADP 2-0 states, "timely, relevant, and accurate intelligence and predictive assessments help the commander maintain operational flexibility, exercise mission command, and mitigate risk."

ISR is defined by JP 1-02 as an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. Army Doctrine Reference Publication (ADRP) 1-02 uses the same Joint definition and refers to ADP 2-0, which tells us that ISR is part of intelligence in unified land operations. Relevance is based the user's mission and operational environment. Relevant ISR must be tailored and available based on the user's dynamic needs.

If we break ISR down to its three defined components, *intelligence* is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations (JP 2-0).

Surveillance is the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means (JP 3-0). Surveillance involves observing an area to collect information (FM 3-55). Surveillance provides broad, relatively continuous monitoring to detect changes in enemy force status, activity or threats (ATP 3-55.6).

Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (JP 2-0). Reconnaissance complements surveillance by targeting specific objectives at specific intervals, rather than in a continuous monitoring mode (ATP 3-55.6).

The one term that does not have a doctrinal reference or commonly accepted definition is *edge.* The LandWarNet (LWN) Initial Capabilities Document (ICD) defines the *tactical edge* as:

> "the boundary, considered to be everything forward of a deployed tactical network's Defense Information Systems Network (DISN) point-of-presence/service delivery node (SDN). As with tactical unit boundaries, the contours of the tactical edge will vary by service, mission, phase of an operation, bandwidth availability, and other factors (technical and nontechnical). The tactical edge is tiered with bandwidth availability and organizational boundaries as major factors defining the tiers. The lowest tiers of the tactical edge include disadvantaged/dismounted and mobile users."

The Aerial Layer Network Transport ICD describes disadvantaged users as "leaders, Soldiers, sensors, platforms, and networked weapon systems not connected with organic communications assets and requiring additional means to acquire network transport and services."

The easiest way to visualize all these terms together as RITE is to describe them in a vignette. The vignette below illustrates the disadvantaged users' dilemma and demonstrates the benefit of RITE's five capability areas.

Picture the vast amounts of terrain between the fixed operating bases where U.S. and coalition forces operated in Iraq and Afghanistan during stability operations. Each day, convoys and patrols left those sites and operated at the "tactical edge" in the open spaces in between our fixed operating locations. Some of them were huge swaths of relatively unpopulated desert or mountainous areas; while others were densely populated urban areas with deeply rooted cultural complexities. The success or failure of their mission often depended on assured and secure means for maintaining situational awareness and communicating between units and echelons while on the move.

At that time, wireless line of sight communications capabilities only allowed for traditional voice communications and small limited amounts of data transport between mobile units and operating locations. Because of these limitations, units waited as vital ISR data and collected information decayed during the mission. This increased the latency in the reporting, processing, and exploitation of information and dissemination of intelligence to those who needed it. In other cases, communications limitations prevented the transmission of new and critical information and intelligence to the mobile units.

Similarly, the bulk of the data captured on a targeted site could not be transmitted back for immediate processing and return of relevant intelligence to the units performing the information collection. The greatest need for immediate feedback on the value of intelligence operations is during the operation at the point of collection. During Operation Enduring Freedom, small units operating in remote Afghan villages needed to make 'detain' or 'do not detain' decisions in minutes on the objective. Biometric data collected on persons under control needed to be quickly compared against the databases maintained in sanctuary locations in order to make those choices efficiently and effectively.

In response to this gap and other similar gaps, U.S. commanders in Afghanistan issued several urgent needs statements prompting the fielding of QRC material solutions to extend access to processed intelligence beyond fixed operating locations. RITE 3G and the Last Tactical Mile (LTM) Pilot are two examples of mobile wireless network extensions and cellular solutions designed to improve the transmission of critical information to and from the edge via mobile handheld devices. The QRCs made it possible for feedback to be available to the Warfighter in a matter of minutes. Mobile units sent their collected information to the enterprise for exploitation and analysis. Moments later, they received analyzed relevant intelligence, thereby minimizing unnecessary confinement of neutral people while ensuring that key insurgents did not slip through their fingers. These types of capabilities formed the nucleus of the *RITE Concept and Requirements Strategy*.

RITE as a Conceptual Framework

The conceptual framework for RITE begins with the following problem statement: ***Soldiers operating disconnected from fixed bases lack sufficient ISR/information collection, networking, and processing capabilities at the tactical edge to perform their missions.***

Detailed and timely intelligence is essential for commanders to gain and maintain situational understanding of the threat and the operating environment. High tempo combined arms maneuver and wide area security operations require effective information collection with the lowest possible processing and exploitation times and the least amount of latency. Additional capabilities are required to improve commanders' situational understanding and decrease the amount of time it takes for mobile or dismounted teams to submit collected information and receive relevant feedback from the intelligence enterprise.

RITE as a Requirements Strategy

The RITE requirements strategy addresses the need to connect the disadvantaged user at the tactical edge to the intelligence enterprise, enabled by a suite of on-the-move ISR/information collection capabilities, including sensors, processors, and applications on mounted/mobile/handheld (M/M/HH) devices. The RITE requirements strategy seeks to encourage the development of flexible, expansible, and robust communications architectures, with integrated processing and dissemination enabling faster, more powerful sensing, and collection capabilities. The strategy aims to enhance the synchronization and integration of ISR and information collection activities during dynamic, high tempo unified land operations.

In the gap analysis, the authors identified five major capability gaps (lack of capabilities) documented and validated by TRADOC through multiple capabilities based assessments and initial capabilities documents.[2] These five gaps are:

- ✦ Insufficient collection.
- ✦ Limited network connectivity.
- ✦ Limited network capacity.
- ✦ An inability to display and share relevant tactical information.
- ✦ A lack of capabilities to enable collaboration.

Table 1. RITE Capability Areas

Capability Gap	RITE Capability Areas	RITE Concept Capabilities
Collection	Advance Collection at the Edge	• Networked sensors and data relays. • Sensor control from the tactical edge. • Soldier as a sensor (passive and active. tactical collection.
Connectivity	Robust and Secure Network Transport	• Extended-range wireless transmission systems. • Mobile Cellular transmission systems. • Man-packable, fixed site, and unattended transmission systems.
Capacity	Processing & Dissemination at the Edge	• Networking: At-the-Halt (ATH), At-the-Quick-Halt (ATQH), On-the-Move (OTM), and On-the-Objective (OTO). •Decreasing bandwidth requirements through: ■ Sensor processing at the point of collection. ■ Micro-processing on edge devices. ■ Efficient disseminationpaths via edge networking. ■ Leverage cloud architecture.
Display/Share Relevent Tactical Information	Edge Applications	• Mobile Application Services Framework. • Customized prebuilt widgets and applets. • Metadata tags to minimize data pulls. • Multi-level security protocols. • Standard Sharable Geospatial Foundation.
Enable Collaboration	Mounted/Mobile/Handheld Devices at the Edge	•Nett Warrior (NW) End User Devices (EUDs) and Joint Battle Command-Platforms (JBC-P) enabled by Joint Tactical Radio.

It is necessary to mitigate these gaps in order to deliver relevant ISR to Soldiers at the edge. TRADOC determined that there are five interdependent required capabilities (See Table 1) that together combine to create a composite capability to enhance commanders' situational understanding and enable efficient use of ISR assets at the edge. These required capabilities are:

1. Advanced collection methods at the edge.
2. Robust and secure network transport.
3. Processing and dissemination at the edge.
4. Edge applications.
5. M/M/HH devices at the edge.

Capability Area 1. Advanced Collection at the Edge. In response to the first gap, the RITE strategy will focus capability development efforts to improve the disadvantaged user's ability to employ and control advanced collection methods at the edge. The object of this capability area is to improve situational understanding for commanders by increasing the timeliness, efficiency and effectiveness of information collection. The future force needs developments such as networked sensors and data relays, sensor control from the tactical edge, and improvements in both passive and active tactical collection capabilities to enable the Soldier as a sensor. Advanced collection at the edge will also enable future force structures, such as the multifunctional team, which are designed to support highly dynamic, mission-focused, and time-sensitive targeting and site exploitation efforts.

Capability Area 2. Robust and Secure Network Transport. The objective of the second capability area is to improve two-way connectivity between joint forces and disadvantaged users at the tactical edge, sensor-to-sensor cueing, and processing of collected data in order to answer information requirements when and where the information is needed. This area includes capability developments that extend the range and reliability of future wireless network transmission systems, create mobile cellular systems and encourage improvements in man-packable solutions to provide sufficient connectivity with multiple levels of security to disadvantaged users who are beyond line of sight: at the halt, at the quick halt, on the move, and on the objective. Potential solutions must network transport systems designed for fixed, mounted, dismounted, aerial, and aerostat platforms.

Capability Area 3. **Processing and Dissemination at the Edge.** Limited frequency space, lack of capacity, lack of lightweight power supplies, the cost-prohibitive nature of space-based capacity, and the sheer distances anticipated in the future operating environment require innovative solutions to increase edge processing. The third RITE capability focuses on solutions to improve sensor processing at the point of collection through implementation of micro-processing devices at the edge and establishment of more efficient dissemination paths through smart routing. Capability developments in this area also seek to leverage distributed architectures to move metadata and only push the precise "real" data when requested. As a means of mitigating the capacity gap, this capability area proposes a new understanding of the earliest point of consumption and seeks to achieve an order of magnitude improvement in information processing and dissemination.

Capability Area 4. Edge Applications. To improve data and information exchange capabilities and to decrease the total time from asset selection/tasking to dissemination of final product to the commander, this capability area explores the potential of a mobile application services framework utilizing custom prebuilt widgets and applications along with metadata tagging to display and share relevant tactical information. Powerful yet simple applications and widgets for routine correlation of data within a cloud computing environment can improve information sharing and situational understanding. The long term objective of this capability area is to collapse the many transit case equipment sets and stove-piped solutions for disadvantaged users into a common set of software-defined applications and widgets that Soldiers can choose from to populate their M/M/HH device, decreasing their physical burden and increasing their effectiveness.

Capability Area 5. Mounted/Mobile/Handheld Devices at the Edge. The technological advancement of small computing devices such as smart phones, tablets, and microcomputers embedded in everyday devices continues at an amazing pace. The final capability area of RITE focuses on realizing the full potential of M/M/HH devices (supporting applications from the fourth capability area) to bring processing power and dissemination capabilities to the disadvantaged user at the edge in the smallest, most powerful form factor required for the mission. Through the mounted computing environment (CE) and mobile/handheld CE working groups and in coordination with the program managers for Joint Battle Command-Platform and Nett Warrior End User Device, the RITE strategy promotes the improvement of future increments of existing capabilities to address the fifth gap.

Conclusion

The ultimate objective of RITE is to unify, integrate, and synchronize ISR at the edge, and to align Army capability development initiatives across each of the six warfighting functions (mission command, movement and maneuver, intelligence, fires, sustainment, and protection). The combined capabilities of RITE not only address the aforementioned gaps and improve edge capabilities, they also neutralize the adversary's ability to acquire newer, better technologies on the open market. To maintain dominance, we must use an agile acquisition approach to keep pace with changes in commercial technologies. For example, advanced communications technologies such as context aware and spectrum sensing cognitive radios are in development at academic and industry laboratories today. The USAICoE is developing requirements for a new collection capability that will utilize advanced radio technologies as a mesh sensor array.

The RITE Concept and Requirements Strategy will inform the future capability developments for Army capability sets, synchronizing the transition of emerging technologies with the Capability Set Management approach. The strategy will also align capability development efforts with the principles, tenets, and technical standards established by the six CE working groups under the common operating environment initiative. Lastly, it will inform the office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology as they develop the Science and Technology and Research Development Test and Evaluation investment priorities for the future.

Endnotes

1. TRADOC Pam 525-3-0, U.S. Army Capstone Concept, December 2012, 24.

2. The Intelligence Warfighting Function Capabilities Based Assessment, Joint Direct-Support Airborne Intelligence Surveillance and Reconnaissance Initial Capabilities Document (ICD), LandWarNet LWN ICD, Net-enabled Mission Command ICD (including Appendix K essential capabilities), Joint Aerial Layer Network ICD, Aerial Layer Network Transport ICD, and the Department of the Army Network Integration Evaluation 14.1 Capability Gaps.

Bob Wilkinson is the Booz Allen Hamilton team leader for the RITE project at the USAICoE and the G2 for the 311th Signal Command (Theater) as an Army Reserve Colonel. Nick Green is a Booz Allen Senior Associate and Intelligence Capabilities Analyst who previously managed the transition of multiple MI QRCs through the Capabilities Development for Rapid Transition process. Rob Nelson is a Booz Allen Intelligence Capabilities Analyst. He retired as a 352N Warrant Officer SIGINT Technician with 24 years of service. Tom McDermott is a Booz Allen Intelligence Capabilities Analyst and is a former MOS 35N who retired with 20 years of service. Together they are developing Relevant ISR to the Edge as a Concept and Requirements Strategy for TRADOC and Tactical Mesh Sensor System as a new capability for the Army.

GREAT SKILL Program

Military Intelligence Excepted Career Program

Our Mission

The GSP identifies, selects, trains, assigns, and retains personnel conducting sensitive and complex classified operations in one of five distinct disciplines for the Army, DOD, and National Agencies.

Who are we looking for?

Those best suited for this line of work do not fit the mold of the "average Soldier." Best qualified applicants display a strong sense of individual responsibility, unquestionable character, good interpersonal skills, professional and personal maturity, and cognitive flexibility. **Applicants must undergo a rigorous selection and assessment process that includes psychological examinations, personal interviews, a CI-scope polygraph and an extensive background investigation**.

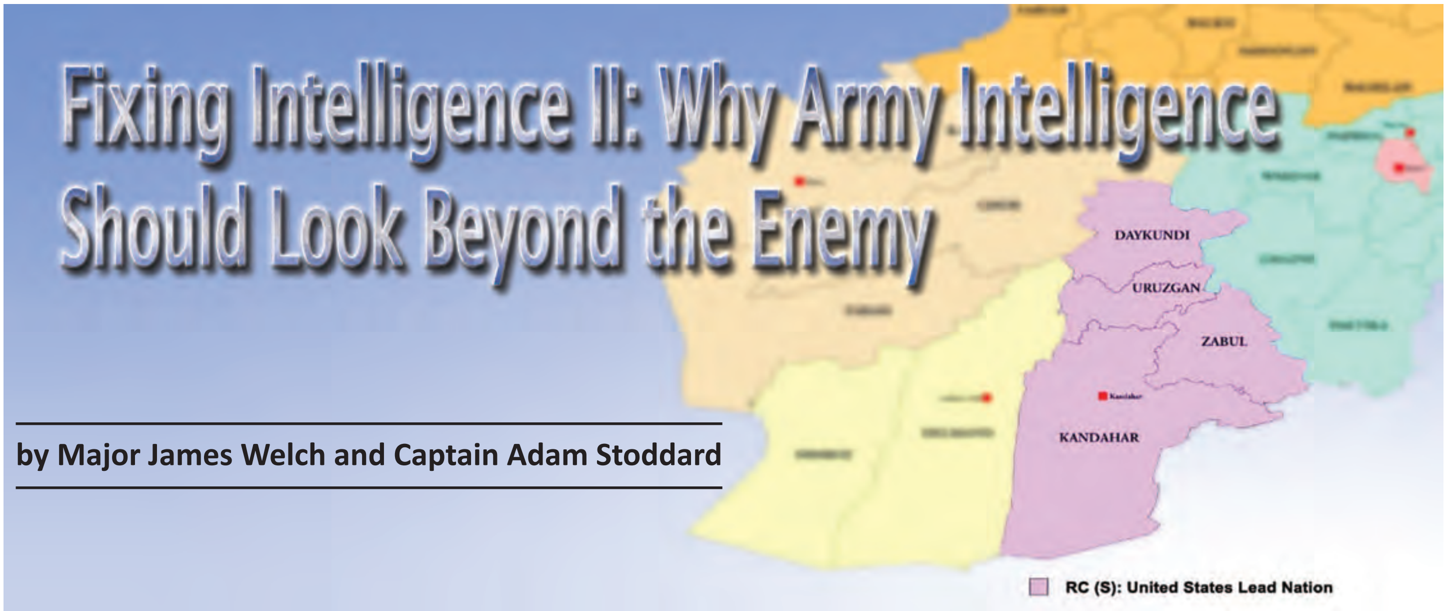
Basic Prerequisites:

✦ Active Duty Army.
✦ 25 years or older.
✦ Hold a TS/SCI clearance.

For a full list of prerequisites, please visit our website (SIPRNET http://gsd.daiis.mi.army.smil.mil) or contact an Accessions Manager at gs.recruiting@us.army.mil or call (301) 833-9561/9562/9563/9564.

Fixing Intelligence II: Why Army Intelligence Should Look Beyond the Enemy

by Major James Welch and Captain Adam Stoddard



Introduction

The proven success of the Stability Operations Information Center (SOIC) in Afghanistan–a white and green analysis cell that 'looks beyond the enemy'–must now be made a permanent part of Army doctrine and remain at the Army division level, even in peace time. The information provided by the SOIC will augment the pre-existing G2 section, and ensure the Division Commander is provided with a much broader perspective. Failing to implement this change risks not capitalizing on opportunities to gain a more comprehensive understanding of the battle space, and fails to reap the lessons learned during the last twelve years of fighting in Iraq and Afghanistan.

Background

Upon our arrival at Kandahar Airfield, where our division headquarters would assume command of Regional Command-South (RC-S), the 3d Infantry Division (3ID) G2 section assumed responsibility for the RC(S) SOIC. Our predecessors in the 82nd Airborne Division had established a SOIC whose analysts were able to study and analyze the portions of the battlefield not always covered by traditional intelligence analysis. By understanding the backgrounds and activities of Government of the Islamic Republic of Afghanistan officials, Afghan National Security Forces leaders, and informal powerbrokers, and how these individuals' actions affected the mission of RC-S, SOIC analysts were able to provide the Commanding General (CG) a more complete picture of the battle space.

Army doctrine has previously recognized the importance of this information and Army Doctrine Reference Publication (ADRP) 2-0 makes this point when referencing civil considerations. However, as yet there is no formal element in a standard division intelligence (G2) section that is assigned the task of analyzing this type of information. It was not until LTG Michael Flynn called upon the military to pursue the concept of SOICs in Afghanistan that such a section was formalized for conventional units. He articulated the concept of SOICs in the paper, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," co-authored by Captain Matt Pottinger and Mr. Paul Batchelor. Since then, SOICs have proven to be an effective tool for helping leaders better understand the Afghan battle space.

SOIC Case Study: Afghanistan 2012-2013

Although the RC-S SOIC was not necessarily manned as prescribed by LTG Flynn, it was staffed in a manner that allowed it to become a vital part of the RC-S intelligence section. Like the 82nd Airborne before us, the 3ID SOIC was led by an Army major who also served as the CG's Key Leader Engagement (KLE) advisor. Due to the officer's accessibility and knowledge of the CG's priorities, the SOIC analysts were better able to attune their priorities to ensure the CG's needs were met.

Assisting the major was an Army captain who served as the Deputy SOIC chief. As the SOIC chief was often away on KLEs, it was vital to have a deputy who could manage the ongoing production of the SOIC analysts. The SOIC was further manned by two Defense Intelligence Agency (DIA) analysts, as well as a Central Command (CENTCOM) supported DIA analyst whose primary duty at CENTCOM was Afghanistan analysis. In addition to the DIA personnel, the National Geospatial-Intelligence Agency (NGA) provided one analyst whose primary responsibility was to support the SOIC analysts in gathering host nation data and portraying this information as needed.

Finally, the RC-S SOIC was fortunate to be rounded out with several contractor billets. These billets were an absolute necessity as the level of detail required for proper analysis made it essential to divide the battle space into numerous areas of responsibility.

How it Works: Fusing the "White and Green" with the "Red"

Traditional thoughts on military intelligence (MI) suggest that our primary consideration should be about the enemy, his most likely and most dangerous courses of action, and how we might counter those actions. However, as has been learned in Iraq and Afghanistan, MI professionals must also know and understand the individuals who make up the white and green side of the battle space, the government and security leaders of the host nation.

As typical intelligence analysts are often overwhelmed with understanding and targeting the enemy, they do not always have the time necessary to fully evaluate this portion of the battle space. However, SOIC analysts work in tandem with those analysts responsible for studying enemy (red) targets and networks, allowing the G2 section to present the commander a much more comprehensive understanding of the battle space. SOIC analysts are not only responsible for studying host country government officials, security forces, and informal power brokers, they also reach out to the various entities that work with these leaders and develop mutually beneficial information sharing relationships.

Relationships Critical to Success

The hallmark of the RC-S SOIC was the ability of analysts to gather information in the smallest detail, in order to provide a thorough analysis of their assigned areas of responsibility. The SOIC analysts were able to do this because of the relationships they established with those Soldiers and civilians deployed throughout RC-S. SOIC analysts regularly received information via email distribution, phone calls, and personal visits. Additionally, RC-S SOIC analysts traveled across southern Afghanistan in order to meet with special operations forces, U.S. State Department officials, military advisors, and conventional military forces.

Among those entities that provided the SOIC with the most detailed information were company intelligence support teams (CoISTs) and Human Terrain System (HTS) social scientists. Understanding who owns the local land, who directs the local tribes, and who makes decisions at local levels proved essential to understanding the battle space and providing the CG with the most timely and accurate information. As SOIC analysts have discovered, CoISTs are particularly adroit at understanding this level of detail. Additionally, HTS social scientists are particularly adept at making visual observations in the field, attending village to district jirgas, and advising company, battalion, brigade, and division leaders on the cultural aspects of an area.

These types of relationships allowed the SOIC analysts to gain critical information and get a better understanding of the battle space from a perspective not always known at a division level (or sometimes even at a brigade level) headquarters. Through these relationships with sometimes disparate organizations, the SOIC was able to present the intelligence enterprise with a more comprehensive understanding of the RC-S terrain.

Open Source Intelligence (OSINT)

To assist SOIC analysts in understanding the green and white space, and how the actions of those actors affect the mission, the SOIC capitalized on the enormous amount of information available from open source means. While this has traditionally included the monitoring of media sources and internet sites for information that may be of intelligence value, SOIC analysts also monitor Facebook, Twitter, and blogs. These types of social media offer a great deal of information–often from people who are on the ground and witnessing critical events as they occur. For example, throughout the Arab Spring social media was used as a means to share valuable information in situations that were otherwise under media blackout. As has been the case in Afghanistan, journalists and local powerbrokers are often the first people to hear about an event, and the former often share this information using social media.

In addition to social media, SOIC analysts were familiar with the other resources of information that shed light on their area of responsibility. This included media articles, documentaries, reports from non-governmental organizations, information provided by local governments, studies conducted by universities and think tanks, and any other type of publicly accessible information that helped to better understand the area.

Information Brokerage

As LTG Flynn highlighted, there must be an information broker to manage the volume of information gathered by the SOIC analysts, past and present. This issue has yet to be adequately addressed. However, if an effective, standardized method for storing and analyzing the massive amount of information is properly implemented–one that is compatible with the rest of the intelligence community (IC)–this will allow the vast amount of information collected by SOIC analysts to be readily accessed and available to consumers in a timely manner. At least two systems have already proven to be incredibly useful throughout the IC as multifunction intelligence toolsets. No matter which system is ultimately used, SOIC analysts must be well versed on the use of that system in order to effectively capitalize on the technology available.

It would be of great benefit to the SOICs and the IC if the other producers of white and green information, such as the CoIST, HTS, and advisor teams, also used the same software. This would ensure the information gained by these entities is not lost with the transition of units and it would allow for greater collaboration with the IC and other government agencies. A dedicated data manager on the SOIC team could serve as the information broker and ensure information has been properly added and tagged to the storage system.

The Way Ahead: Implementation in Army Doctrine

With the drawdown of forces in Afghanistan, some may say SOICs have served their purpose and are no longer needed. On the contrary, the future utility of SOICs, as proven in Afghanistan, will enable division intelligence leaders and division commanders to gain a comprehensive understanding of future battlefields.

Whether the SOIC is formed from various entities within the division headquarters or a part of the division G2 section, Army doctrine must change to make the SOIC an enduring part of Army intelligence. While an organic G2 section would be best suited to fulfill such a role, there are two other options that could help to fill this current void. Rather than have an element within the division G2 section, a SOIC could be a part of a battlefield surveillance brigade and attach to a division headquarters when needed.

Already being in the same unit as many other robust intelligence sections, they would come into theater with excellent relationships already established. Another option could be to build a SOIC using Soldiers from the civil affairs, information effects, and intelligence sections of a division staff. These Soldiers would be organic to their regular sections (G9, G7, and G2, respectively), but bring their skill sets together to form the SOIC.

However, the recent shift to regionally aligned brigades makes these two options undesirable. With this shift, Army intelligence doctrine must adopt the SOIC as a permanent part of the division G2 section. Because divisions will now have brigades prepared to respond in particular geographic areas, units would be better served with a permanent section rather than an ad hoc section formed only in response to conflicts. This will ensure division commanders have a more complete understanding of an area before they are charged with deploying their Soldiers into harm's way.

At a minimum, a non-deployed SOIC should be manned with a section leader, a deputy, and two analysts. The SOIC personnel should maintain relationships with the organizations that will assist in manning the SOIC once deployed. This would include the sharing of information, cooperation on projects, and other efforts to both inform and maintain these critical relationships. Once deployed, the SOIC Soldiers would fall into the deployed SOIC set-up, which should include the addition of NGA, DIA, State Department and allied nation representatives, as required by the location and mission. Ideally, the SOIC would be manned by the same interagency personnel with whom the SOIC Soldiers would have collaborated during home station preparation.

The volume of information gathered by SOIC analysts and the level of detail they understand will greatly benefit brigade combat teams. SOICs must now be made a permanent part of Army divisions and included in Army doctrine. To take no action would be to ignore lessons learned during the last twelve years of fighting in Iraq and Afghanistan.

MAJ James Welch served as the RC-S SOIC Director from August 2012–May 2013 during 3ID's deployment to Kandahar, Afghanistan. CPT Adam Stoddard served as the Deputy Director for the RC-S SOIC from February 2013–May 2013. He continues to serve as the RC-S SOIC Director under the Fourth Infantry Division.

U.S. ARMY CYBER COMMAND

ARMY CYBER

The Army is Serious About Cyber Operations

by Command Sergeant Major Rodney D. Harris
Army Cyber Command CSM

The Army, having recently graduated the first two groups of Cyber Defense noncommissioned officers (NCOs) at Fort Gordon, Georgia, is well on its way to realizing the benefit of the investment we are making in our cyber mission force. Having had the opportunity to spend time with these elite cyber skilled NCOs, I'm excited about the future of our cyber mission force and the quality of NCOs that are signing up to be part of the Army Cyber team.

Today we are working through tough challenges associated with using these Soldiers in a heavily contested environment while simultaneously working through Army processes to establish this new capability. The task is to define this unique skill and the special considerations that must be made to recruit, train, manage, and retain the talent necessary to be successful.

I would like to share some points in reference to Army Cyber, our current status as the Army's newest operational command, and some of the topics we are addressing as we find common solutions to the challenges we are facing today as seen from our senior enlisted leaders.

My first lesson learned in Army Cyber Command has been that the application of leadership principles in highly technical fields requires a different approach to connect with the Soldiers we lead. While the fundamental elements of leadership are shared across most aspects of military operations, I have found that to have a creditable place on the team in a cyber organization, leaders must spend the time necessary to truly understand what our operators are doing in their specific roles on the team.

Often we tend to rely on our training systems to ensure the proper certifications are in place. Our goal is to ensure these Soldiers have the legal authority to sit behind their workstation while relying on technical experts to get the mission accomplished. But if we expect to know our Soldiers and relate to the challenges associated with the unique aspects of these tasks then we must spend time to know the technical details of their jobs.

Since assuming the responsibilities as the Army Cyber Command Sergeant Major I've spent a great deal of time engaged with our cyber teams across the force and gained a good understanding of what it takes to be a cyber professional on our team. I've spent time with our operators across the Army.

Having been asked the question why I spend so much time with them, my response is shaped by my time as a Bradley master gunner. My experience has been that once I was no longer working on guns and planning ranges and training qualifications, if I wanted to stay connected to our Soldiers and understand what their concerns and challenges were, I had to go to the motor pool and break track with them. I now see our operation centers as my motor pool. Cyber leaders must spend the time with our operators to understand what they do even when we are well out paced intellectually in their domain.

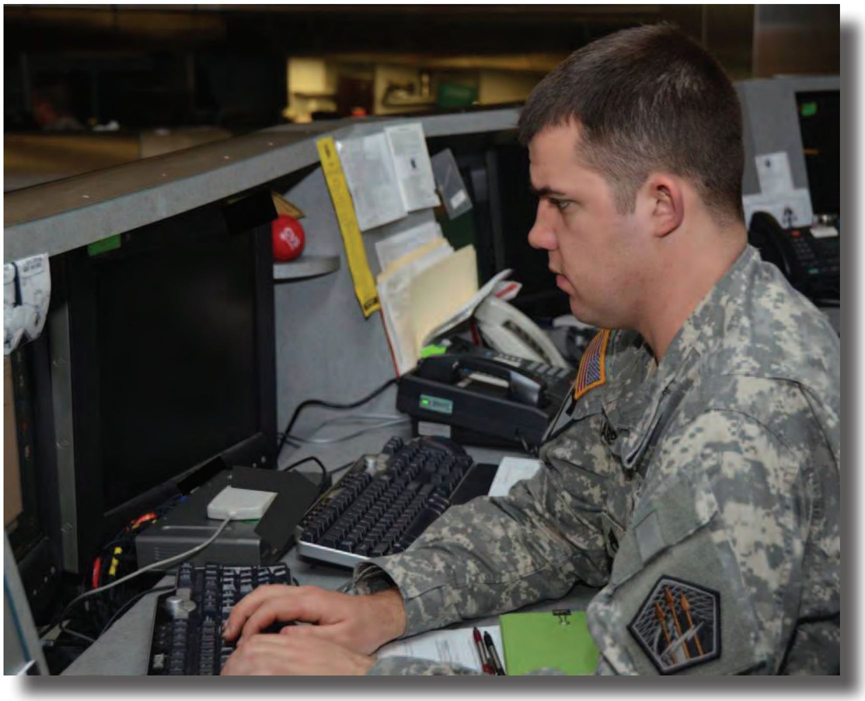
I've also spent time visiting with senior leaders across the Army discussing cyber operations. I'm certain that we have a significant challenge associated with educating our force about our mission and the important role our teams will play on the future battle field as we fully integrate into full spectrum operations across all domains of warfare.

Many senior leaders are still cyber illiterate about basic processes that we might think are commonly understood. Ask the question what happens when a Soldier clicks on a link in a phishing email and the reply is usually something like it will destroy his computer and "that's what he deserves."

Many still haven't recognized the fact that we are all interconnected and one action by one Soldier can have impacts on our weapon systems, our navigational systems, our mission command capabilities and more.

The very definition of cyberspace is complex and still debated across the Department of Defense. However, most people do understand what their network is and that it is connected to the worldwide internet and that other networks across the globe are also connected to the internet. They also understand that their computers, FBCB2, BFT, precision guided munitions, UASs, AFATADS, DCGS-A, and even our basic rifleman in today's modern battlefield are connected to that network.

When we begin to understand that the cyber battle fields are the pathways and connections between those devices, then we begin understand the importance of what our cyber units do. Once we realize that cyberspace is a domain that can be navigated just like the streets of Fallujah, then it becomes real and relevant to leaders in the Army today.



Unlike within the land, sea, air, and space theaters, cyber operations don't come with the uniforms of an occupying army nor flags stamped on predator drones. The reality is a digital footprint can disappear in a matter of seconds. Not only is it difficult to determine who might have been responsible for an attack, the lines between acts of war, terrorism, espionage, crime, protest and more are frequently blurred. It's not always easy to separate the good from the bad in cyberspace.

That's why it is so important that we get serious about cyber space and invest now in the Soldiers and NCOs that have the ability to apply their skills towards this difficult mission.

We are still in the formation stage of developing our capabilities within the various types of units and teams that make up Army Cyber Command and that doesn't happen without input and participation from these NCOs in the process. As we build capacity and begin operating, we will rapidly generate requirements. Very soon we will not have the forces available to work the volume of requirements once commanders realize the value these organizations bring to their force and warfighting capability.

As we move towards the establishment of a Cyber Center of Excellence we will refine our understanding of doctrine, how we fight, and how we employ these teams and their capability. We will work through the difficult questions such as: What authorities are required? What operational platforms will we need? Will we need to deploy teams to work in close proximity to the key terrain they operate in, or can their task be accomplished remotely?

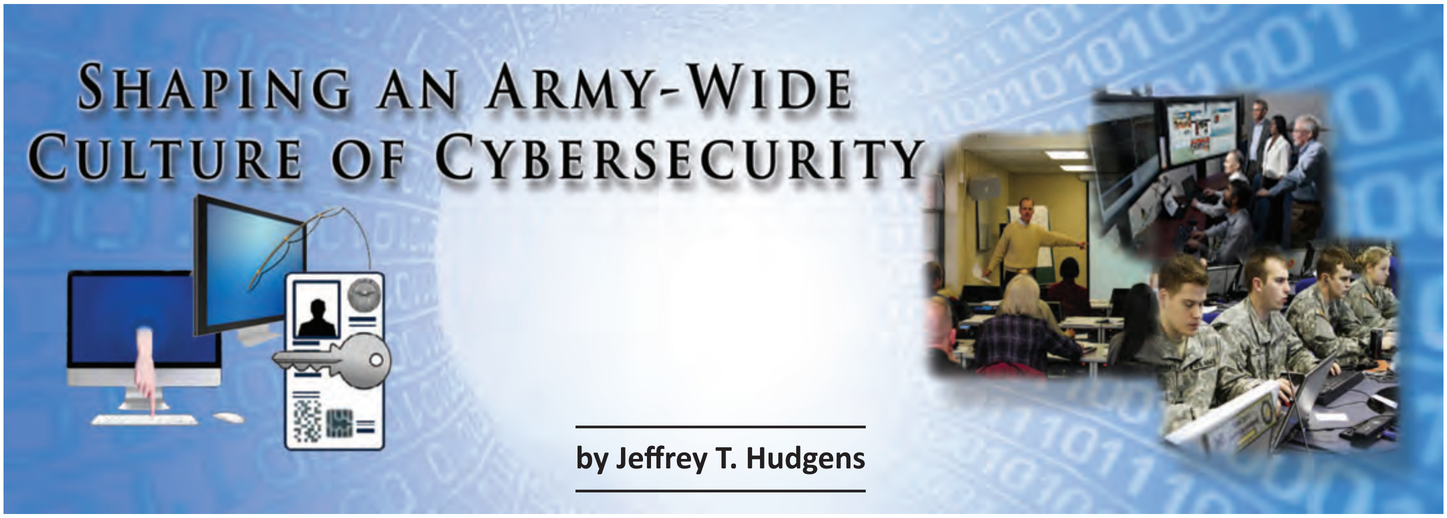
Many key decisions will have to be made about how to manage the talent these Soldiers represent. How do we acknowledge their skill and compensate them accordingly? How do we develop a career model that best employs these Soldiers across the total force and enables them to have the ability to move to the grade of E-8 and E-9 while maintaining skills and ensuring they remain current on the latest technology and techniques required to accomplish these unique tasks.

To be sure these are significant challenges that will require significant effort and investment to address, but our nation has also recognized the seriousness of the threat. Our Army has recognized the importance of employing Soldiers in this critical role and will make the right decisions required to ensure we not only maintain their skills, but also enhance and grow them as we move to meet evolving threats.

I have an *enormous* amount of respect for our cyber skilled NCOs and the amount of pride they take in accomplishing their mission. Most often they do so quietly, unnoticed and with little recognition for their critical role in our national defense.

Shaping an Army-Wide Culture of Cybersecurity

by Jeffrey T. Hudgens



Introduction

As cyber-related threats continue to impact Army networks, information, missions, and people, the need for force-wide awareness of those threats and mitigation measures grows. Network end users, the first-line defenders in the growing cyberspace domain, are critical in ensuring the Army as well as the Department of Defense (DOD), can conduct its operations and provide Information Assurance (IA) and cybersecurity across its networks. Although additional personnel are being added to the cyber workforce to provide greater levels of defense for DOD and Army networks, network end users play a vital and necessary role in ensuring operational viability of those networks.

To highlight the role of end users, the Chief of Staff of the Army on 1 February 2013 directed actions be taken to "improve the Army IA /Cybersecurity posture...," emphasizing that "we must change our culture," our shared set of values, goals, and practices.[1] At the individual level, we must all change our mindsets to one in which we take cybersecurity seriously, and we realize that our individual actions can have significant (and sometimes negative) impacts on operational networks.

The threat in cyberspace is growing more sophisticated, technically adept, and focused on outcomes. Reviewing open-source cybersecurity information and threat trends shows that threat actors, from script kiddies to state-sponsored hacker groups, are increasing their capabilities. While attacks against Army and DOD networks increase, organized cyber crime activities and attacks against individuals are also increasing. Although cyber crime and cyber attacks against individuals may not impact Government systems directly, they can impact the performance of those individuals in terms of lost time and resources, thereby having indirect effects on mission execution.

The MI community can help address the need for timely and relevant awareness of cyber threats for end users by collecting relevant open-source threat information and making that information available through myriad distribution methods. In the case of IA/cybersecurity, the MI community would be providing a "community service" for all end users and supporting the Army's overall leader development, training, and education (LDT&E) efforts. In addition, intelligence is a critical enabler in moving from a reactive IA/cybersecurity posture to a proactive posture.

Historically, network end users have generally viewed degradations with the network, operating systems, and applications as purely technical issues, and therefore a problem for the "6," something that "they need to fix soon." In addition, network end users have generally not viewed themselves as part of the solution. Over the years, this mindset has helped to undermine cybersecurity at multiple levels (individual, organization, etc.) and is, therefore, something that needs to be addressed in the Army's IA/cybersecurity and LDT&E efforts.

As Ms. Deb Plunkett, Director of the National Security Agency's Information Assurance Directorate, stated in a Webcast presentation on 22 January 2013, "We do not have a very security conscious populace… (We) need to provide education and awareness of operational security risks taken by simply logging in."[2] Although IA training is an annual requirement, it is now generally accepted that the once-a-year training is not enough to maintain high levels of user awareness.[3]

Network end users must be aware of and understand network policies and know there are tools and techniques used to support network defense, IA, and policy enforcement. They must also understand how their actions impact operational networks. Some high-level guidance regarding end users is found within DOD 8570.01-M, *Information*

Assurance Workforce Improvement Program, Chapter 6, which includes the following:

- ✦ The trained and aware user is the first and most vital line of defense.
- ✦ IT users need to maintain a degree of understanding about IA policies and doctrine commensurate with their responsibilities. They must be capable of appropriately reporting and responding to suspicious activities, and know how to protect the information and IT systems to which they have access.
- ✦ IA training must be current, engaging, and relevant to the target audience to enhance its effectiveness. Its primary purpose is to educate and influence behavior. The focus must be on education and awareness of threats and vulnerabilities so users do not perform actions that lead to or enable exploitations of the DOD ISs [information systems]. Authorized users must understand that they are a critical link in their organization's overall IA success.[4]

If the annual IA training is not meeting expectations, then how can the Army develop "trained and aware users?" The best approach is establishing and maintaining an enterprise-wide awareness program, supported by senior leaders, that builds upon and complements defensive cyberspace operations and network operations performed by the cyber workforce. However, developing an effective user awareness program can present its own challenges, as evidenced by lessons learned through other prior and ongoing efforts across the whole of Government and within industry. Several analyses regarding network user awareness have been conducted over the past three to four years, and common conclusions highlight five main traits that are essential for success, each of which is discussed in more detail in the following sections.[5] The five traits are:

- ✦ Persistence. Provides awareness and training throughout the year, not just once annually.
- ✦ Timeliness. Uses the "teachable moment" and immediate feedback to maximize training, ensures information is updated frequently and quickly distributed to end users after discovery.
- ✦ Relevance. Provides applicable information in a context that resonates with network users.
- ✦ Presentation. Uses both active and passive approaches, as well as various methods, modes and media, to deliver information and remain engaging.[6,7]
- ✦ Effectiveness. Includes integrated assessment methodologies and analysis to determine whether awareness activities are meeting program goals and to then adjust as needed.

Persistence

The current guidance provided in DOD 8570.01-M only addresses a single "annual" training evolution, the Defense Information Systems Agency (DISA) produced annual IA training. This training alone does not provide enough exposure to relevant and timely information throughout the year that would help to build and maintain an end user's cyber awareness. Although a ramp-up in awareness of cyber threats may occur throughout the year (e.g., supplemental training before a deployment, training rotation, Tier 1 exercise), the overall mean level of cyber threat awareness is generally lower than desired. This effect is graphically displayed in Figure 1 as the lower sine wave and the associated "mean" average of performance.

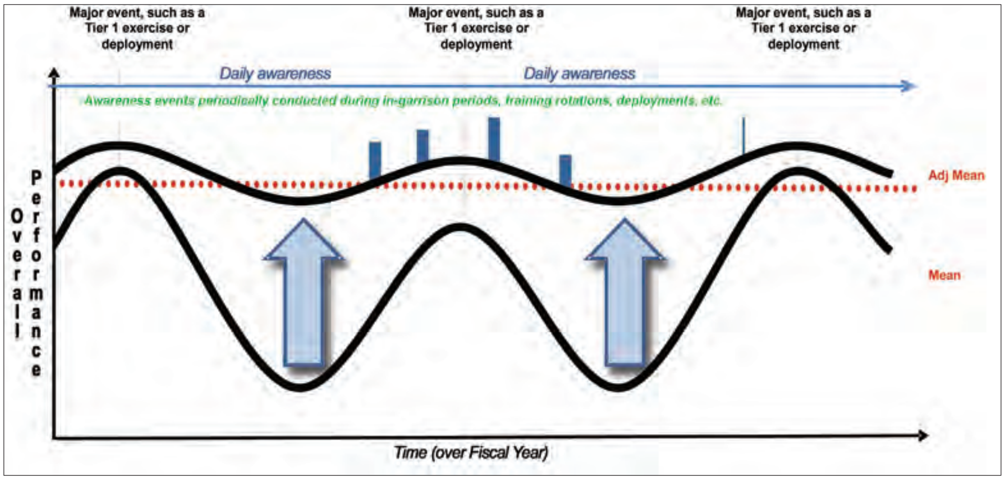


Figure 1. Overall Performance Expectancy based on Persistent Cyber Threat Awareness

In some cases, organization-wide awareness information is provided and training conducted as a reaction to a network incident, such as a data breach or network policy violation. While this approach is sometimes necessary, it is reactive in nature. Instead, a proactive approach to user awareness is more effective.

To raise overall performance and ensure proactive awareness, end users must be provided additional cyber threat awareness in a fashion that is unobtrusive yet impactful. Only through routine, persistent awareness activities, enabled by technology, can individuals' mean levels of "performance" start to shift upward and a culture of cybersecurity start to take hold (as depicted in Figure 1 by the upper sine wave and "adjusted mean" level of performance).

Timeliness

Prior analyses of awareness and training programs have highlighted that many opportunities for immediate feedback to an IA/cybersecurity incident are missed. For example, if a person was involved in an incident, that person may not immediately understand how his action(s) caused the incident, and by the time feedback is provided (if at all), the "teachable moment" has passed.

Therefore, cyber awareness and training should incorporate immediate feedback and training to maximize the potential for learning. For instance, in a phishing awareness and training campaign, simply collecting data about how many users clicked on a link, or opened an executable file within the phishing awareness email, may provide a statistic for a brief to senior leadership, but would not support the end goal of shifting culture. However, providing an end user who "took the bait" with immediate feedback and training would help to maximize the learning retention of that individual.

In addition, the information presented as part of the awareness and training campaign must be current. Given that cyber threats are constantly changing and becoming more sophisticated the MI community, working with training specialists, IA personnel, and network operations staff, among others, can provide valuable support by collecting, processing, assessing and disseminating information that will have same-day impact. For example, information regarding a discovered vulnerability in an Adobe product, widely used by many at home and at work, could quickly be made available to end-users for their awareness. A current scam targeting Army personnel could reach end users quickly and via multiple sources. The key to success is in establishing the means and processes for quickly getting threat information and recommended mitigation measures out to the entire force, enabling end users to take timely actions which bolster cybersecurity and support operational effectiveness.

Relevance

Relevance, or providing information in a context which resonates and connects with end users, is in many ways tied to timeliness. Although the cyber threat is constantly changing and becoming more sophisticated, many user awareness programs have not kept pace, relying on static information that might be updated once annually at most. Over time, much of the information presented is irrelevant and does not discuss the current threat.

Even more of an issue, however, is that most threat information presented to end users is focused on threats to government systems and data, many times using scenarios that are more applicable to the enterprise than to the user themselves. While protection of government systems, data, and ultimately, operations, is the ultimate goal, this "inside the fences" approach does not have the desired effect on learning simply because many end users do not feel the relevance to themselves as individuals. In order to inculcate a culture of cybersecurity across the force, end users need to be provided awareness of how they can personally make a positive impact.

From a threat awareness perspective, the MI community, working with U.S. Army Cyber Command and the Signal community, can help to improve relevance to end users by collecting and providing "outside the fences" information that end users can more readily relate to, that they feel a personal stake in, and that they understand has potential impact to their personal lives and resources. Simply put, "make it personal." That means including more information within awareness training and activities that focuses on users in home and travel settings. In those cases, the end user becomes the de facto network operations center, responsible for those things that ultimately impact the equipment they are using, and therefore having a greater (perceived) stake in cybersecurity.

Given that many Army personnel use their personal equipment to access government web mail, it becomes even more critical that they understand how their actions at home and on travel can impact government systems and missions. Relevant information provided to end users might include:

- ✦ Threats related to cyber crime, including online scams.
- ✦ Vulnerabilities in common operating systems and applications, so that users can update/protect their personal equipment against potential backdoors into government systems.
- ✦ Mitigation measures, such as considerations for home router settings and methods for securing one's smart-phone.
- ✦ Steps one can take to be more secure on social networking sites.
- ✦ Considerations for operations security when using social networking and emails.

By using a balanced "inside the fences/outside the fences" approach, end users will feel more personally involved and responsible. The effectiveness of awareness efforts will then start to increase and provide greater value and return on investment. Ultimately, a shift in culture toward a more cybersecurity-conscious force at home and on travel will translate back into the government workplace, resulting in enhanced cybersecurity and operational security.

Presentation

A common issue among awareness programs is that, in many cases, information provided does not make the impact it should have on the end user simply because the presentation format does not align with the end user's preferred learning style. It is typical to find a "one size fits all" approach to providing information, such as an on-line PowerPoint brief. Yet educational specialists tend to agree that within the general populace there are several generations of learners, each with its own favored means of learning. In general, older generations tend to prefer in-class sessions with instructor interaction, while younger generations tend to prefer distributive learning and technology focused approaches.[8]

To meet an awareness program's objectives, various methods, modes, and media should be used so that end users can more readily learn in a manner that meets their personal learning preferences. Examples are:

- ✦ *Methods*. Academic and practical exercises.
- ✦ *Modes*. Computer-based training, gaming, role playing, practical exercises, guest speakers.
- ✦ *Media.* Text, slides, video, Internet.

In addition, to keep the end user population engaged, awareness information and activities can be presented using both active and passive techniques. Active techniques require user interaction, such as acknowledging an alert or answering a question. Passive means do not require user interaction; it is up to the individual whether or not the information is observed or activity performed. An example of a passive technique is posting new threat information to a central viewing site, such as AKO; the end user has the choice whether to view the information or not.

Effectiveness

Assessments and metrics analysis is a necessary and critical component of a successful user awareness program. A key reason many awareness and training programs fail is because they lack embedded assessment methodologies, which include conducting baseline assessments, taking regular measurements, and determining where and how adjustments need to be made. Some programs are established but never measure baseline awareness, nor do they routinely assess awareness over time to determine trends. The lack of assessments and failure to determine what works and what does not work for the target audience then leads to content stagnation, a subsequent drop in the program's usefulness, and expenditure of resources in an ineffective manner.

There are several methods for collecting metrics and feedback, although no one technique provides a full picture of the effectiveness of an awareness program. Surveying the end user population can be effective if initial and follow-up surveys are collected. A "practical exercise" technique is to conduct a phishing awareness campaign, where random users are chosen to receive phishing training emails without prior knowledge of the "test" email. From the results, program managers can establish some baseline and follow-up metrics to measure whether end users' behavior is changing over time. In other words, are end users paying attention to the threat awareness information being presented through other techniques? Industry is seeing a rise in the number of organizations introducing phishing campaigns for employees, resulting in a positive shift in their cybersecurity postures. Future Army cyber awareness/training programs need to include assessment methodologies, such as a phishing campaign, and thorough analysis from the very beginning in order to gauge effectiveness and determine return on investment.

Way Ahead

To start an Army-wide shift in culture, the Army should adopt a "marketing campaign" aimed at getting end users to think of their workstation, networks, and data as things that should be defended, not just used, while ensuring end users understand how their actions can and do have implications for operational success. A shift in culture will take much advertising and encouragement, and should be driven from the top. The level of effort required for the awareness campaign is akin to the seat-belt campaign in the 1980s. At the start of that campaign, car drivers viewed the Government's efforts as invasive. Now, wearing seatbelts is the norm, something that is just habit. This is where cybersecurity needs to be among end users–a habit.

The Army has taken steps to supplement awareness for end users. Current and past efforts include, or have included:

- ✦ Secretary of the Army memorandum, Mandatory Information Assurance/Cybersecurity Awareness, 1 February 2013.
- ✦ ALARACT 329/12: Anti-Terrorism Quarterly Theme–Cyber Threat Awareness (Q2/FY13).
- ✦ HQDA/Office of the Provost Marshal General pamphlet: The Cyber Attack Cycle.
- ✦ HQDA/Office of the Provost Marshal General pamphlet: Cyber Threat Vignettes, November 2012.

- ✦ AKO (NIPR): "Hot Topics" section provides "Cyber Alerts" and links to other cyber/IA-related materials.
- ✦ AKO: National Cybersecurity Awareness Month (October) materials.

With all the challenges involved with user awareness programs, how might the Army proceed in establishing and maintaining an effective program? The Army does not need to reinvent the wheel; it can and should leverage existing cyber awareness pilots that are working to address the challenges discussed previously, drawing on the extensive analysis and lessons those pilots have produced. The DOD Chief Information Officer staff, DISA, Navy N2/N6, U.S. Strategic Command, and U.S. Coast Guard, have been coordinating for the past two to three years on cyber awareness efforts at various levels. In addition, DOD has been coordinating with the National Initiative for Cybersecurity Education and Department of Homeland Security, which are collaborating on a national-level campaign for cybersecurity awareness.

The U.S. Strategic Command has been conducting a user awareness pilot as part of its Cyberspace Training Initiative/Cyber Training and Readiness programs and is developing a "user awareness toolkit" that DOD CIO is interested in using on a DOD-wide basis. Based on lessons from these various organizations and efforts, recommendations for moving forward with a more robust Army-wide IA/cybersecurity awareness program are provided in Table 1.

Table 1 Recommended Actions

Success Factor	Recommended Actions
Persistence	• Implement persistent, year-round awareness of cyber threats, policies, and mitigation measures to supplement annual DISA IA training. • Harvest open source cyber-related information (cyber threats, tips, alerts, mitigation measures) and distribute to end users on a daily basis.
Timeliness	• Determine distribution channels to quickly move information to all end users. • Establish central repository for one stop information sharing.
Relevance	• Include information related to both home and mobile threats, in addition to threats to government systems and operations (MI and Signal communities collaborate on content). • Provide information in context related to current events and threats.
Presentation	• Include both active and passive measures in awareness activities. • Take into account the various learning methods, modes and media preferred across multiple generations of learners.
Effectiveness	• Develop phased implementation strategy that includes assessment methodologies and metrics collection parameters. • Establish active phishing awareness campaign as an active measure for testing and assessing end users awareness of phishing as a threat technique (senior leaders are not exempt). • Determine baseline and assess program effectiveness throughout the year (using surveys, phishing metrics, etc.).

Conclusion

A robust and proactive user awareness program, supported by the MI community working with other communities, can help to shape the culture (or mindset) of end users in a way that supports overall IA and cybersecurity efforts while supporting mission execution and day-to-day operations. By taking the steps identified above and applying prior lessons from other organizations, the Army can effectively begin to change its IA and cybersecurity culture. Because content is a key factor in the success of a user awareness program, the MI community's involvement in helping to identify and provide relevant threat information, including information that addresses threats to end users at home and during travel, is essential to both network operations and mission success.

Endnotes

1. In this case, culture is best described by Merriam-Webster dictionary as "the set of shared attitudes, values, goals, and practices that characterizes an institution or organization."

2. Notes from FCW Webcast: ''Operational Awareness: The Key to Better Cybersecurity." Speaker: Debora A. Plunkett, Director of the Information Assurance Directorate (IAD), NSA, 22 January 2013.

3. The annual requirement for IA training is mandated through the Federal Information Systems Management Act. DISA is responsible for implementing and managing DOD's IA training.

4. As of August 2012, DOD CIO was working to modify the language within DOD 8570.01-M, Chapter 6 to include additional direction regarding user awareness.

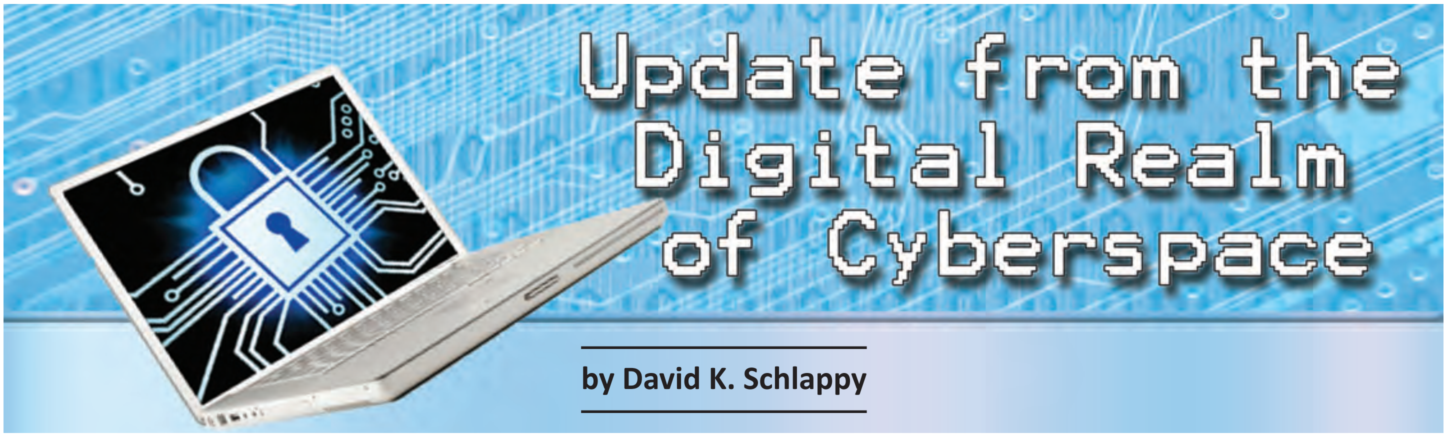
5. Based on U.S. Strategic Command User Awareness pilot findings; U.S. Coast Guard user awareness pilot; DOD CIO/US Navy co-led user awareness pilot efforts; discussions with DISA and the National Initiative for Cybersecurity Education.

6. An active approach is one that requires user interaction, a passive approach does not.

7. Methods, modes, and media are discussed within Chairman, Joint Chiefs of Staff Manual 3500.03D, Joint Training Manual for the Armed Forces of the United States, 15 August 2012.

8. Based on U.S. Strategic Command's Cyberspace Training Initiative interviews with behavioral psychologists and educators.

Jeff Hudgens supports the U.S. Army's Intelligence and Security Command Training and Doctrine Support Detachment as a senior analyst, focused on cyberspace operations and network warfare. Prior to his current position, he was the contract job manager for U.S. Strategic Command's (USSTRATCOM) Cyberspace Training Initiative (CTI), developing awareness, education and training-related products in support of combatant commands. As part of the CTI effort, he led development of a multi-faceted network user awareness campaign, focused on users in work, home, and travel settings. While at USSTRATCOM, he also worked as a cyber-requirements developer, cyber planner, and network security and accreditation analyst.



Update from the Digital Realm of Cyberspace

by David K. Schlappy

Introduction

The Department of Defense (DOD) and the U.S. Army have made significant progress within the cyber domain, but only after grappling with critical issues for many years. There are still many serious force modernization actions that still need to occur. A large portion of that effort has just begun or is soon to begin. This is an exciting effort from the DOD to Joint to Army service levels as the entire community shapes our future by building mature cyber capabilities.

This article provides an update on the actions ongoing within the cyber domain using the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) construct, and addresses some of the most recent developments regarding the cyber aspects of doctrine, organization, and personnel.

Doctrine. What's available and what's yet to be published. Joint Publication (JP) 3-12, Joint Cyberspace Operations, published 2 February 2013, is available on the SIPRNET Joint Electronic Library. JP 3-12 provides the fundamental constructs and guidance to assist joint force commanders, their staffs, and supporting and subordinate commanders in the planning, execution, and assessment of cyberspace operations.

It defines cyberspace operations as the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. It discusses and explains the Joint Staff, combatant command, U.S. Strategic Command, U.S. Cyber Command, functional and Service component relationships and responsibilities, and military operations in and through cyberspace, and it establishes a framework for the employment of cyberspace forces and capabilities.

Combined arms doctrine is coming to grips with the cyber domain and cyber activities with the introduction of cyber electromagnetic activities (CEMA). This process occurred much like the development for Information Operations. The Army codified the concept of CEMA in ADRP 3-0, Unified Land Operations, and ADRP 6-0, Mission Command. The mission command warfighting function now includes four primary staff tasks:

- Conduct the operations process (plan, prepare, execute, assess).
- Conduct knowledge management and information management.
- Conduct inform and influence activities (IIA).
- Conduct CEMA.

The Electronic Warfare Proponent Office at Fort Leavenworth, Kansas, submitted Field Manual (FM) 3-38, Cyber Electromagnetic Activities (CEMA) to the Combined Arms Center Commanding General for signature, and was signed on 25 October 2013. FM 3-38 is the first doctrine field manual of its kind, the concept of integrated and synchronized CEMA is new.

FM 3-38 provides an overview of principles, tactics, and procedures on how the Army will integrate CEMA as a part of unified land operations. At its heart, CEMA are designed to posture the Army to address the increasing importance of cyberspace and the electromagnetic spectrum and their role in unified land operations. CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare (EW), and electromagnetic spectrum management operations (EMSMO).

The Army continues to support the Secretary of Defense and joint requirements for information operations, EW, and cyberspace operations through the execution of IIA, CEMA, and the integration of 20 other information-related activities. These separate activities are tied through Mission Command, but have 21 distinctly different processes for carrying out their operating requirements. FM 3-38 will join the rest of the FMs that are a part of the Doctrine 2015 initiative.

FM 3-12, Army Cyberspace Operations, currently has an approved program directive and is under development. The

Intelligence Center of Excellence (ICoE) expects the release of the initial staffing draft of FM 3-12 to occur mid to end November 2013 and final publication to occur around the September 2014 timeframe. FM 3-12 is meant to provide a baseline of fundamental tactics and procedures for commanders and staffs regarding the employment of cyberspace operations.

ICoE has just started work on ATP 2-91.9 tentatively titled "Intelligence Support to CEMA" with an anticipated publication date of December 2015. The publication will serve as the doctrinal foundation for Army intelligence professionals and commanders at all levels and will provide the information necessary to effectively provide intelligence support to CEMA at all echelons.

It will describe the integration of CEMA into the intelligence warfighting function; outline core functions and missions of intelligence support to cyberspace operations, electronic warfare, and electromagnetic spectrum management operations, and provide specific techniques and procedures. It will also discuss the CEMA structure, organizations, and capabilities; planning and collection for CEMA; and the conduct of CEMA intelligence support for unique missions. ATP 2-91.9 will be a classified publication available on JWICS.

Organization. Pending Secretary of the Army approval, the Army plans to establish an Institutional Unit of Effort (IUE) within the U.S. Army Training and Doctrine Command to manage the DOTMLPF force modernization proponent responsibilities for cyberspace operations. A combined team from the Army Intelligence Community (HQDA G-2, the U.S. Army Intelligence and Security Command, and ICoE) will provide dedicated on-site support for the planning efforts to bring the IUE from a conceptual existence to a fully operational capability.

Personnel. As a long term objective, the IUE will provide the foundational analysis and supporting data for an informed decision on whether the Army may need to design and create a cyber career management field/military occupational specialty (MOS). However, for the MI Corps, Soldiers in MOS 35Q will be the CEMA trained personnel.

Conclusion

Changes to DOTMLPF supporting CEMA and intelligence support to CEMA will continue into the foreseeable future as the Army establishes its policies, doctrine, organizations and capabilities. The future within the cyber domain will be complex and no one has the crystal ball to understand exactly what we may face. Therefore, it is critical for the Army to continue developing flexible solutions nested with Joint cyber operations while also capturing the unique nature of Army operations.

Mr. Schlappy is a retired Army Major with 26 years of service at both tactical and strategic levels. Among his varied assignments, he served as the S2, 210 Fires MLRS Brigade, 2nd Infantry Division in Korea, the 66th MIG in Germany, and as an Intelligence Planner, J5, Multinational Forces Iraq, in the U.S. Embassy, Iraq. He currently serves in the Doctrine, Concepts, Experimentation, and Lessons Learned Branch at Fort Huachuca, Arizona with a focus on the cyber domain.

Release of MI Pub 2-01.2

The U.S. Army Intelligence Center of Excellence has published Military Intelligence (MI) Publication 2-01.2, Establishing the Intelligence Architecture, dated 4 February 2014.

MI Publication 2-01.2 is a commandant approved publication that provides a guide to planning, preparing, deploying, and redeploying the intelligence architecture from corps to maneuver company level during the conduct of offensive, defensive, and stability missions and tasks. The intelligence architecture is an important part of the overall communications architecture, which is largely dependent on organic communications capabilities at every echelon. Continuous and close coordination between the intelligence and signal staffs is required to ensure that the architecture meets the user demands.

The primary audience for MI Publication 2-01.2 includes MI officers, noncommissioned officers, and staffs from the company intelligence support team to corps, to include personnel serving in MI companies, MI battalions, and theater MI brigades. Considerations for joint and multinational operations are included. It also serves as a reference guide for personnel who are developing doctrine, leader development products, materiel and force structure, and institutional and unit training for intelligence.

To access MI Pub 2-01.2 on IKN: https://ikn.army.mil, then go to: Resources–MI Active Doctrine.

To access MI Pub 2-01.2 on AKO: https://www.us.army.mil/suite/doc/42170809.

This document is marked as FOUO. You must log in with your CAC and then copy/paste the link into your browser.

Brigadier General Bud Strom Writing Program

The BG Bud Strom Writing Program is a voluntary program open to Army MI students attending a course sponsored by the USAICoE, as well as those Army MI students attending courses at the Reserve Component Training Sites. Participation is open to the Active Army, Army National Guard, and U.S. Army Reserve.

The USAICoE established the BG Bud Strom Writing Program to:

- Raise the consciousness of MI students of the importance of good writing skills within their discipline.
- Foster the development of excellent writing skills in enlisted Soldiers and Officers, both Active and Reserve.

This Writing Program will recognize, on a quarterly basis, the outstanding writing skills of one student in each of the following categories:

(1) Category A: Enlisted Initial Entry Training (IET) Army Soldiers, both Active and Reserve, attending USAICoE-sponsored training.

(2) Category B: All other Army students, both Active and Reserve, attending USAICoE-sponsored training or training at one of the Reserve Component training sites (to include MOS-T, OES, WOES, NCOES, and Functional Courses).

To participate, students must meet the following criteria:

(1) Be enrolled as a student in a USAICoE-sponsored course or in an MI course at a Reserve Component Training Site at the time of article submission. Although the participant must be a student at the time he/she submits an article to the review board, he/she does not have to be enrolled at the time the Board meets or at the time of recognition.

(2) Must be in good standing within the course at the time of article submission.

(3) Must not be under unfavorable personnel action or UCMJ.

The CG, USAICoE, or a designated representative, will present the quarterly BG Bud Strom Writing Program Award during regularly scheduled Military Affairs Committee (MAC) luncheons at Fort Huachuca in February, May, August, and November. The top scoring papers from both categories will be published in the Military Intelligence Professional Bulletin (MIPB).

Staff Intelligence Support to Tactical Units: A Way Forward

by Captain Daniel J. Akey

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

The Current S2 Question

Does the current staff Intelligence section (S2) functionality and relationship to tactical units maximize support to those units and their operations? A fair critique of the current Intelligence support arrangement would reveal that there are several major limitations inherent in the current structure. Staff Intelligence support to the average tactical-level unit realizes neither the potential for increased and focused Intelligence support nor the potential growth of the assigned Intelligence professionals. As a result, both the unit and the Intelligence professionals suffer.

The impact of this condition is most apparent in these symptoms:

- The often anemic relationship between staff Intelligence sections and their counterparts at both higher echelons and adjacent units.
- Intelligence professionals who often possess an insufficient level of preparation and manning for optimal mission support.

The current system of staff Intelligence support also utilizes Intelligence professionals primarily as security program and training managers in a garrison environment. This arrangement forces assigned Intelligence personnel to devote large amounts of time to building relationships within a local Intelligence community (IC), often only once they have arrived in their area of operations (AO). The time lost developing the network necessary for effective Intelligence support could instead be utilized to provide more focused support of their assigned unit's mission.

The Evolution of Intelligence Support

The evolution of the Army's tactical-level staff Intelligence support should be two-fold.

- ✦ First, the functionality of the tactical-level Intelligence staff section, the S2, must be redefined.
- ✦ Second, serious consideration should be given to altering the current relationship between tactical units and Intelligence staff support.

Redefining the S2. What should be the function of the S2? Currently, Intelligence professionals are utilized primarily as security experts for the majority of their tactical careers. This is largely due to the current garrison functionality of the S2 and the fact that the majority of S2 personnel will spend the majority of their tactical time in garrison.

There is an inherent challenge with the S2 managing security programs and training in that these functions are those of the Operations section (S3) which has operational tasking authority and manages training. Since it is the S2 who currently manages security programs and training, these programs are frequently viewed and treated as being in conflict with operational training and often as secondary in priority. To the contrary, security holds a place of primacy in the priorities of work and ought to be treated with the same operational respect in a garrison environment.

The security role of S2 personnel in garrison can more effectively and efficiently be accomplished by Operations personnel. One manner in which to bring about this end state would be to use the Army Aviation model for the S2 officer in charge (OIC). In an Aviation unit the S2 OIC position prescribed by the unit's Modified Table of Organizational Equipment (MTOE) is generally a 15C35, an Aviation officer who has completed the Military Intelligence (MI) Captains Career Course. The garrison security function of the S2 position at a brigade or battalion/squadron level could be fulfilled as effectively by an officer organic to that unit's operational purpose, such as an Infantry officer for an Infantry unit or an Aviation officer for an Aviation unit. The S2 would then serve only as a security program and training section manager and become a subordinate function of the S3 as an S2/3.

Altering the Relationship. How do we shape the Intelligence staff support of tomorrow? Who will perform the Intelligence function in support of tactical units? The most significant constraints Army Intelligence professionals face with the current staff Intelligence support arrangement are personnel and practical training. S2 sections are generally small when fully manned and often lack the prescribed manning. While limited manning is frequently manageable for steady-state requirements, the impact of minimal manning is greatest with regards to the formation of soldiers. Mentorship within the MI trade is often lacking and many NCOs do not have the tactical support experience to provide adequate and informed intelligence-specific guidance. Likewise, many officers are disconnected from their peers and colleagues throughout the Intelligence field and rarely find access to mentors within the MI Corps.

Once the responsibility for security operations has been assumed by a redefined organic S2/3, Intelligence professionals can become subject matter experts (SMEs) on current and future areas of military operations. The argument could be made that the best method for facilitating this enhanced Intelligence support would more closely represent an operational control relationship in stark contrast to the current unit task organization, which incorporates assigned Intelligence personnel.

The model that ought to be adopted resembles the current weather support provided to the Army, and other branches, by the Air Force. By modifying the Intelligence staff relationship with tactical units by utilizing attached team-based Intelligence support, staff Intelligence professionals would be able to provide exponentially enhanced support to tactical units.

Attached Intelligence Teams

Experience, understanding of the AO, and communication with other Intelligence professionals looking at the same operational area are arguably the three elements most critical for the success of an Intelligence staff section. All these elements are often lacking under the current structure. A modified team-based support structure would incorporate all three elements intrinsically.

The MI Corps ought to consolidate Intelligence professionals who would, under the current system, be assigned to tactical staffs into larger Intelligence brigade support elements. It is important to note this would not impact the current Intelligence units or their missions; but would rather, affect staff Intelligence professionals otherwise assigned to non-Intelligence units. These larger modified units would have an enduring Intelligence mission in garrison, focused on developing region-specific expert knowledge.

The redefined garrison role of Intelligence professionals would effectively eliminate the AO-specific Intelligence learning curve by circumventing the tendency to treat deployment operations as on the job training. Intelligence SMEs would then be equipped to contribute advanced cultural, geographic, and political knowledge in teams attached to tactical units. In practical application, these Intelligence brigade support elements would be either consolidated in one location–perhaps Fort Huachuca, Arizona–or distributed within Major Command areas of responsibility. The teams attached to deploying units would, being organic to these larger Intelligence groups, have intimate reach-back capability incorporating tactical mission support with the enduring Intelligence mission of their owning Intelligence group. Greater integration into the larger IC is likely to follow bringing an enhanced Intelligence support network.

With comparatively unlimited personnel support, tactical Intelligence staff teams would not only have a cohesive relationship with their own team and those attached to adjacent units, but would also have increased visibility of relevant Intelligence beyond what they would likely possess in the current arrangement. Greater visibility of the "big picture" and continuous dialog would be followed by increasingly accurate assessments and predictive analysis. In essence, this modified system would be a tremendous Intelligence force multiplier.

MI Careers

The impact of this reorganization to an Intelligence professional's career would be overwhelmingly positive. The career improvements will be most evident in the enhancement of professional development. With a redefined relationship between Intelligence staff and tactical units to which they will be attached, garrison operations for Intelligence professionals will allow for greater investment in the education and training of Intelligence professionals. Continued Intelligence training will become an integral part of the battle rhythm of the new Intelligence groups, in contrast to the current system where such training is exceptionally rare due to manning shortages and garrison requirements. Also in contrast to current methodology, training will not be based on scenario information which is consistently unable to provide realistic or adequate Intelligence training.

Mentorship and relevant counseling will be dramatically increased and improved in the Intelligence professional's career, particularly in the early, most formative years. Rating schemes will also become increasingly fair for Intelligence professionals as raters and senior raters of an Intelligence background will be more deeply invested in the future of each individual Intelligence professional. In addition, the standards by which Army Intelligence professionals are measured will become more clear and quantifiable. The modified structure would also provide a significant increase in Soldier leadership opportunities for NCOs and company grade officers and provide enhanced mobility and variety of experience within Intelligence careers.

The Way Forward

Serious review should be given to the systemic limitations of Intelligence staff support to tactical units in the current arrangement as there is a direct correlation between the current understanding of S2 functionality and the limitations to effective Intelligence staff support. The first step in realizing the potential of Intelligence staff support is to reestablish the primacy of security as a priority of work in garrison by building an operational security section, the S2/3, to become the proponent for security programs and training.

Once Intelligence staff professionals have handed operational security programs over to operations personnel, due focus may be given to Intelligence training and preparation for support to tactical missions. In order to maximize the potential support and growth of Intelligence professionals, serious thought should be given to the consolidation of tactical Intelligence staff personnel and creating units with the resources, personnel, mission, and training time necessary to develop regional Intelligence SMEs capable of supporting military operations of any variety, anywhere in the world.

The way forward has limitations as does any arrangement. As with any change, there are growing pains inherent to the adoption of this plan. What this plan does, however, is solve two questions that need to be asked: How can staff Intelligence professionals better support tactical units? And how does the Army's Military Intelligence Corps better develop its leaders of tomorrow?

Captain Akey is an MI Officer currently assigned to 304th Military Intelligence Battalion stationed at Fort Huachuca, Arizona. Prior to this assignment he served over three years as the S2 OIC for 6th Squadron, 17th Cavalry Regiment stationed at Fort Wainwright, Alaska. While assigned, he deployed to northern Iraq as the S2 OIC for Task Force Saber. Prior to earning his commission in 2008 through Officer Candidate School, Captain Akey earned a degree in philosophy from Franciscan University in Steubenville, Ohio. He is a graduate of the MI Captains Career Course at Fort Huachuca, Arizona and is currently working on the completion of a Master's Degree in Intelligence Studies from American Military University.

Proponent Notes

Language Training for MOS 35M

There are two ways for 35M Soldiers to receive language training:

1. Language Training at Reenlistment: Soldiers may request language training at reenlistment. The languages available are annotated in the Selective Reenlistment Bonus (SRB) MILPER messages and are subject to change, availability, and Soldier minimum qualifications. Soldiers must request language training when speaking with retention due to the language training seats not being visible on the RETAIN system. Before a Soldier asks for the training the Soldier needs to have taken the DLAB and meet the minimum qualifications for the requested language. The majority of language training opportunities are Arabic and Persian-Farsi. This option is open for all reenlistments except for Career Soldiers (10 year +) and is the preferred method to obtain the training.

2. Language Training for Soldiers Not Within Reenlistment Window: Soldiers not currently within their reenlistment window must contact 35M Branch Management (HRC) and request training-enroute during PCS provided the language is listed on the current SRB Message. Again, the priority is Arabic and Persian-Farsi and language training seats are subject to change, availability, and Soldier minimum qualifications. Branch will assist the Soldier through the process, verify qualification and schedule the Soldier for training through ATRRS for attendance in a training-enroute PCS status.

MOS 35S Soldiers Needed for Special Forces Assignments

35S Airborne volunteers needed! The Army is looking for motivated 35S Soldiers in the rank of SPC(P) through SSG to fill the ranks of the elite Special Forces Groups. Current requirement for six SGTs and two SSGs exist within each of the Special Forces Groups. Duty assignments include Fort Bragg, Fort Campbell, Fort Carson, Eglin Air Force Base, and Joint Base Lewis-McChord. If a Soldier is in a reenlistment window, the Soldier can request for Option 3–Airborne training. If the Soldier is not in a reenlistment window, the Soldier can send the completed Airborne packet (to include an Airborne physical) to their Professional Development NCO or Assignment Manager.

FY13/14 Warrant Officer Accessions

MI met mission for all Warrant Officer MOS in FY13. The first warrant officer accession board for FY14 convened 18-22 November 2013. MI selected 38 applicants for the following MOS: 350F, 350G, 351L, 351M and 352N. MI met the accession mission for the board. The next accession board for FY 14 is scheduled for 13-17 January 2014. The following MOS will be assessed during the January board: 350F, 352N, 352S and 353T.

FY 13 Accession Mission

	350F	350G	351L	351M	352N	352S	353T
Goal	45	15	24	24	35	6	6
Achieved	45	15	24	24	35	6	6

FY 14 Accession Mission

	350F	350G	351L	351M	352N	352S	353T
Goal	35	12	22	18	32	4	6
Achieved to Date	10	4	7	6	11	0	0

The Office of the Chief, MI (OCMI) is the MI Corps Personnel Proponent office and executes the personnel life cycle management functions relative to DOTMLPF for MI and Functional Area 34, Strategic Intelligence. The USAICoE and Fort Huachuca Commanding General, as the MI Proponent, enlists the help of OCMI, to ensure the Army has the sufficient number of MI Officers, WOs, NCOs, and Enlisted Soldiers, with the correct occupational specialty, correct training, and are available for assignment at the right time.

Contact Information:

OCMI Director at (Comm) (520) 533-1728/1173

OCMI Career Management Page on IKN at

https://ikn.army.mil/apps/IKNWMS/Default.aspx?webId=2330

Military Intelligence Foreign Language Training Center

Language Action

MIFLTC Hosts CLPM Course

Mr. Robert Edwards, assistant U.S. Army Intelligence Center of Excellence (USAICoE) CLPM, facilitated a successful Command Language Program Manager (CLPM) course with the Defense Language Institute Foreign Language Center (DLIFLC) CLPM course chief, CW4 Williamson. It was conducted at Fort Huachuca, Arizona, 16-20 September 2013 and at Goodfellow AFB, Texas, 23-27 September. There were 21 students: 8 Air Force personnel, 55th ECG at Davis Monthan AFB; 7 Soldiers, 500th MI BDE, Hawaii; 6 Soldiers, Ft. Huachuca including 1, 5/104 MI BN (USAR). There were 11 students who attended the GAFB iteration.

Mr. Edwards further coordinated with the Davis Monthan CLPM to demonstrate our language materials cataloging system. Everyone who attended the training agreed that it provided current information and methods about managing an effective CLP. Some points of emphasis:

- DLI development of Commander's Training Course.
- Suggestion from DMAFB CLPM to facilitate Southwest Language Conference with area CLPMs .
- The DMAFB CLPM also suggested Ft. Huachuca and DM alternate hosting a CLPM Training MTT.
- Tailor Individual Language Training Plans (ILTP) for skill development.
- Does the CLP include training to reward as well as to remediate?
- Language proficiency is a non-linear investment. Each level on Interagency Language Roundtable (ILR) scale requires more time/ energy to achieve.

Highlights in this issue:

CLPM Course
SOCOM Course
African Languages
Language Training Corner
Level 3 Linguists
MIFLTC POCs
Website

SOCOM Conducts Advanced Course

The USSOCOM CLPMACC, *"Advanced Competencies and Problem Solving for Language Program Managers,"* 26–28 August 2013 at Davis Conference Center, MacDill AFB. Presentations addressed current language and cultural challenges facing Soldiers, Airmen, Sailors, and Marines in operational environments.

The ARSOF Language Program uses a DLI learner-centered curriculum that provides customized instruction in Arabic, Chinese Mandarin, Korean, Persian Farsi, Dari, Russian, Tagalog, Urdu, Pashto, French, Indonesian, Spanish and Thai.

Interactive web-based instruction from North Carolina State University helps students attain 2/2 with 7 contract and DLI instructors.

LREC: Cross cultural communications, 28 hrs of gen. culture, lessons learned, 40 hours required language study for 2/2 proficiency.

Other Iniatives: African Languages

The complexity of the African continent is manifest in over 2,000 languages and related cultures that are representational of Africa. Currently there have been increased concerns about the political and social instability. There have been repeated requests from language specialists for more accurate and timely language and cultural familiarization training for Africa and the Middle East.

Mombasa market

As part of the TRADOC Culture Center (TCC), the MI Foreign Language Training Center has been in the forefront of providing African Language and Cultural Awareness guides requested by linguists and non-linguists. Our access to multilingual native speakers of Hausa, Yoruba, Igbo, Bambui (indigenous name: Mbeuh) and others provide a rich resource of foundational linguistic talent. For example, our native speaker of Bambui (Mbeuh) comes from English-speaking Cameroon whose national languages are English and French. Besides French and English, he is fluent in Pidgin English and knows Bamilike and Hausa. He provided professionally recorded samples from common greetings and phrases to numeric examples. Additional language samples include Chamba and Kilba from Ghana and Nigeria respectively. We also provided assistance to other government personnel who requested samples of Tunni spoken in Southern Somalia.

A voodoo man in Nigeria

Another frequently used resource is SCOLA, with daily satellite radio and television broadcasts, on the street interviews, and language training materials in more than 150 languages including over 17 from Africa. It is used for military and civilian foreign language training and educational program developers. Our objective is to provide current language and culture solutions for our Soldiers and civilians.

Toward a Lexicon of Cultural Awareness

The Lexicon of Cultural Awareness project is a Language and Cultural Awareness Training (LCAT) application with current language samples that include selected languages from Nigeria, Ghana, Cameroon, Somalia, and Kenya. The purpose is to train non-linguists in certain linguistic characteristics to identify target languages by the smallest cluster of features they may hear from a variety of sources.

Lagos, Nigeria

The need for language triage assistive digital tools for the African continent is essential. Researchers have a scarcity of tools for professionals as stated by a linguist professional: *"Although I have varied experience with language acquisition...in the Army, it is my experience that African languages are another animal entirely."*

Goals and Products

Provide updates and complete the LCAT project currently in development for multi-platform access including mobile devices:

- ✦ Multi-platform tools for triage of language and cultural awareness training.
- ✦ Key Word Thesaurus for 40 African languages with searches.
- ✦ Terminology updates for general audiences.
- ✦ Visuals, animations, and audio mini-lectures.
- ✦ Language, culture samples database for ten selected African languages.

Mogadishu, Somalia

- ✦ New visual material with links to thesaurus entries.
- ✦ Border cultural awareness with visuals.
- ✦ Input from African language job skill professionals.
- ✦ Updated list of spoken Nigerian languages.
- ✦ Interactive Language and Cultural Awareness Sampler linked to Key Word Thesaurus entries.

Somali: Explorations in the Somali Language and Culture, R+ listening and reading comprehension. Focus: Listening comprehension in special circumstances. A self-study review course (R+) in reading and listening comprehension for sustainment, maintenance and improvement. May be used as a supplement in a teacher driven course or for outsideof class assignments.

Somali Bantu mother

Military Intelligence Foreign Language Training Center

Commander
USAICoE
ATTN: ATZS-TC (MIFLTC)
Ft. Huachuca, AZ 85613

Phone: (520) 533-2360, DSN 821
Fax: (520) 533-2751

Language Training Solutions

We're on the web!
https://ikn.army.mil/CultureCenter

Language Study Corner

*Intelligence Debriefing in Target Language (TL)**

ILR Level: 2-3

LX2-L06-004-004: Military debriefing in the TL

***TASK:** Debrief an individual in the TL who has just returned from travel to a foreign country.*

***CONDITION:** Ask another section member to simulate the role of a person who has just returned from travel to a foreign country. Ask him/her about what they saw and did each day. Determine in advance what information might be of military value and prepare your questions accordingly. You may also use a map to help the person remember where he/she has been. The debriefing should last 10-15 minutes.*

***STANDARD:** Debrief a person just returned from a foreign country. Ask him/her about the current political situation to include prominent figures, what status the military currently holds, where centers of business and communication activity are located, if there are any unusual laws or prohibitions, major transportation systems and routes, activists or activist groups, and any other information of intelligence value. Your debriefing should last 15 minutes and use current military symbols and terminology to receive a "GO."*

**https://ikn.army.mil/CultureCenter [TCC website, Language Initiatives, MIFLTC, Language Training Guide, Oral expression LX2-L06-004-004]*

***Note:** The "Language Training Guide" provides a structure to develop language training. It does not provide a lesson plan, links or materials.*

FH Linguists Surpass Army Standard

There were 52 USAICoE linguists who achieved 3/3, above the Army standard, on the most recent DLPT in Amharic, Arabic (4), Arabic-Moroccan, Arabic-Iraqi, Arabic-Sudanese (2), Chinese Mandarin (2), Korean (4), Persian Farsi (4), Portuguese, Pashto, Spanish (23), Russian (2), Tagalog (5) and Thai. These linguists represent the finest from HHC USAICoE, 304th MI BN, 309th MI BN and 344th MI BN.

The ILR sets the following standards for level 3 reading and listening:

- **Reading 3:** Reads with a normal range of speed, almost complete comprehension of authentic material on unfamiliar subjects. Includes news stories, routine correspondence, general reports, and technical material in a professional field. Almost always interprets material correctly, relates ideas and "reads between the lines." Can gist more sophisticated texts. Rarely has to pause over or reread general vocabulary.
- **Listening 3:** Understands essentials of speech in a standard dialect, technical discussions. Understands face-to-face speech, in a standard dialect on general topics of broad vocabulary with some paraphrasing or explanation. Follows conversations between native speakers, telephone calls, radio broadcasts, news stories, Oral reports, and non-technical public addresses. All forms of speech in a professional field. Detects emotional overtones and understands implications.

A DLPT may be scheduled with Fort Huachuca Education Center. The goal is to qualify 95 percent of USAICoE linguists at the 2/2 Army standard.

Moments In MI History

by Lori Tagg , USAICoE Command Historian

In June 1918, Private Edward A. Trueblood, a 24-year-old native of California, sailed to France with the 29th Engineers, American Expeditionary Forces (AEF). After training in the new specialty of Flash Ranging, he was deployed near St. Mihiel. Flash- and Sound-Ranging Sections, which reported to the AEF's G-2 and provided targeting support by determining the location and range of enemy artillery based on the flashes of gun muzzles or sound waves from artillery. Flash rangers, using simple and mobile equipment, relied on ground observations and were most effective in trench and open warfare. Sound rangers, with more sensitive equipment, found success in static warfare.

In September, Trueblood found himself in a 12-foot-diameter flash ranging post with three other soldiers determining the location of concealed enemy machine gun nests which were preventing American advancement. He soon realized the other soldiers had been killed. For the next 24 hours, Trueblood remained at his post, directing fire and protecting his instrumentation without relief because damaged communication lines made it impossible to make his predicament known. A few weeks after this harrowing experience, Pvt. Trueblood was gassed while repairing communications lines and spent the rest of the war in the hospital. He returned to the United States on Christmas Eve.

Flash ranging, a part of acoustic intelligence (ACOUSINT), was one new intelligence discipline to emerge during World War I, along with aerial photography and radio intelligence, which became mainstays of combat intelligence. Flash ranging, however, phased out as radio signals and sophisticated acoustic sensors became more effective for direction-finding.

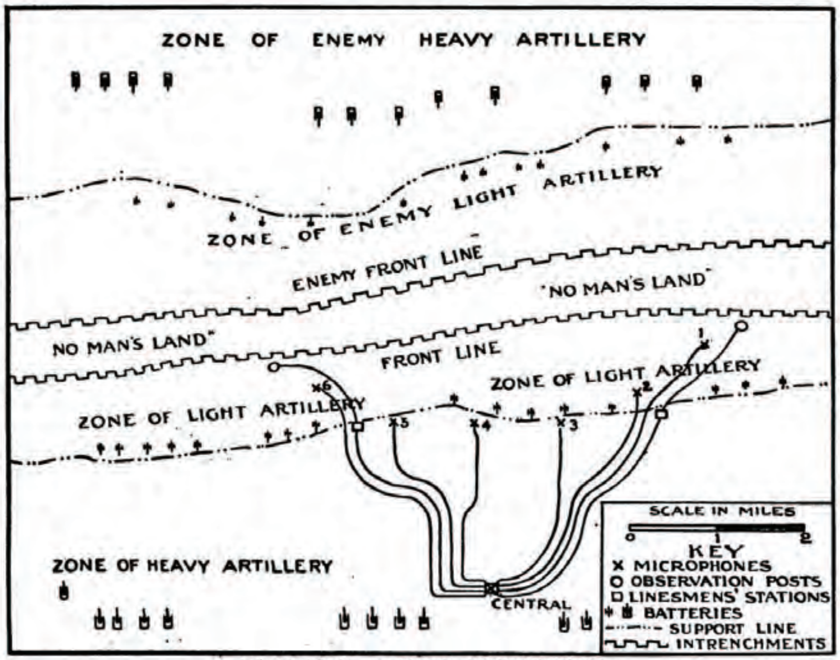


DIAGRAM OF A SOUND RANGING BASE

While all bases are not established exactly the same, a plan similar to the above is more often followed.

Culture Corner

A Dispatch from the Culture Center: Mongolian Culture vs. Money

by Timothy Baigent

Stepping out of the Chingiss Khaan airport in Ulaanbaatar Mongolia (yes, it is Chingiss not Genghis), I am struck by the smell of third world dust and cigarette smoke. There is just something about cigarette smoke outside of America that smells different. Standing with about 30 bewildered ROTC cadets amid the chaotic nature of a developing nation, my feeling of being home is in direct contrast to the dismayed look on the faces of the cadets. As I look around the parking lot we see brand new Mercedes parked next to old Soviet era jeeps held together with spare parts from whatever was at hand. I turn to the cadets "Welcome to one of the fastest growing economies in the world, you are not in Kansas anymore."

The main reason I came to Mongolia was to support the U.S. Army Cultural Understanding and Language Proficiency program (CULP). This is a fantastic forward thinking gem tucked away at Fort Knox, Kentucky with a worldwide reach and career lasting impact. CULP enriches the summers of ROTC Cadets by sending them worldwide to absorb other cultures and serve as ambassadors for the future leaders of the Army. In Mongolia we participated in Khaan Quest, a joint military exercise that combined field training with medical service to the Mongolian people.

Photo by Timothy Baigent

Author and cadets at Khaan Quest.

I came to work with the cadets but I was also on a personal quest to capture the story of an unfamiliar culture. I found a powerful story in an unusual place, the economy. Depending on how you manipulate the statistics the Mongolian economy is one of, if not the fastest growing economies in the world. This is the result of a huge mining boom that has overcome the country in recent years. Overcome is the correct word. The mining boom has created political strife in the nation, brought a significant international presence that has never been seen prior, caused the scarring of the land which is held sacred to the people, and lastly has introduced lots and lots of money into the economy. The question that formed in my mind after a few days was: Will this culture survive its own success?

Mongolian history has been a nomadic one. Some recent figures state that as much as a third of the population of Mongolia is still nomadic. They live in circular tents called *gers* and roam the vast Mongolian hills herding sheep, goats, cattle, horses, and even reindeer. Living off of meat, dairy products, and vodka they are proud of their ability to thrive where most would not last a week. Moreover, they do so with great peace when most would panic living this far out on the edge.

Ulaanbaatar is the coldest capital in the world and has given birth to a group of people that controlled more land mass than any other people in the world. As tough as these people are they are also just as hospitable. Their nomadic nature created a collectivist culture where people's doors are always open and there is a tremendous willingness to share with their traveling brethren. Unlike other nomadic cultures there is a wonderful equality between men and women. You can't help but fall in love with the people of Mongolia. Hospitable, tremendous egalitarian nature, tough as nails but tender and caring…what's not to love.

Yet there is conflict raging in the streets and fields all over Mongolia. It is hard to see as it is not fought with the traditional bows and arrows still made by hand today as seen in this photo.

Photo by Timothy Baigent

This battle is much different as it is for the very soul of the nation. The culture of Mongolia is under attack and many people I spoke with are unable to give any insight as to the outcome of this self inflicted cultural clash. Money is everywhere in Mongolia right now. Not the money of old, herds of animals, but the wealth that mining has created. There is now a stark contrast between the haves and have nots.

We arrived under U.S. Embassy escort for a meeting with a well placed official of the Mongolian National Police. The initial reason for this meeting was to expose cadets studying criminal justice to another criminal justice system. I used it as an opportunity to explore this growing problem. I took the opportunity of a pause by the speaker to ask the official what the biggest criminal difficulty they faced was. “Statistics show that most of our calls are dealing with theft.” So it seems the have nots are taking from the haves to get by. My next question was to probe the issue a little more. I asked, “What do you see as your biggest challenge going forward?” Pause for translation, pause for thought. “The future of Mongolia is very bright.” As the answer was being translated the official moved on to the next point in the presentation. I wonder if I was blown off or if there was a translation error.

I sat through another thirty minutes of slides on the structure of the Mongolian police when a student slowed everything down with a question. After the response more questions are solicited. I asked more directly now, “Mongolia has seen a large influx of money that I think may be resulting in some of the theft.” Waiting on translation… a nod of the head from the official…is that a nod of understanding of the translation or acceptance of the statement? Nothing. I continued, “I guess my question is this, the culture of Mongolia is one of great hospitality and equality. With all this new money dividing the have and have nots, is the money going to win or will the culture win and there will be a better distribution of money?” I could tell by the look on the officials face that they understood this time. They paused then started a response, “I have my personal thoughts on that.” They stop…recalibrate “As an official for the National Police I would like to refrain from answering that question.” At this point the embassy official escorting us turns and stated, “I think that is your answer.” The silence was the answer, the pain on the officials face was the exclamation point.

Is the love of money the root of all evil? On the streets of Mongolia it may not be the root of everything evil but it is the biggest issue for the National Police. I left the meeting wanting to investigate the issue further. Standing atop of a hill overlooking Ulaanbaatar my eyes moved from the Soviet era monument to the city below. There is tremendous construction underway but the real story is in the hills behind the city. These are the ger camps, people residing in tents fighting to scratch out a living in the big city. Dwelling in tents is nothing new for the Mongolian herder, doing so in the capital is. Living the traditional nomadic life is still a major part of the fabric of the culture of Mongolia. Ger vacation camps are a big business in Mongolia. That being said, many herding families are realizing that change is in the wind. If they want to provide for their family a key in this new economy is going to be education. With few educational opportunities afforded to the nomadic people they are choosing to give up their traditional life to provide these opportunities for their children. Proud herders live in the hills above Ulaanbaatar struggling to adjust their skills to the needs of a big city. As any proud parent, they make the sacrifices needed to provide for their kids’ future. They continue on even if that adjustment to the future means the death of their past.

A proud people chiseled out of the rock hard earth were able to thrive when the world threw everything it had at them. There were conflicts, yet they thrived. Living on the desolate outskirts of the coldest capital in the world eating nothing but meat and a slew of dairy products made from the animals they milked daily, yet they thrived. There was nothing the world could do to break the spirit of the Mongolian herder. This is a spirit content with so little, undaunted by some of the worst conditions nature can throw at a person. They are tough people willing to fight any foe yet kind enough to welcome any stranger. They are unshakable…that was until the earth revealed its secret deposits hidden deep under the frozen dirt. Below is a photograph that captures some of that spirit.

Photo by Timothy Baigent

Here, I was interacting with a local monk. He was nothing like the meek monks I have interacted with during my time in Southeast Asia. Although clothed in the garments of a religious leader he still keeps the boots of a warrior. His posture is hard and left my group of 30 cadets hesitant to request a photo. Knowing their culture I approached him and was rewarded with the gracious hospitality Mongolians extend to fellow travelers. I got my photo and was able to share some candy with him after. He then very willingly entertained an onslaught of photos from eager cadets that now knew, despite his tough exterior, he would not bite.

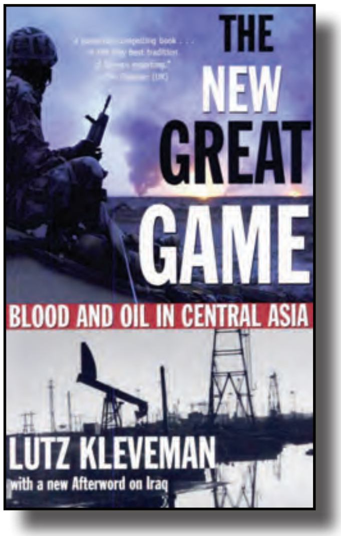
Loading into a cramped bus with more people than seats we set off to the airport. The students are elated to get home and are singing a mix of rap and country songs. I sit in with mixed emotions of missing family but savoring my last minutes in this great land. As we sit in gridlocked traffic a very intoxicated man plays human pinball as he bounces from one car to another trying to get to the bus stop on the other side of the street. My heart hurts as the voice in my head yells, "Sober up people, you are losing who you are." The world is on the brink of losing one of its last great treasures, the truly nomadic Mongolian culture. I arrive at the airport and leave the nation with a question wrapped in a slight glimmer of hope for a positive answer. "Will the Mongolian culture survive its financial success?" This hope lies in the spirit of the toughest, kindest most self-reliant people I have ever met. That spirit is captured in this final photo. As our cadets overcome the anxiety of climbing onto the top of an unfamiliar animal there sat this little child. To the utter shock of everyone the child rose and commanded the obedience of this massive beast of burden.

Photo by Timothy Baigent

With unreserved confidence he helped provide for his family by taking this cadet on a ride. When most children would run for the safety of their parents at the sight of a little bee this child shows why Mongolians are so different. Why they were able to hold more land mass that any empire in history and why the world should never underestimate what they can do.

For more information on Culture Matters call (520) 454-1234.

Professional Reader



The New Great Game: Blood and Oil in Central Asia by Lutz Kleveman

Grove Press: New York, 2003, 304 pages
ISBN: 0802141722

German-born Lutz Kleveman wrote The New Great Game: Blood and Oil in Central Asia as an examination of central Asia's natural resources, the policies regarding those resources, and the potential for border and regional violence. Although published in 2003 and somewhat dated, the views postulated are still relevant as most of the same political leaders are dealing with most of the same long-term policy challenges. Kleveman's thesis is simple: the world is addicted to fossil fuel and will pay with blood and treasure to possess it.

The U.S., Russia, China, Iran, Pakistan, India, and Europe are all vying for control of natural resources as if engaged in some great game in Central Asia and the Caucasus. The real strength of this book, and therefore what makes it a very good introduction for scholars new to the region, is its depth of first hand research. Kleveman traveled to Azerbaijan, Georgia, Chechnya, Kazakhstan, Turkmenistan, Uzbekistan, Kyrgyzstan, Afghanistan, China, Iran, and Pakistan to see how the 'game' was being played. In each of these countries he interviewed government officials, oil field workers, border guards, soldiers, aid workers, to name only a few.

Three things that all of those countries have in common are: vast natural resources, arbitrary borders, and many angry young men. The latter two are legacies from the former Soviet era. Kleveman argues that the right strategic policy decisions on the first commonality, vast natural resources, could lessen the threat of violence presented by arbitrary borders and many angry young men.

Anger and resentment against the U.S. were common results from Kleveman's interviews across the Caucasus and central Asia. In this 'New Great Game' for control of natural resources, the U.S. is considered by many to be the worst aggressor in the rush for oil. The perception, as presented by Kleveman, is that the U.S. intends to permanently remain in the region as a hindrance to Russian, Iranian, or Chinese hegemony. Other concerns over a persistent U.S. military presence include the potential for civilian violence against the U.S. followed by military action, such as a preemptive intervention.

The balance of power in the Caucasus and central Asia is delicate due to the artificially created borders, all legacies of the Soviet era. Language and ethnicity, which normally separate states, is not the case in this region. Kleveman used the borderland between Russia and Georgia as a case study in flash points. In 2002 Russian-Chechnyan rebels/terrorists were using the Pankisi Gorge of northeastern Georgia as a safe haven for training in their campaign against the Russia government. The Georgian-Chechnyans in the gorge are tribal 'Kists' and support their cousins' struggle against Moscow.

Georgian President Shevardnadze defied Moscow and refused to allow the Russian military to conduct anti-terrorist operations in the gorge. Instead, he struck an agreement with the U.S.to allow Special Forces to train Georgian military forces for anti-terrorism missions. Russian President Vladimir Putin took this as an insult and counter balanced the U.S.-Georgian training mission with the insertion of Russian Special Forces in the disputed Georgian regions of Abkhazia and South Ossetia. Although not leading to a 'shooting war' at that time, this tension underlines Kleveman's understanding that the artificial borders of the post Soviet era add to the intrigue.

The final chapter, *Angry Young Men*, is an epilogue that many may read as full of anti-American sentiment. He makes a compelling argument that American arrogance of power will potentially affect international relationships. Further, many individuals that he interviewed contend that America is using the Global War on Terror in Central Asia, to contain Russia, China, and Iran. Kleveman indicates that he senses a significant shift in the perception of the U.S. from being an admirable ally to an arrogant and aggressive power that with imperialist dreams. He is also concerned that those individuals who are disgruntled with the alliances that the U.S. continues to make with corrupt despots in the region could lead to them to embrace militant Islam and anti-American sentiments.

In conclusion, Kleveman's book is an easy way to learn about the Caucasus and Central Asia through the personal journey of a brave journalist. Lutz Kleveman traveled thousands of miles and interviewed dangerous leaders and mild mannered aid workers in order to gather impressions from the street. The theme of his book centers on the vast oil and natural gas resources of the region, the ill-accepted borders, and the angry young men who feed the regional tension. The conflicting strategic interests of the U.S., Russia, China, and Iran, Pakistan and Europe will continue to dominate this region until enduring policies, acceptable to all parties, can be implemented.

Reviewed by Colonel Daniel M. Frickenschmidt
Assistant Chief of Staff, USAICoE

Contact and Article
Submission Information

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

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

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

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

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

What we need from you:

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

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

Submit articles, graphics, or questions to the Editor at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. Our fax number is 520.538.1005. Submit articles by mail on disk to:

MIPB
ATTN ATZS-CDI-DM (Smith)
U.S. Army Intelligence Center of Excellence
Box 2001, Bldg. 51005
Fort Huachuca, AZ 85613-7002
Contact phone numbers: Commercial 520.538.0956 DSN 879.0956.

Captain Kevin M. Ryan
2013 Recipient
Lieutenant General Sidney T. Weinstein Award for Excellence in Military Intelligence

Captain Kevin Ryan was born May 29, 1984 in Boston, Massachusetts. In 2006, he graduated from Norwich University as a Distinguished Military Graduate and received a commission as a Second Lieutenant of Military Intelligence. He then completed the MI Basic Officer Leader Course at Fort Huachuca, Arizona. As part of a unique accession program, he was selected to serve with the 75th Ranger Regiment and subsequently completed Airborne School and Ranger School. In 2007, he served a one-year tour in South Korea as the S2 for 4th Squadron, 7th Cavalry Regiment, 1st Heavy Brigade Combat Team, 2nd Infantry Division. As the Senior Intelligence Officer for the Brigade's Reconnaissance Squadron, he led air and ground collection missions along the DMZ in support of the Division Commander's PIRs.

From 2008-2010, CPT Ryan served as Assistant S2 for the 2nd Ranger Battalion, 75th Ranger Regiment in Fort Lewis, Washington. He deployed twice as part of a Joint Special Operations Task Force and in January 2009 served as a Deputy J2. He was the senior Army intelligence officer in a U.S. Navy Special Operations-led task force. This joint team developed actionable intelligence that led to the apprehension of more than 100 high value targets and the reduction of a deadly explosively formed projectile cell in Baghdad.

During a subsequent deployment, CPT Ryan served as the senior intelligence officer on an expeditionary Special Operations Task Force in Afghanistan, responsible for direct action raids in Regional Command East. He led a small team of analysts and collectors who developed targetable information on some of the most dangerous insurgents in Eastern Afghanistan. This unique team had the highest kill/capture success rate in the entire Special Operations Task Force serving Afghanistan.

After graduating in the top five of his MI Captains Career Course, he was assigned to the 1st Squadron (Airborne), 91st Cavalry Regiment (1-91 CAV), 173rd Airborne Brigade Combat Team, in Schweinfurt, Germany. In July 2012, CPT Ryan and his intelligence team deployed with 1-91 CAV to Logar Province, Afghanistan. His team managed ISR assets and provided intelligence support to 10 brigade-level operations, more than 50 squadron operations, and hundreds of troop operations. Intelligence-driven operations in Logar led to the kill/capture of more than 50 insurgents, the disruption of countless improvised explosive device (IED) and indirect fire attacks, and the complete destruction of a high profile attack/vehicle-borne IED network. Furthermore, CPT Ryan provided the necessary intelligence to close and transition three major combat outposts successfully. In December 2012, he was selected to command the 173rd Airborne Brigade Combat Team's Intelligence Company.

CPT Ryan is a graduate of Ranger School and Jumpmaster School. His awards include the Bronze Star Medal with one Oak Leaf Cluster, Army Commendation Medal with one Oak Leaf Cluster, Iraq Campaign Medal, Afghanistan Campaign Medal, Korea Defense Service Medal, Combat Action Badge, Ranger Tab, and the Basic Parachutist Badge.

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

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

PIN:103945-000