

MI Professional Bulletin

April - June 2015
PB 34-15-2

Hybrid Threat

Information Operations

Cyber

VBS2
U.S. ARMY



Intelligence Challenges



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 is 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 Scott D. Berrier

Chief of Staff

COL Todd A. Berry

Chief Warrant Officer, MI Corps

CW5 Officer Five Matthew R. Martin

Command Sergeant Major, MI Corps

CSM Jeffery L. Fairley

STAFF:

Editor

Sterilla A. Smith

usarmy.huachuca.icoe.mbx.doctrine@mail.mil

Design and Layout

Gary V. Morris

Cover Design

Gary V. Morris

Military Staff

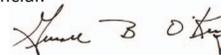
MAJ Craig T. Olson

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
1514001**

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

From The Editor

As a reminder, MIPB is now online at IKN on the open front page at <https://www.ikn.army.mil/apps/IKNWMS/Default.aspx?webId=2248>. You will find several of the most recent issues there as well. For earlier issues (2013 and earlier) please go to the MIPB site on IKN after you CAC in.

The following themes and suspenses are established for:

July-September 2015, *Reserve and National Guard*, deadline for submissions is 21 May 2015 (closed).

October-December 2015, *Intelligence Support to Situational Awareness in 2025 and Beyond*, deadline for submissions is 2 September 2015.

January-March 2016, *Institutional Training*, deadline for submissions is 11 December 2015.

April-June 2016, *Considerations for Separate Brigades' Intelligence Teams*, deadline for submissions is 3 March 2016.

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.

Please call or email me with any questions regarding your article or upcoming issues.

In the January-March issue I attributed authorship of the article "The One Army School System" to John Craig. This is incorrect. The author was Major Sarah E. Fraticelli, RC Branch Chief, TDID.

Sterilla Smith
Editor



FEATURES

- 5 Theater Collection Battalion Team Validation: Anchor Point Operations with Regionally Aligned Forces**
by Major Jason Buchanan and Captain Charles Lewandowski
- 10 Becoming the Regionally Aligned Intelligence Force**
by the 4th Infantry Division G2 Section
- 14 Decisive Action and the Corps G2**
by Colonel Jim Sisemore
- 18 Establishing the Intelligence Architecture and Tactical Communications Plan in a Multinational DATE Exercise**
by Captain Benjamin A. Smith
- 23 Why COIST Matters**
by Victor R. Morris
- 28 The Future of Tactical intelligence: 5 Ways to Meet the Challenge**
by Colonel Todd A. Megill (USA, Ret.) and Colonel Stephen P. Perkins (USA, Ret.)
- 36 Living Up to Its Legacy: GRCS PED Innovation for Complex Operational Environments**
by Sergeant Michael Peralta, Sergeant Christopher Dake, and Chief Warrant Officer Four Ross W. Glidewell
- 40 Enabling Decision Confidence by Mitigating Four Interacting Dilemmas Facing the Army Intelligence Enterprise**
by Colonel Nichoel E. Brooks and Jami Forbes
- 44 Intelligence Support to CENTCOM Materiel Recovery Element**
by Major Joshua J. Smith
- 49 Intelligence Challenges in Eastern Afghanistan**
by Lieutenant Colonel Jim Reed, Major Ken Wright, and Chief Warrant Officer Four (P) Erin O'Hara
- 54 Use of SIMEX Can Maximize Training Opportunities for MI Soldiers**
by Major James Welch and Chief Warrant Officer Two Kirk McKenney
- 57 Vigilant Pacific: 205th MI Battalion Enhances FVEY Partnership and Interoperability in the Pacific**
by Captain Brian Vaeni
- 60 Online Radicalization**
by Captain Michael C. Wigley
- 64 Lessons Learned: Managing Linguists**
A Collaborative Effort by Corporal Thomas Warden, Specialist Cameron Severts, Captain Matthieu Ruiz, Captain Lauren Nowak, Mr. James Marcil, Major Jonathan Beckmann, Major Timothy Hunt, and Lieutenant Colonel Jay Haley
- 68 Ensuring Operational Readiness through Mission Command Principles**
by Captain Douglas W. North
- 70 Enhancing Adult Learning within the MI Warrant Officer Advanced Course**
by Chief Warrant Officer Three LaMesha Craft and Mrs. Rose Phillips

DEPARTMENTS

2 Always Out Front
3 CSM Forum
4 Technical Perspective
73 Training Development and Support Directorate

76 Culture Corner
78 Moments in MI History
Inside Back Cover:
Contact and Article Submission Information

Always Out Front

by Major General Scott D. Berrier
Commanding General
U.S. Army Intelligence Center of Excellence



I am excited, humbled, and honored to take command of the Intelligence Center of Excellence at this important juncture in our Army's history. Fort Huachuca and Team Huachuca have grown to masterfully meet the Army's needs during a long period of conflict. Together with DA G2, INSCOM, the rest of the Army intelligence community, and the Joint intelligence community, we will continue to move Military Intelligence forward to meet the ever increasing demands on intelligence in the future.

This issue's theme is *Overcoming Intelligence Challenges*. One of the largest hurdles we will face as an Army, and as MI professionals, is how we overcome day-to-day and long term adversity and challenges. The world has indeed changed in recent years, it is highly complex and evolving by the second. Enabling our future MI force to more effectively and efficiently process, exploit, and analyze information from multiple disciplines is vital to accomplish our diverse missions. *TRADOC Pamphlet 525-3-1, The U.S. Army Operating Concept (AOC)*, 31 October 2014, challenges the Army not only to win in a complex world, but to prevent conflict and shape security environments, all while operating as part of our joint force with multiple partners. While that sounds easy, with the AOC's directive comes tremendous challenges for Army intelligence professionals.

Similar to the development of a rigorous PT program, the skills necessary to overcome challenges need to be thoughtfully exercised. First you have to understand the guidance and direction provided by your higher headquarters. Then you develop a road map to accomplish your commanders' intent. Early in the process you must look for roadblocks, hindrances, and limitations that will prevent your success. Simple tasks such as ensuring your systems are not out of date, training certifications are in place, and understanding your unit's priorities are crucial. Make sure the routine things are done routinely; then you are ready to tackle the unforeseen and complicated challenges as they arise. Furthermore, we must try to change our perspective. It's difficult to abandon the comfort of routine, but intelligence must reflect the changing world in which we operate, we must be postured to change with it.

Technology will challenge us in every aspect of intelligence. The rapid evolution in information and telecommu-

nication technology has fundamentally transformed the operational environment in which we operate. Mankind produces more information at a faster rate and from more devices than ever before. Personal computers, cell phones, and the internet have allowed individuals to not just "be reached" but "to reach out" to vast numbers of people. Nonetheless, we must view technology as an opportunity, not a challenge. The same technology we see as one of the many intelligence challenges may be used to protect our own information systems, conduct advanced analytics, and improve dissemination of products to users in the field.

Yet another challenge we face is our reliance on technology to assist us in our analysis. Critical and creative thinking is essential to the development of skilled analysts and we cannot rely solely on technological tools to develop our conclusions. Critical and creative thinking are often viewed as opposites; the creative thinker has wild, off-the-wall impractical ideas while the critical thinker is serious, deep, and analytical. Consider, instead, these two ways of thinking as complementary and equally important. They need to work in unison to connect the seemingly unconnected and to add value to the challenges we face to effectively fuse ideas from different perspectives and disciplines. Only when we combine deep analytical thought with the advantages of our robust technological toolsets can we anticipate and meet the needs of the commander.

Intelligence challenges are enduring problems and are routinely difficult to overcome. However, our vision is clear and we know where we want to go. Every challenge and every difficulty we successfully confront, serves to strengthen our will, confidence, and ability to conquer future challenges—it simply makes us who we are and the best at what we do. Herodotus, the Greek philosopher, said, "Adversity has the effect of drawing out strength and qualities of a man that would have lain dormant in its absence." As we forge ahead, intelligence professionals will have to train more effectively, run faster, and think harder not only to predict particular events, but to spot, track, and interpret trends and patterns in a rapidly changing and unique world. 

"Always Out Front!"

CSM FORUM

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



Team,

Please see the note below from the Military Intelligence Noncommissioned Officer Academy (NCOA) here at Fort Huachuca. This is important information that needs to be shared at all echelons.

The Advanced Leader Course (ALC) and Senior Leader Course (SLC) are required institutional training and professional military education that prepare NCOs to assume the roles and responsibilities of SSG and SFC. However, there has been a trend of unfilled training seats for these courses at the NCOA. In FY 2014, MOS 09L, 35F, 35G, 35L, and 35M ALCs graduated less than 80 percent of the required graduation quotas. For FY 2015, based upon completed courses and current course reservations, only SLC and the 35F ALC are projected to meet 80 percent of the required graduation quotas. Projections also indicate the MOS 35L and 35T ALCs will meet less than 50 percent of the required graduation quotas.

Units must send their eligible personnel to NCOES at the first available opportunity. We are hurting and hindering the development of our NCOs by not ensuring their availability and readiness to attend NCOES courses. Leaders need to be proactive and plan ahead to ensure their NCOs are prepared to go to school and complete course requirements, such as meeting the Army body composition standards IAW AR 600-9 and passing the APFT. These two issues have been the primary reasons NCOs do not graduate ALC and SLC once they arrive. We are here for you and your NCOs should you have any questions or concerns.

Thank you for what you do every day for this great country and for the MI Corps. Please visit my website on IKN for the latest updates concerning the Force and our Corps. 

Always Out Front!

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

USAICoE Critical Task Site Selection Board Schedule				
MOS/AOC/SI	Tentative Date	Type	Location	Concentration
35P	19-23 October 2015	Full	Goodfellow AFB, TX	SIGINT Cryptologic Linguist
09L	16-20 November 2015	Full	Lackland AFB, TX	Interpreter/Translator
35M/351M/35F	1-12 February 2016	Full	Fort Sam Houston, TX	HUMINT Collector/Officer
WOAC	22-26 February 2015	Full	Fort Huachuca, AZ	MI Warrant Officer
SI-1D	March 2016	Full	IKN/ISN-Virtual	GEOINT Imagery Officer
35Q	March 2016	Full	TBD	Cryptologic Network Warfare
FA 34	June 2016	Virtual	N/A	Strategic Intelligence Officer (SIOC)
35D (AOC)	August 2016	Full	TBD	MI Officer
SEMA	November 2016	Virtual	IKN/ISN-Virtual	Aviator, MI Tasks



Technical Perspective

Chief Warrant Officer Five Matthew Martin
U.S. Army Intelligence Center of Excellence



It is an honor and a great privilege to be selected as your 6th Chief Warrant Officer of the Military Intelligence (MI) Corps. As I look forward to my new role and the opportunity that stands before me, I must reflect on the Warrant Officers that came before us and the dynamic changes within our Warrant Officer Cohort. It's easy to see that the MI Warrant Officer has evolved into the military's premiere technical leader. This evolution is associated with many different events but most notably is the last 13 years of war. Persistent conflict in Afghanistan and Iraq brought a dynamic change which led to Warrant Officers taking an increasingly active role as diverse and specialized leaders in combat.

Today's Warrant Officers are adaptive technical experts, combat leaders, trainers, and advisors. Senior leaders seek to leverage our knowledge, skills, and abilities to lead formations of intelligence professionals, providing clarity within an exceedingly complex environment. Currently, we are faced with an operational and environmental landscape that is fiscally constrained, subjected to manpower reductions, with a high operational tempo and adversaries that seek to challenge our resolve and reduce our ability to maintain the initiative.

Given these variables, we must embrace an environment that continues to change and we must collectively rise to the challenges of tomorrow. To meet the increasing needs, our Warrant Officers must be transformational and multidimensional leaders, technically and tactically relevant, and embrace a profession that demands lifelong learning to successfully operate at all levels of Army and Joint Interagency, Intergovernmental, and Multinational environments.

To lead our MI Warrant Officers I want to share with you some of my thoughts that will ultimately shape my themes, goals, and objectives.

1. **Communication.** As an essential element of our success, we will continue to enhance our communications through the Senior MI Warrant Officer Forum and the Intelligence Leader Development Resource (iLDR) website.* These key venues facilitate discussions with senior leaders and develop a network of senior Warrant Officers across all MI formations to gather and communicate our message.

2. **Collaboration.** To effectively pursue initiatives or resolve current and future challenges we must achieve greater collaboration. Through a collective and cohesive team we can innovate, solve complex problems, exchange knowledge, and posture our cohort to effectively support our current and future force.

3. **Talent Management.** To improve our talent management processes, we need a holistic approach that places our best qualified Warrant Officers into carefully selected assignments and progressive professional development opportunities where they can best serve the Army, gain critical experience, and effect change.

4. **Force Structure.** To posture our Warrant Officers at the point of greatest need, we must conduct an all-inclusive grade and position (W01-CW5) review. To the greatest degree possible, we must align Warrant Officer assignments and create positions to optimize experience and opportunity.

I am extremely proud to represent the MI Corps and I look forward to meeting and working with each of you in the near future! 

*<https://www.ikn.army.mil/apps/iLDR>

**Always Out Front!
This We'll Defend!**

Theater Collection Battalion Team Validation: Anchor Point Operations with Regionally Aligned Forces



by Major Jason Buchanan and Captain Charles Lewandowski

Background

The US Army Europe (USAREUR) deployed forces from the 173rd Infantry Brigade Combat Team, Airborne to four Baltic states and Poland in late Spring 2014 to demonstrate U.S. continued support to the collective security of our NATO allies in light of on-going actions by Russia in Crimea and Ukraine.¹ The U.S. took several immediate steps to demonstrate solidarity with our NATO allies such as augmenting the air, ground, and naval presence in the region, and enhancing previously scheduled exercises. These exercises are known as Operation ATLANTIC RESOLVE (OAR). The purpose of OAR now and into the future is to continue to demonstrate U.S. resolve to NATO allies and reassure the alliance that the U.S. is committed to meeting our nation's Article 5 obligations.² OAR will be a series of rotating regionally aligned force (RAF) units through the Baltic States for the foreseeable future.

Framework for Sustained Support to OAR

Many of the 173rd IBCT (A) deployments to Poland, Latvia, Lithuania, and Estonia under OAR were short notice deployments with little intelligence preparation of the operational environment (OE). Thus, several intelligence teams from the 66th Theater Intelligence Brigade's (TIB) collection battalion, the 2^d Military Intelligence (MI) Battalion, deployed with the 173rd IBCT (A) to assist in identifying threats and force protection (FP). Several problems immediately became clear for the TIB. First, how does the 66th TIB maintain the capacity to deploy trained and validated intelligence teams to OAR? How do the TIB teams integrate with the various RAF elements for the duration of the operation? Lastly, how does the 66th TIB maintain enduring support to both OAR and support to FP at USAREUR, while simultaneously maintaining a deliberate emphasis on professional development, schooling, training events, and continual personnel turnover?

2^d MI Battalion realized long before OAR the need to maintain trained and validated intelligence teams to support the myriad requirements emerging from both USAREUR and U.S. Army Africa (USARAF). The Battalion has incredibly skilled and talented warrant officers, officers, senior NCOs, and MI Civilian Excepted Career Program (MICECP) participants who remain operationally engaged at the field offices on a daily basis. However, the Battalion has an even greater number of junior soldiers working at the operational level who have far less required experience to perform in the same environment, or to be able to deploy in the absence of a senior mentor while performing at the same high level. Whether it is the junior enlisted Human Intelligence (HUMINT) Strategic Debriefer in the Balkans, or the young sergeant in his first assignment as a Counterintelligence (CI) Probationary Program (CIPP) Agent in a field office, the challenge is the same: *How do we generate and sustain intelligence capacity capable of performing at the operational and strategic intelligence level?*

Historically, the field office is 2^d MI Battalion's intelligence platform for launching and performing Title 10 operations. (Figure 1 shows the battalion's geographic dispersion of its multiple field offices.) These field offices offer excellent venues for intelligence personnel to perform their skills as a variety of intelligence collective and individual tasks occur daily. However, there are a number of tasks not performed within them, and when there is a mission to deploy outside of a field office it is often made up of a team of intelligence personnel from different field offices. Considering that 2^d MI Battalion maintains field offices and not tactical CI teams, it became imperative for the Battalion to develop a validation process to ensure each Soldier was trained and ready to deploy to meet varied mission sets.

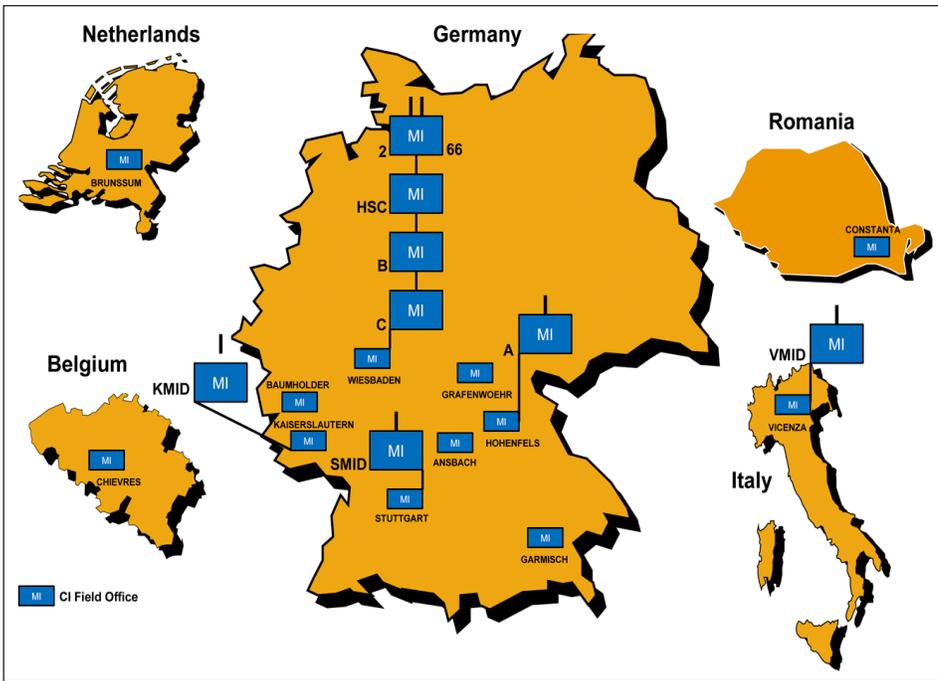


Figure 1. 2^d MI Bn Area of Responsibility.

Building Tailored Teams

When building a CI or HUMINT team, the Battalion and Company leadership considers variables such as individual skills, experience, duty location, availability, and degradation to the field office. Each team is tailored to meet the particular mission requirement. While CI and HUMINT soldiers working in the field office are operationally engaged on a day-to-day basis, Company and Detachment commanders also ensure that all Soldiers meet standard training requirements in all mission essential and warrior tasks

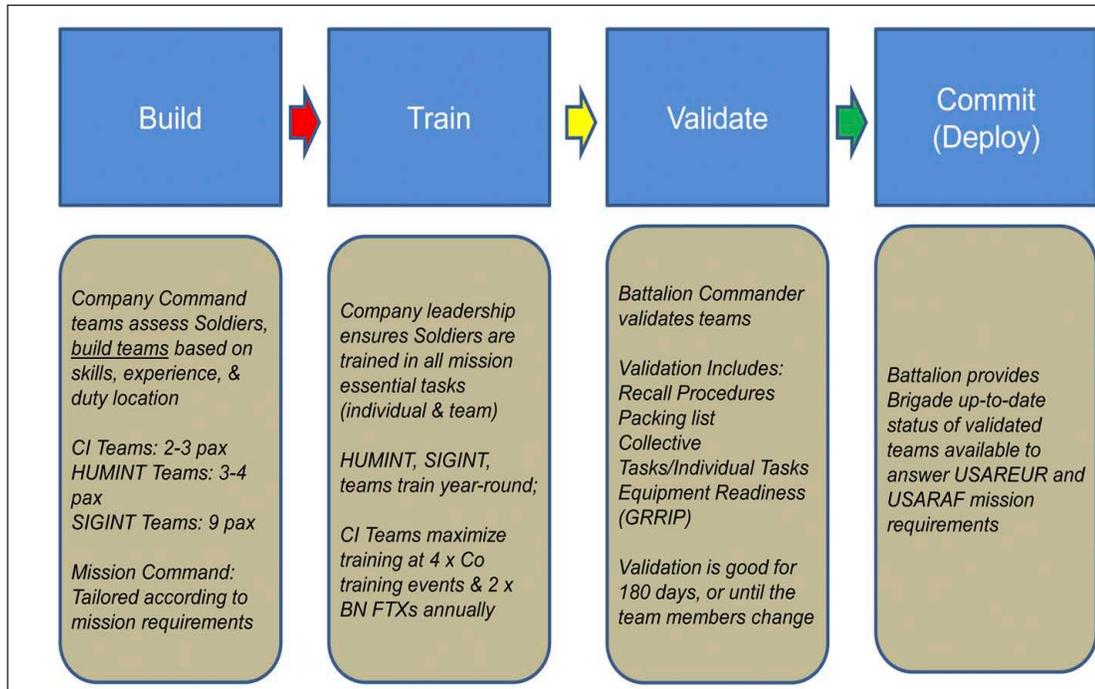


Figure 2. 2^d MI Battalion Semi-Annual Team Validation Process.

through quarterly Company training exercises. Each of these events culminates in a semi-annual battalion validation exercise, which serves to validate each CI and HUMINT Soldier in respective critical tasks. (Figure 2 captures the 2^d MI Battalion process to generate validated teams.) Validation remains in effect for 180 days. Therefore, any given field office becomes the platform from which validated CI and HUMINT Soldiers form deployable teams.

2^d MI Battalion conducted its first validation exercise to train intelligence teams in May 2014 just prior to the start of OAR. The May 2014 validation exercise revolved around a scenario specific to one of the many contingency plans (CONPLAN) for which it main-

tains intelligence teams. Though the scenario differed from OAR, many of the collective and individual tasks remain relevant to both types of intelligence operations. The Battalion conducted the validation exercise in the Baumholder Training Area (BTA), bringing in intelligence teams from the Battalion's field office platforms and detachments.

The Battalion formed intelligence teams on Day 1 and briefed each team on the scenario and flow of the exercise on Sunday night. On Day 2, each team developed an intelligence update and prepared to move into the BTA MOUT

site to meet with the many role players with varying personality roles from both 650th MI Group and 66th TIB. An Observer Controller (O/C), internally sourced from 2^d MI, shadowed each team armed with the scenario, a list of individual and collective tasks, and a Go/No-Go checklist to assess whether the team met the necessary gates for validation. O/Cs conducted any necessary retraining on the spot or into the evening. As teams progressed through the scenario meeting sources,

host nation liaison, and debriefings, each day culminated with a brief to a senior member of 2^d MI, which further developed our junior Soldiers' briefing skills and confidence.

At the end of each day, and again at the end of the week, 2^d MI leadership and each O/C met to assess the progress of each team's validation. The Go/No Go checklist provided the quantitative team assessment while daily briefings to Battalion leadership provided the qualitative evaluation leadership used to assess validation. The weeklong validation exercise resulted in a comprehensive approach by which the Battalion Commander could confidently validate each team for a future deployment in support of a RAF element, a CONPLAN, or other operational tasking in either USAREUR's or USARAF's areas of operation.

Nearly one week following the validation exercise OAR began and eight intelligence teams began deploying into the Baltic States in support of 173rd IBCT (A). The validation process proved highly successful with intelligence operations progressing on several fronts. The next challenge for the collection battalion involved the long-term integration and support to RAF units. OAR creates unique challenges for units considering some elements have a constant, yet rotational, presence during the operation as opposed to other elements whose presence emerges through various joint exercises. 2^d MI Battalion used a three pronged strategy to integrate intelligence teams into these varying units starting with an offset intelligence team rotation, integrating the RAF concept into the battalion's validation exercise, liaison with country teams, secure communications, and lastly through live environment training (LET) in one of the Battalion's intelligence platforms.

Enduring Operations: OAR

"OAR is going to be around long after everyone in this room rotates out of Germany," stated LTG Hodges, the USAREUR commander, during his in-brief with 66th TIB. While RAF units rotate in and out of the Baltic States, 66th TIB intelligence teams remain as an anchor point to assist them. The first way 2^d MI anchors intelligence teams with units includes offsetting our intelligence team rotations with RAF unit rotations. Thus far, most units rotate on a 90-day rotation in and out of Baltic States. Therefore, 2^d MI follows the rotation of units closely and offsets intelligence team rotations to ensure an experienced team remains in each supported nation state to brief rotational units and maintain continuity with both host nation forces and RAF units.

Intelligence team activities with the RAF units vary, depending on the discipline of the team. Some teams live with the units in barracks and attend daily synch meetings to keep the commander advised of the threat. Other

intelligence teams conduct FP for the units through liaison with host nation, country teams, and U.S. embassies. These teams accomplish their tasks by living on the economy away from the unit in hotels or apartments, working with the host nation to identify threats. These teams still maintain contact with the local commanders due to their operational relationship, but accomplish more for FP through their other host nation and embassy contacts in OAR.

Fall 2014 Validation Exercise

After the first rotation of intelligence teams through OAR, 2^d MI realized the need to address some shortfalls during the next battalion validation exercise in Fall 2014. Several of these shortfalls included younger Soldiers understanding the varying personalities of the embassy, debriefing techniques, technical understanding of communications systems, and managing the relationship with the RAF units. This required modifying the scenario to an OAR-specific situation with in-depth roles incorporating the different embassy staff personnel. The OE needed more depth to include foreign intelligence entities, terror groups, and a criminal network. Lastly, Battalion leadership needed to incorporate some RAF elements to assist with debriefings and even potentially link up with their intelligence teams.



A 2^d MI Battalion HUMINT team meets with its O/C to receive an AAR at the Baumholder training area from 25 September – 3 October 2014 during the Battalion validation exercise. Photo courtesy of the Baumholder Training & Audiovisual Support Center.

Many after action reviews with teams rotating out of OAR revealed that most teams did not understand the basic structure of the embassy staff at the outset of their deployment, nor the key personnel they needed to interact with in order to be successful in their mission. Thus, the Fall 2014 validation exercise scenario developed in-depth roles for embassy personnel to include the Defense Attaché Office, the Regional Security Office, Legal Attaché, and Military Liaison Officers. Additionally, instead of a time centric scenario where role players came to the teams as walk-ins or potential sources, the Fall validation exercise allowed for a fluid scenario where teams decided when and with whom they needed to talk. The result was a dynamic scenario that challenged teams to think for themselves while forcing

them to coordinate with the proper embassy personnel or local liaison engagement, or fail to identify a piece of necessary intelligence due to a lack of coordination.

The Fall validation exercise expanded the OE scenario to match the multi-faceted operational situation OAR teams face in order to create adaptive teams that could think critically in the Baltic States. One layer included the many threats from foreign intelligence entities collecting on U.S. forces and the teams themselves. Another layer included the potential for terrorist groups operating in the area. While this threat is not immediate in OAR, the potential always exists and an additional layer was added to the complexity of the OE situation to develop critical thinking. Lastly, the scenario included roles for criminal networks in order to capture the varying levels of organized crime that exist in some of the Baltic States with the potential nexus to CI threats. Each day of the validation exercise the scenario inundated intelligence teams with information regarding these networks and each night the teams sorted out the scenario and updated the battalion leadership.

Most RAF train-ups at home station or in Germany include collective training for combat arms tasks, but often lack specific collective tasks for intelligence teams. This is a shortfall identified at the European Foundry Platform where even intelligence training is tailored depending on the intelligence disciplines. With OAR rotations set and future RAF units identified, it became easier to reach out to the intelligence personnel in the units and offer their intelligence teams the opportunity to participate in 2^d MI's validation exercise. 2^d MI offered intelligence teams from 1/1CAV and 2CR, the next two rotational RAF units, the opportunity to train at the validation exercise. Both units accepted and sent teams through the Fall validation exercise. This exercise allowed both units to gain unique training through an exercise tailored to their future mission in OAR and allowed each of the units to put names to faces considering 2^d MI would soon support them during future rotations.

Other Considerations

One way intelligence teams report the intelligence they discover on these threats while in OAR is the Global Rapid Response Information Package (GRRIP). However, the GRRIP is a technically complex system that can require help desk assistance with the most menial tasks. Considering the multiple issues with GRRIP the battalion incorporated sustainment training into the validation exercise. The sustainment training involved teams fresh from rotation (and now subject matter experts on the system), giving classes on their best practices with key tasks including establishing communications and keeping the systems working. This training



A RAF HUMINT Team meets with a member from their unit to conduct a debriefing at the Baumholder training area from 25 September – 3 October 2014 during the Battalion validation exercise. Photo courtesy of the Baumholder Training & Audiovisual Support Center.

proved vital to RAF intelligence teams as well. The result of training proved useful as 2^d MI Battalion's intelligence teams are the only teams communicating with secure means while in the Baltic States. Additionally, 2^d MI Battalion now provides GRRIP to RAF units through the anchor point concept so they can communicate in allied NATO training areas as well.

2^d MI provides other opportunities to integrate RAF units through the battalion's many intelligence platforms across Germany, Italy, and Belgium. RAF intelligence soldiers can participate in LET opportunities in one of the many field offices, working alongside 2^d MI Soldiers and MICECPs. These LETs provide RAF Soldiers the opportunity to conduct host nation liaison, covering agent program, strategic debriefing, and report writing under the tutelage of senior intelligence personnel. A LET is the perfect precursor to OAR considering RAF soldiers also get to experience the reporting process through USAREUR G2X.

2^d MI Battalion's field offices provide the intelligence teams that protect USAREUR's missions, facilities, families, and soldiers, and also provide the intelligence teams that support operations like OAR. Instead of dedicated intelligence teams housed in barracks awaiting deployment, 2^d MI's teams remain engaged daily conducting intelligence operations on a variety of fronts. Thus, the final challenge 2^d MI faces while supporting OAR is maintaining that long-term support while also maintaining support to ten field offices in four different nation states across Europe. 2^d MI accomplishes this though creating composite teams, the battalion's semi-annual validation exercise, and maintaining an active order of merit list (OML) of deployments for both MICECPs and soldiers.

By the third OAR rotation, 2^d MI Battalion had to rotate eight CI Agents every 179 days from the field office platforms. Since field offices maintain a persistent mission to provide Title 10 CI support to FP, sustaining both Title 10 support and OAR became untenable. CI Agents are a finite resource, and reducing an entire field office's capabilities is impractical. Therefore, in an effort to accommodate both enduring mission sets, the Battalion exercised the art of command by creating composite teams comprised of one HUMINT soldier paired with one fully credentialed CI agent or MICECP to deploy to OAR. This effort alleviated the manning constraints by mixing intelligence disciplines forward in OAR, while also keeping the same intelligence disciplines operationally engaged in protecting USAREUR garrisons in the rear.

Maintaining the composite team concept poses a unique challenge in itself. Each CI Agent, HUMINT Soldier, and MICECP must be eligible to participate in OAR based on the OML. 2^d MI accounts for this through the semi-annual validation exercise by creating a training scenario that encompasses individual MOS specific tasks and collective tasks associated with OAR. These exercises keep Soldiers' collective and individual tasks trained, while keeping them thinking critically outside of their normal duties in the field office. The validation exercise also allows a dispersed battalion to come together twice a year to train and share best practices from across the unit. An additional purpose the validation exercise serves is bringing intelligence Soldiers from varying duty locations together for training. Considering that is how they deploy. Teams often comprise a member from each field office, considering the cost to a field office if two personnel deployed from one office at a time. Lastly, the varying scenarios ensure that intelligence professionals remain challenged and agile against the vast emerging threats they face.

An active OML including both MICECP and Soldiers is imperative to maintain intelligence team rotations in and out of OAR and other deployment requirements while maintaining the requirements to each garrison through the field offices. 2^d MI currently rotates teams through OAR every 120 days. This keeps the rotations offset from the RAF and teams under the 179 temporary change of station requirements. Initially 2^d MI sought to deploy only Soldiers to OAR with MICECPs maintaining continuity in the field offices, but soon realized there are simply too few Soldiers to maintain that type of cycle. Thus, MICECPs started rotating through, which allowed these civilians to gain a holistic set of intelligence skills and bring those skills back to the platforms. This OML keeps Soldiers and MICECP rotations fair and all

members of the team mentally fit with rotations every third or fourth time.

Conclusion

The combination of these four personnel measures ensures that 2^d MI Battalion maintains an operational presence in OAR for the expected long duration of the operation. Without measures like an OML, MICECP and Soldier rotations, the validation exercise, and composite teams one mission would surely suffer. However, the priority of both OAR and FP support to USAREUR garrison are both too important to fail.

USAREUR is using OAR to usher in a new era of theater security cooperation across Europe. The Baltic States are just the beginning. Long term, OAR may encompass a mixture of persistent and intermittent presence in nation states throughout Europe through RAF elements engaged for 90 plus days or simply a team of RAF elements conducting a joint exercise. As 66th TIB continues its transformation into the TIB for Europe, the unit faces several other challenges to provide an anchor for RAF unit integration into Europe while remaining constantly engaged in multiple forward deployed locations to counter potential threats. Measures such as the semi-annual validation exercise, RAF integration into the validation process, deploying composite teams, an OML, communications systems training, and off-setting intelligence teams ensures that 66th TIB maintains the multiple competing priorities in OAR and ensuring a *Strong Europe* well into this new era of operations. 

Endnotes

1. US EUCOM Communications and Engagement Directorate Media Operations Division, *Operation Atlantic Resolve Fact Sheet*, 2014. Retrieved 25 January 2014 at http://www.defense.gov/home/features/2014/0514_atlanticresolve/FactSheet_OperationAtlanticResolve_3Jul14.pdf.
2. U.S. Army Europe Homepage, *What is Operation Atlantic Resolve?*, 2014. Retrieved 25 January 2015 at <http://www.eur.army.mil/landforceassurance/>.

Other Reading

Uri Friedman, Russia's Slow-Motion Invasion of Ukraine, *The Atlantic*, 29 August 2014. Retrieved 25 January 2015. At <http://www.theatlantic.com/international/archive/2014/08/russias-stealthy-slow-motion-invasion-of-ukraine/379312/>.

MAJ Buchanan is the Battalion S3 for 2^d MI Battalion, Wiesbaden, Germany. He has served in a variety of positions including multiple deployments as a Battalion S2, MICO Commander, and MiTT Intelligence Advisor. He holds an MA from San Diego State University and an MSSJ from the National Intelligence University.

CPT Lewandowski is the Battalion Operations Officer for 2^d MI Battalion, Wiesbaden, Germany. He has served in various HUMINT roles during multiple Iraq and Afghanistan deployments, most recently while serving as an SFAT advisor to the 205th ANA, BDE.



Becoming the Regionally Aligned Intelligence Force

by the 4th Infantry Division G2 Section

Introduction

In September 2014, the 4th Infantry Division (4ID) became Service-Retained, Combatant Commander Aligned (SRCA) or the Regionally Aligned Force (RAF) to U.S. European Command (EUCOM). Within 90 days of redeploying from Afghanistan, the Division transitioned to this new mission, which included reorientation toward a new theater of operations and deploying under a newly developed paradigm.

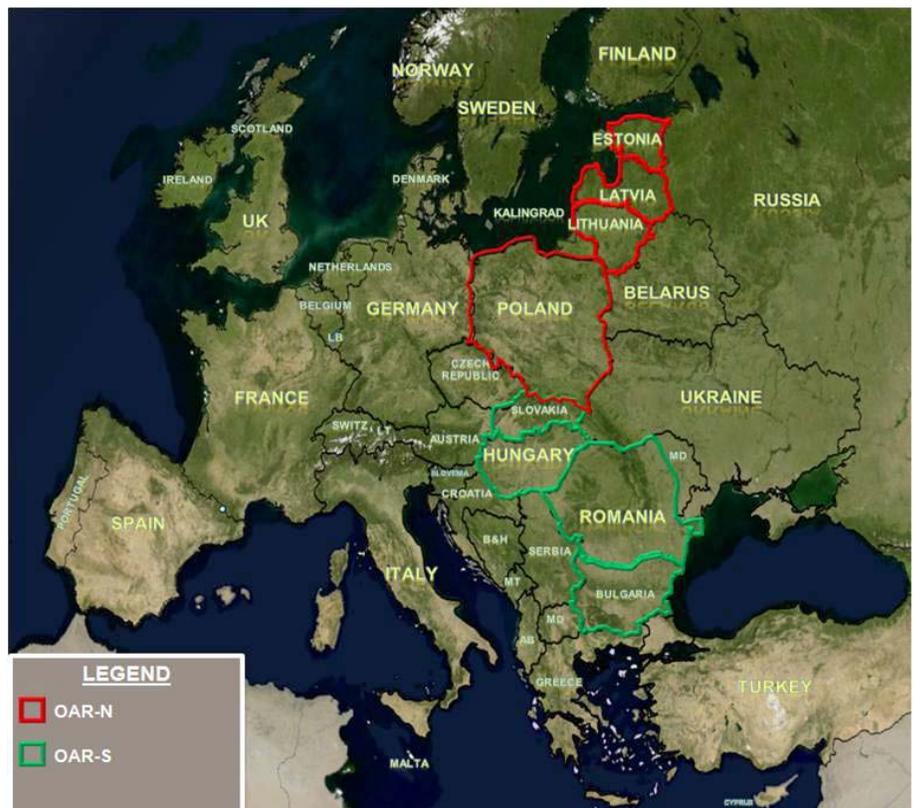
This article is written from an Intelligence Warfighting Function (IWfF) perspective and details the initial steps and processes 4ID executed during the transition to the European RAF mission. It also provides recommendations to Division and Brigade G2/S2s when planning for and initially executing this mission. The intent is to provide the initial lessons learned for units transitioning to the RAF construct and outlines a process for developing the task organization for the RAF IWfF. This article also provides recommendations to Army intelligence leaders to consider when enabling RAF units to execute overseas missions.

A US Army Europe Unit Stationed in CONUS

The most important aspect of becoming a RAF unit is quickly gaining situational understanding. Only through situational understanding are commanders and leaders able to make informed decisions that avoid second and third order consequences and reduce risk during operations. The Army has focused on US Central Command (CENTCOM) operations over the past 14 years. This has created an Army that is generally unfamiliar with the threats, geography, history, and cultures within other geographic combatant commands. Within this section are the steps 4ID executed with

US Army Europe (USAREUR) to quickly enable the Division's IWfF to move from a relationship of dependence to one of contribution toward the European RAF mission, more specifically OPERATION ATLANTIC RESOLVE (OAR). Early engagement, connectivity, and training/exchange programs were the pillars of this process.

The 4ID and USAREUR G2s began coordinating with one another months in advance of the official RAF assignment date. This occurred during several early engagements to include two USAREUR G2 staff site visits to Fort Carson. The first visit was four months prior to assuming the EUCOM RAF mission and the second was shortly after mission assumption. The agendas for these visits were relatively similar, but this was necessary given the long lead times needed to become a USAREUR unit eight hours behind Central European



time. In addition to developing a personal relationship between the staffs, agenda items during these visits were: intelligence updates; communication networks and diagrams; intelligence federation; OAR planning; product formats; battle rhythm, and training and exercises. The key USAREUR intelligence personnel participating in these visits were the G2 OPS/Plans OIC, G2 Network OPS OIC, G2 Training and Exercises OIC, and the S3 Plans/Knowledge Management Officer from the Operations Battalion of the 66th MI Brigade. This small group enabled the 4ID IWfF to move quickly toward an initial RAF operating capability and situational understanding.

Theater intelligence updates are the domain of USAREUR's theater intelligence brigade (TIB), 66th MI BDE. Immediately establishing a dialogue with 66th MI enabled the 4ID IWfF to draw on intelligence subject matter expertise, detailed production, theater product format standards, and quickly become a member of the European intelligence community of interest. As the Army's European theater intelligence "anchor point," the 66th MI BDE has fulfilled the U.S. Army Intelligence and Security Command's concept of a RAF unit's IWfF being able to quickly integrate into a theater of operations. 66th MI provided the base analysis for 4ID intelligence products, live environment training (LET) opportunities, and access to the Distributed Common Ground System-Army (DCGS-A) communication architecture. These actions detail only a fraction of 66th's capabilities, but they are the key facets that enabled the 4ID G2 section to leap forward toward gaining situational understanding.

Connectivity with European intelligence networks is the foundational layer of being a RAF unit. There are two critical intelligence networks that a European RAF unit requires: DCGS-A and Battlefield Information Collection and Exploitation Systems (BICES). DCGS-A, of course, is the Army's Intelligence ABCS system and BICES is a US-NATO classified intelligence sharing network. After some initial challenges, the 4ID DCGS-A servers are now replicating data from the 66th MI Brain. This enabled 4ID to track adversary order of battle and share structured and unstructured intelligence data.

4ID's BICES capability continues to grow on Fort Carson with over 60 users and will become even more important as the Division's forward deployed Mission Command Element

develops closer ties with NATO Allies involved in OAR. Overall, RAF units must have intelligence network connectivity to develop situational understanding. The USAREUR G2 in conjunction with 66th MI has established the base for 4ID's RAF mission, which has prepared us to become a federated European intelligence production partner.



Conducting LET and posting liaison officers (LNO) are two efforts that have also facilitated situational understanding. Within six months of being assigned the EUCOM RAF mission, 4ID had numerous Soldiers deployed on LET opportunities. Paid for with Foundry dollars, the LET locations initially centered on 66th MI in order to establish a link with the TIB. This program will soon expand to other EUCOM and NATO intelligence locations based on OAR operational requirements.

Soldiers of all ranks executed and benefited from these LET deployments, however, the greatest return on the LET investment came from E5s and above. More senior 4ID Soldiers developed lasting relationships with 66th MI senior analysts and leadership of the 66th MI. This has created an open dialogue that still continues even after returning to home station. This dialogue has expedited intelligence coordination and enabled 4ID to further extend its intelligence reach. LET opportunities are critical to gaining situational understanding of regional nuances.

The second mechanism for nesting with USAREUR was the deployment of a LNO. 4ID maintains two LNOs at the USAREUR Headquarters, one operations officer (Lieutenant Colonel) and one intelligence officer (Major). The intelligence LNO's primary function is to synchronize intelligence operations, planning, and travel of 4ID personnel with

USAREUR policies and procedures. This position and LET opportunities come at a cost to the USAREUR G2, the 4ID G2, and various budgets, but they have paid significant dividends for both headquarters and RAF operations.

Another training/exchange program for developing situational understanding is staff education. When 4ID first began its education process, one of the senior staff members remarked during an initial RAF briefing that he “did not know there was a Russian territory on the Baltic Sea between Lithuania and Poland.” This comment illustrates the Army’s focus on CENTCOM over the past 14 years and the requirement for staff education. The 4ID G5 planned and coordinated a staff leadership professional development program focused on OAR countries and Russia. This program consisted of military and academic guest speakers and usually occurred in the form of briefings (classified and unclassified). While large audience briefings reached the most personnel, small discussions and deep dives on the same topic always garnered greater understanding especially within the IWfF.

IWfF Design

Given the OPTEMPO and myriad of intelligence requirements, flexibility and modularity are critical tenets for task organizing a Division’s IWfF for RAF while still executing other Division-level operations. The 4ID IWfF supports OAR, RAF exercises and theater security and cooperation events, Fort Carson prepare to deploy order (PTDO) missions, subordinate brigades’ intelligence training, and senior mission command functions on a daily basis. There is no joint manning document to guide divisions, so determining what intelligence capabilities to have in time and space is a dynamic problem continuously assessed and coordinated. 4ID determined that reach operations were the best course of action to accomplish all intelligence missions.

Establishing an intelligence hub at home station enabled the G2 leadership to dynamically move resources to support all operations. 4ID intelligence elements forward supporting OAR send requirements to home station where a dedicated team of analysts conduct analysis and production. This type of task organization requires Soldier management at the “name tape-level” in order to maximize capabilities and provide a modicum of predictability for Soldiers. Developing a standard training progression for Soldiers supports this type of task organization and will increase subject

matter expertise. 4ID now deploys a Soldier on an OAR focused LET mission followed by a 6 month OAR deployment and then concludes with a period of time on the OAR Reach team. When Soldiers are not involved with OAR, they are supporting other intelligence requirements (PTDO, training and other senior mission commander tasks). This design maximizes support to the 4ID Commander’s intelligence requirements and establishes an architecture for federation.

Federation

Formally federating intelligence within EUCOM is another step toward integrating the RAF unit. Shrinking intelligence staffs and budgets demand that the IWfF becomes more efficient with the use of its resources. One clear course of action is to formally federate intelligence production across EUCOM and its subordinate units. One unit that has started this process even though it not a part of EUCOM is the National Ground Intelligence Center (NGIC). NGIC’s Program of Analysis is a synchronized effort with geographic and functional commands to formally forecast intelligence production by quarter.



This strategic federation effort enables Defense Intelligence Agency (DIA), Joint Intelligence Operations Center Europe (JIOCEUR), USAREUR, and 66th MI BDE to focus their resources on other requirements, thereby becoming more efficient. Developing a formal, broad federation plan within EUCOM down to the division-level will create efficiencies that enable the IWfF to better cover strategic, operational, and tactical level threats. Not formalizing this plan by OPORD or memorandum of agreement between commands makes any agreement personality-based and likely to dissolve when an intelligence leader departs the position.



are not cheap and therefore must be managed. RAF units must be careful not to spend themselves out of a mission and to utilize methods that conserve fiscal resources.

The final challenge is talent management. The Army invests large amounts of money in making MI analysts subject matter experts. PCSing these analysts every three years increases the risk of wasting this investment if not properly managed. Officers and NCOs who spend three years studying European threats should not then be moved to an intelligence unit only to start the journey to expertise again. Assuming follow on duty assignments keep individuals competitive for pro-

Remaining Challenges

While the term RAF is solidified in the Army's lexicon, there are still many challenges for RAF units executing it. As discussed in the Design section, there are a multitude of intelligence requirements that the RAF Division IWfF must still execute. Being a RAF unit does not "fence" the IWfF from non-RAF requirements. This is a daily leadership challenge which requires prioritization and coordination of effort. While writing this article, Fort Carson units are deployed in support of all geographic COCOMs. Each of these units requires a distinct measure of intelligence support from the 4ID Division G2 section either prior to or during deployment. This dynamic is manageable, but it does reinforce the requirement to maintain flexibility and modularity.

Another challenge is the RAF budget. One of the benefits of the RAF concept is the lower costs for the Army. CONUS RAF units cost less than forward based units, thereby the Army's overall operating budget is reduced. The TDY costs that come from being eight time zones away from Europe

motion, Human Resources Command should assign Soldiers with regional expertise to units with like focuses within DIA, the COCOM JIOC, NGIC, or other commands. This will continue the return on the Army's original investment, reduce time spent training, and increase the depth of the Intelligence Community.

Conclusion

4ID's transition to a EUCOM RAF unit is still occurring. Unanticipated challenges are discovered often as the mission and requirements change. This continuous dynamic will drive the closer integration of 4ID with EUCOM, USAREUR, and 66th MI. Overall, the 4ID IWfF is grateful for the support that has enabled it to execute OAR, RAF, and our nation's mission in Europe. The USAREUR G2 and 66th MI have made the transition to RAF a seemingly smooth process because of its early engagement and continuous, active dialogue. 4ID will continue to report lessons learned with the intent of enabling follow on units to avoid unnecessary delays in the execution of their RAF mission. 

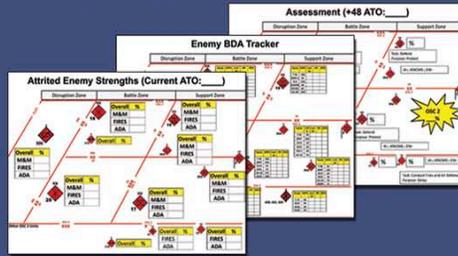
The Army Publishing Directorate has authenticated and released ATP 2-19.4, Brigade Combat Team Intelligence Techniques dated 10 February 2015.

ATP 2-19.4 provides techniques for intelligence support to brigade combat team (BCT) operations. The techniques in this manual apply to the range of military operations and all echelons of the infantry, armored, and Stryker BCTs. The principal audience for ATP 2-19.4 is commanders, staffs, and Soldiers responsible for planning, preparing, executing, and assessing tasks of BCT intelligence cells.

This publication supersedes FM 2-19.4 (25 November 2008), ATP 2-19.5 (14 June 2013), TC 2-19.63 (9 November 2010), and TC 2-50.5 (6 January 2010).

This publication is available at https://armypubs.us.army.mil/doctrine/ATP_1.html

Decisive Action and the Corps G2



by Colonel Jim Sisemore

In February 2015, III Armored Corps completed one of the Army's first corps level Decisive Action (DA) Warfighter Exercises (WFX) since the Army began operations in Afghanistan and Iraq. Following 12 years of counterinsurgency warfare, few staffs are accustomed to the fast paced, firepower intensive environment of a DA fight. Within III Corps, the G2 Section focused on core processes as it prepared to support the exercise. This article highlights ten lessons learned (and in some cases relearned) by the III Corps G2 during its preparations and execution of WFX 15-03. It is hoped that these lessons will assist other division and corps G2 staffs prepare for and excel during their exercises.

WARSIM and DCGS-A

The threat picture supporting DA WFXs, is developed within WARSIM (Warfighters' Simulation), an advanced virtual environment used to simulate most of the Army's Warfighting Functions. Junior Intelligence leaders, accustomed to the precision intelligence developed to strike high value individuals, quickly become frustrated with the less than precise threat picture developed by WARSIM. Within the DA environment, operations occur at a much faster pace, with larger formations across the depth of the area of operations. The hybrid threat in WARSIM is, in many instances, more complex, but presented in much less detail than many analysts expect. Unlike operations in Afghanistan and Iraq, where target development was supported by interagency and multi-national partners, in the fast paced DA environment analysts are required track large enemy formations across a wide front. For some analysts, this was the first time they were required to look at a DA threat since their initial entry training at Fort Huachuca. This hybrid threat requires analysts to pay attention not only to the security area, but to also template and confirm major enemy elements. This change in analytic focus is less intuitive for today's war-tested Soldiers and must be retrained.

To support the analysis of the threat picture, WARSIM simulates the Army's intelligence weapon system, the

Distributed Common Ground System-Army (DCGS-A). Operators of this central intelligence system have to be more than just system operators, they must be trained analysts. During a DA exercise, WARSIM can produce in excess of 500 threat reports per hour. This large number of reports requires a constant monitoring of the system. Soldiers must understand how to correlate reports and eliminate redundant or irrelevant data points. They must also identify holes in the enemy picture and make informed decisions to complete the overall situation template. Analysts must review all reports, ensuring they do not overlook a key indicator or "golden nugget" that identifies a significant enemy formation or asset.

One of the critically important indicators in air planning is enemy air defense artillery (ADA) formations. These formations must be identified for SEAD (Suppression of Enemy Air Defense) missions in support of joint fires and general air-route planning. Analysts must understand the enemy order of battle (OB) and how enemy ADA systems are employed. If the locations of these formations are not known, Soldiers must be trained to template those systems for SEAD fires. Analysis of DCGS-A reporting is critical to the success of the intelligence warfighting function and operators must be trained beyond basic 'buttonology' to fully employ the system.

Two weeks prior to the WFX, III Corps secured an Interim Authority to Operate (IATO) for its Analysis and Control Element, BLOCK II (ACE BK II), an All-Source Fusion and single source subsystem. Scheduled to become DCGS-A enabled in the future, ACE BK II enabled III Corps to receive single source reporting, providing Electronic Intelligence and Communications Intelligence reports needed to refine the threat ADA picture. Operated by Signals Intelligence Soldiers, ACE BK II, like DCGS-A is a weapon system and must be trained as such. Due to the late approval of the IATO, our Soldiers had limited time to train on and understand recent software improvements to the system. However, as the ex-

ercise progressed, this system became an important link in supporting our aviation elements in flight planning.

Lesson 1: Ensure Intelligence Soldiers are trained on their Weapon Systems—DCGS-A and ACE BLOCK II.

Lesson 2: Never forget that Soldiers, not machines, do analysis. Allocate time to train analysts on fighting in a DA operating environment.

Shift Change and a G2 Common Picture

During the WFX, we discovered a disconnect between what the G2 Operations Section, located on the COIC (Command Operations and Information Center) floor, was tracking and what our ACE Soldiers were tracking as they processed intelligence reports. This disconnect impacted the G2 as a whole as we worked to portray a common, relevant threat picture. An easy fix to this divide was to have our G2 Battle Major from the COIC floor attend the ACE shift change and brief current and future coalition operations. This was a win-win for the G2 as we quickly developed a shared enemy picture. This combined brief gave our ACE Soldiers an improved view of planned coalition missions and allowed them to better understand where their actions impacted mission success. The Battle Majors briefed at both the morning and evening shift change and we quickly reduced the friction and gained a shared understanding across the G2.

Lesson 3: Take every opportunity to share information between the operations floor and the intelligence Soldiers in the ACE. A joint brief can benefit both current operations and ACE Soldier understanding.

DCGS-A and CPOF: Who's in Charge?

Both systems are critical. CPOF (Command Post of the Future) is used to collaborate and share maneuver plans and graphics across echelons. CPOF is the primary visualization tool used within corps and division headquarters and is used to establish the COP (common operational picture) across all formations. DCGS-A is the Army's primary tool to gather intelligence across echelons, from space to mud, in a common system. Within the intelligence community, DCGS-A is clearly our foremost operating system and remains crucial to the success of the overall community in presenting a predictive, relevant enemy picture. While analysis and tracking is conducted on DCGS-A, maneuver commanders at the division and corps level are familiar with and expect a combined "blue and red" picture on CPOF. To assist in meeting this expectation, DCGS-A has the capability to execute an "automatic update" of enemy icons to CPOF. Once the parameters are set, this action eliminates the need for an analyst to manually send updates to CPOF, ensuring a timely threat picture is portrayed on CPOF. Although this function is a great improvement to previous manual updates, it came with an added training requirement for our analysts.

After setting parameters for the update within DCGS-A, we discovered that some enemy icons from days-old reports reappeared on the COP. These old or "ghost" icons caused confusion early in the exercise. The entity manager (an ad hoc position filled by an All Source Technician) must work to ensure that updates sent to CPOF are current and clear of ghost reporting. During high intensity periods, these updates can become a distracter and cause hours of extra work if not maintained by a competent DCGS-A operator (and) analyst.

A training aspect that paid dividends for the III Corps G2 was to ensure select intelligence Soldiers were trained on CPOF as well as DCGS-A. While there are many advances in DCGS-A and its functionality, maneuver commanders expect presentations on CPOF no matter what the Warfighting function. During the WFX, intelligence, sustainment, and fires all presented data using CPOF. The terms "paste board" and "effort list" must be understood and trained to ensure the G2 remains relevant to the commander during these presentations. While DCGS-A allows the sharing of data to other intelligence elements across various echelons, CPOF was used during all staff presentations to the commander and subordinate headquarters. It is imperative that intelligence Soldiers understand how to manipulate CPOF and ensure data can be presented to the commander in that forum.

Lesson 4: A DCGS-A entity manager is a critical enabler to ensure the joint COP is updated for the Commander and staff.

Lesson 5: Ensure intelligence Soldiers understand how to use and manipulate CPOF to support product development and presentations.

Order of Battle and BDA

Returning to a DA environment requires a "back-to-the-future" view of conducting intelligence operations. Prior to 2001, OB Technicians, usually crusty warrant officers who were central figures in the development of both doctrinal and situation templates, were invaluable within the G2. Our current corps MTOEs show several All Source Technicians, but not a true "OB Tech." After years of counterinsurgency warfare, the ability to look at a threat picture, determine if it makes sense, and identify gaps in collection was lost. In its place was the development of association matrixes and pattern of life analysis to support individual targets. After the WFX began, it became all too clear that our knowledge base as a G2 was not where it needed to be for a DA fight. Only our older analysts were capable of looking at a doctrinal template, overlay it on the terrain to develop a situation template, and determine where to focus collection assets.

Similarly, Battle Damage Assessment (BDA) analysis and tracking needed to be reenergized across the formation for

reporting and support to targeting. For a corps in a DA environment, joint fires planning and execution took primacy, with the G2 Section recommending targets and target reengagement within the Air Tasking Order (ATO) cycle. Target refinement and ATO modifications are topics for another article, but within these key tasks, the G2 Section played an essential role in supporting the staff to meet the Corps Commander's objectives.

Within the targeting cycle BDA reporting from subordinate units and coalition air force units needed to be collated and assessed for validity. This data in turn was briefed daily to the commander and used to feed an overall G5 assessment. The G2 Section also supported the targeting process with projected BDA for the 48 and 72 hour ATO windows. This predictive analysis was something most junior analysts were uncomfortable with and few had the maneuver experience to determine where the enemy would be located in 48 and 72 hours, much less assess their projected strengths. While this task can be trained, it took senior officers and NCOs to guide this process. This analysis ultimately drove decisions in the targeting meeting and board for the corps commander. Picking the right warrant officer or NCO to head this effort is critical for the success of the targeting effort.

Lesson 6: Train BDA and Order of Battle analysis. Both are critical to the targeting process—a key task at the corps and division level in DA.

Collection Management and the FSCL

Fortunately, the Army greatly increased its ability to conduct collection and the prioritization of collection assets during the past 12 years of war. Warrant officer collection managers have a solid understanding of collection assets and capabilities. As previously discussed, however, understanding the threat environment and what targets needed collection priority became an important task to support the corps targeting process. Tied to the confirmation of the situational template, collection must focus on confirming enemy locations, determining his intent, and be prioritized for targeting by using the High Payoff Target List (HPTL). The Corps used both kinetic and non-kinetic targeting means as determined by the targeting working group. Understanding assets and capabilities was central in this process.

Clearly the G2 targeting team must understand the enemy's OB and possible courses of action. Tied to this understanding is an appreciation of how the friendly commander intended to defeat the enemy commander's plan. Priority intelligence requirements (PIR) and the friendly scheme of maneuver must be understood by all, with PIR updated as necessary. Within III Corps, proposed PIR changes were discussed at the targeting working group and were then

presented to the commander at the targeting board for approval. This ensured PIR were tied to maneuver planning and decision points, and offered a forum for staff input into the process.

In defining a collection area focus, III Corps used the Fire Support Coordination Line (FSCL) as its intelligence hand over line between division and Corps assets. The Corps remained focused forward of the FSCL, with the divisions focusing assets between the FSCL and its intelligence hand over line with subordinate brigades. This separation proved less challenging for the Corps than the divisions, as the Corps continued to focus collection and fires deep to shape the battlefield for the division's next fight. However, between the divisions and subordinate brigades, the intelligence hand over line was challenging due to the fast pace of the operations and frequent boundary changes. While the Corps' fight remained forward of the FSCL, extra effort must remain on defining the collection requirements in support of the division and brigade fights. A way to review this focus is in consolidating and combining subordinate collection requirements as possible. Within III Corps, this was done during a twice daily collection working group. It was only through this formalized effort that the corps balanced subordinate requirements with the Corps Commander's priorities.

Lesson 7: Ensure the collection management team is tied into fusion to develop collection priorities to identify key enemy assets. Update PIR as part of the targeting process.

Lesson 8: Ensure subordinate collection requirements are synchronized within the corps collection process to track asset requirements and balance the overall effort.

Sensor-to-Shooter Link

Within III Corps, the GEOINT (Geospatial and Imagery Intelligence) team is collocated within the ACE in garrison and during field operations. During the WFX, we used our GEOINT Soldiers to operate our imagery workstations as well as monitor JSTARS (Joint Surveillance Target Acquisition Radar System) and the UAS (Unmanned Aircraft System) work stations. Within the Corps ACE, our GEOINT team is further located next to our targeting team, resulting in a proactive sensor to shooter link tied into our joint fires effort.

Within WARSIM, UAS systems are replicated by the MUSE (Multiple UAV Simulation Environment) system. For WFX 15-03, the Corps operated four simulated Gray Eagle (GE) lines that were task organized from a subordinate division's GE Company. The MUSE simulation allows imagery Soldiers to monitor and interact with GE "pilots" to confirm and target enemy formations. Using a stateside version of mIRC

(Internet Relay Chat), imagery Soldiers were able to locate and send targeting data on HPTs to our joint fires cell for attack. This proved extremely successful, testing our ability to dynamically re-task assets and force our operators to follow HPTL guidance. A significant success was the identification and destruction of a threat SA-20 radar system and launchers by fires. The success of finding and destroying targets proved our sensor-to-shooter link was effective and allowed our Soldiers to gain confidence in their capabilities.

Another success was the use of MTI (moving target indicators) for cross-cueing and targeting. Within WARSIM, the MUSE also supports MTI generation, simulating a JSTARS feed. During the WFX, III Corps consistently used MTI to cue UAS for target identification. From this cross-cueing, our imagery Soldiers were able to confirm the target and then send that information to our joint fires cell for targeting. While impacted by adverse weather during portions of the exercise, this cueing effort proved to be one of our most reliable “eyes on” targeting sources.

While the GE has the capacity to carry ordnance and engage individual targets, it was decided early in the planning process that its reconnaissance value far outweighed the utility of a GE engaging single tanks with ordnance. The decision to reduce the weapons payload allowed for longer loiter times over targets and subsequently more enemy equipment destroyed using joint fires.

Lesson 9: In the DA Environment, JSTARS is a valuable cross-cueing platform for targeting.

Lesson 10: While UAS systems can engage individual targets, their value as a reconnaissance and targeting platform provided greater value in the DA environment.

Conclusion

WFX 15-03 proved both challenging and a great learning event for the Soldiers of the III Corps G2. Many of the skills lost or forgotten in the past 12 years of war were quickly retrained and put to use. Unlike the current event-driven Mission Readiness Exercises that corps and division headquarters often conduct prior to a combat deployment, the DA scenario drives the staff to execute combined arms maneuver to defeat an enemy. During III Corps’ WFX preparation, it was clear that old lessons needed retrained, while younger Soldiers and junior leaders had to be introduced to doctrine and core functions previously never trained. Most of the lessons discussed in this article are quick wins for any organization preparing for a DA exercise. During the 8-day event, the G2 section was able to identify shortfalls and quickly build solutions that paid dividends throughout the remainder of the exercise.

As the Army faces increased budget cuts and reduced combat deployments, DA WFXs will return as the “norm” in training division and corps headquarters. The execution of combined arms maneuver in a DA environment enables formations to regain skill sets lost over time. It is hoped that the lessons highlighted above will enable other formations to better prepare for and conduct their WFXs. 

COL Jim Sisemore is the G2 for III Corps and Fort Hood. He previously served as a battalion commander at Fort Campbell and as a brigade S2 at Fort Drum.

ATP 2-91.8, Techniques for Document and Media Exploitation (5 May 2015) has been published. ATP 2-91.8 updates and expands existing doctrine on document and media exploitation (DOMEX) based on technology and emerging lessons learned in current Army operations. It discusses intelligence support to DOMEX at all echelons. This manual informs commanders and staffs about the mission, requirements, and capabilities of DOMEX assets. It provides commanders and staffs with tools to integrate and synchronize DOMEX activities and techniques.

The principal audience for ATP 2-91.8 is Soldiers and civilians engaged in or supporting intelligence activities contributing to DOMEX in a tactical, operational, or strategic environment.

This manual supersedes TC 2-91.8 (8 June 2010). Soldiers may access this document at https://armypubs.us.army.mil/doctrine/ATP_1.html.

Establishing the Intelligence Architecture and Tactical Communications Plan in a Multinational DATE Exercise



by Captain Benjiman A. Smith

Introduction

During the last 12 months, the Joint Multinational Readiness Center (JMRC) at Hohenfels, Germany conducted four Decisive Action Training Environment (DATE) exercises. Each of these exercises trained a multinational brigade comprised of battalions and companies from over 13 different nations, many of them NATO allies.¹ One recurring problem exposed during each of these multinational exercises is the challenge of sending timely and accurate intelligence reports from multinational intelligence collection platforms and units to current operations analysts at the Brigade Tactical Operations Center (TOC), and then sharing that correlated information with multinational partner nations.

JP 2-01 identifies such challenges in the Intelligence Process, stating “the increased tempo of military operations requires an unimpeded flow of automatically processed and exploited data that is both timely and relevant to the commander’s needs.”² This challenge exists for U.S. units operating in the multinational DATE scenario at JMRC because such units cannot rely solely on U.S. mission command systems to provide “automatically processed and exploited data” to multinational partners.

In order to succeed in the multinational DATE scenario, U.S. and multinational intelligence sections must pass timely and accurate intelligence information from the individual collector to the BDE TOC during mission planning and execution in order to maintain situational awareness and enable the commander’s decision making process. The BDE TOC must then process these individual pieces of information and create an enemy situational template (SITTEMP) and common operating picture (COP), within foreign disclosure regulations, easily shared with all subordinate units and facilitating situational understanding.

This will require most U.S. units to reconsider unit standard operating procedures (SOPs) developed during home station training before deploying to the JMRC. Successful intelligence sections in the multinational DATE scenario blend analog, FM radio, and digital mission command systems during mission planning and execution in order to es-

tablish an effective intelligence communications plan that provides redundant forms of communication and supports their commander’s decision making process.



U.S. Army photo by SSG Carol A. Lehman

The BN S2 from the Czech 41st Mechanized Battalion discusses current operations with a U.S. Army OCT during training exercise Saber Junction 2014 at JMRC in Hohenfels, Germany. The Czech BN staff successfully maintained both a digital and analog COP in order to better share information with a subordinate Bulgarian Mechanized Infantry Company and adjacent U.S. BNs from the 173rd Airborne BCT.

Current Trends and Doctrinal Guides

A recent article published in the Military Intelligence Professional Bulletin highlights how a U.S. brigade combat team (BCT) used digital command systems at the National Training Center to enable mission command.³ The authors tout the success of 2/4 ABCT using the Distributed Common Ground Station–Army (DCGS-A) to publish an enemy SITTEMP to other digital mission command systems, specifically the Command Post of the Future (CPOF) and the Force XXI Battle Command Brigade and Below (FBCB2). In doing this, 2/4 ABCT became a “digital” unit, not just digitally equipped, allowing the BDE to publish near-real time situational awareness updates and analytical assessments to every U.S. vehicle and command post simultaneously.

MI professionals across the Army should applaud this effort, as it demonstrates the tremendous power of integrating complex U.S. digital mission command systems to maintain situational awareness in the DATE scenario. While these techniques are effective for U.S.-only training exer-

cises, they are generally unsuccessful in multinational DATE exercises at JMRC because multinational partner nations rely heavily on analog (FM radio and map) systems to pass intelligence information and generally do not have digital mission command systems compatible with U.S. digital systems.

When partner nations do have digital systems that advertise digital interoperability with U.S. systems, they are rarely tested before the training exercise and are quickly abandoned for more practical forms of communication. When U.S. BDEs and BNs have multinational partner nations attached or assigned in support, intelligence planners must alter their SOPs to consider the challenges in communicating with these formations. Existing MI doctrine highlights the need for considering multinational partners when establishing the intelligence architecture.

MI Pub 2-01.2, *Establishing the Intelligence Architecture*, discusses ways that BN and BDE staffs should organize intelligence communications systems in a deployed environment. In addition, this publication instructs intelligence planners to establish a Primary, Alternate, Contingency, and Emergency (PACE) intelligence communications plan that links three important groups. One intelligence PACE plan links intelligence collectors with intelligence analysts at BDE and BN, facilitating processing and exploitation of intelligence information. The second intelligence PACE plan links intelligence analysts at BDE and BN with subordinate units, facilitating dissemination and integration of intelligence information to help commanders make decisions.⁴ Intelligence personnel must also work closely with their Signal Corps counterparts to develop these communications plans and match them against their unit's overall communications capabilities.

MI Pub 2-01.2 further instructs the intelligence staff to "update the communications plan to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces."⁵ Redundant forms of communication assist in maintaining consistent situational awareness in the DATE scenario when units move frequently and the operational environment constantly changes. U.S. units conducting multinational DATE tend to rely heavily on digital, and U.S.-only forms of communication (DCGS-A, CPOF, text chat programs, VoIP telephones, etc.) as their primary and alternate forms of communication. Many U.S. units do not establish and re-transmit an FM operations and intelligence (O&I) radio frequency as a backstop to digital forms of communication. Exclusive digital communications by U.S. units stresses multinational partner nations' intelligence sections, potentially denying them routine access to sources of information and resulting in multinational units' inability

to maintain situational awareness on events outside of their formation. Successful U.S. units stress using shared forms of communication common among multinational partners and look to optimize their strengths during training exercises.

JMRC Observations in the Multinational DATE Scenario

JMRC and U.S. units training in the EUCOM theater of operations have the advantage of relying on NATO to provide technical and doctrinal standardization agreements (STANAGs) that help establish interoperability among member nations. These NATO standards are leveraged by JMRC to make training exercises more realistic and to overcome complex interoperability challenges, such as making mission command systems from different nations communicate over a secure tactical network. Units training outside of the EUCOM theater of operations could use many of the best practices discussed in this article, but may not have certain advantages, such as standardized data formats to make national mission command systems compatible. Any unit training in a multinational environment should look to identifying the similarities and differences of their partners during the exercise design process, and develop solutions to overcome interoperability challenges before conducting training.

Most multinational armies, and particularly NATO allies, have FM communications systems that are compatible with U.S. SINCGARS and use NATO doctrine similar to U.S. doctrine. When FM communications platforms are not compatible, U.S. and NATO partners utilize a tactical voice bridge to link different radio communications platforms using different waveforms and COMSEC.⁶ Multinational partner nations' strengths generally include good analog battle tracking procedures using paper maps and acetate, FM radio reporting procedures, and standardized reporting procedures from subordinate units and intelligence sensors. In many cases, multinational partners have experience operating in Iraq and Afghanistan and remain prepared to leverage web based intelligence databases like the Combined Information Data Network Exchange (CIDNE) if a database is available.

Multinational partner nations also frequently adhere to doctrinal graphics and symbols in accordance with FM 1-02, *Operational Terms and Graphics*, and its NATO equivalent AAP-6, *NATO Glossary of Terms and Conditions*.⁷ Doctrinal terms and graphics taught to U.S. leaders at Army schools (Officer Basic Course, branch specific captain's career course, battle staff, etc.) represent a "common language of doctrine" among all U.S. and multinational personnel. Many multinational formations struggle to establish digital

systems that are linked with U.S. digital platforms at adjacent and higher unit headquarters, but excel at maintaining a COP using maps and acetate overlays. The JMRC plays an important role in helping U.S. and multinational units overcome these digital interoperability challenges by integrating existing NATO interoperability solutions and standards into the exercise design process.

U.S. Army photo by PFC Shardsia Washington



U. S. and Lithuanian soldiers track current operations using a map and acetate overlay during training exercise Saber Junction 2014. Analog battle tracking was critical for this BN TF, which included Infantry Companies from Estonia, Latvia, Lithuania and the United States.

During multinational DATE exercises, JMRC establishes an unclassified coalition network (CONET) to provide a digital communications platform that all exercise participants can use. This platform replicates real-world systems, such as the Battlefield Information Collection and Exploitation Systems (BICES), but without the functionality of the NATO Intelligence Toolbox and Joint Operations Intelligence Information System.⁸ In addition, JMRC provides web based applications on this platform (CIDNE, Adobe Connect, etc.) which replicates some of the functionality and database solutions that the U.S. and NATO allies have used successfully to share information in Afghanistan and Iraq. These systems allow all participants to have access to unclassified exercise data and operational environment resources without signing an information sharing agreement for each exercise. JMRC also facilitates multinational units fielding their nations' mission command systems that are accredited with the Multilateral Interoperability Program (MIP).⁹

This emerging program allows multinational units to use their own digital mission command systems, linking them to U.S. mission command systems and allowing all formations to share a digital COP that includes the enemy SITTEMP. The Danish 1st Armored Infantry Battalion Royal Life Guards tested this system during JMRC training exercise Combined Resolve III. During the exercise, the Danish Army connected their MIP compliant Danish Army Command and Control

Information System to a computer server linked to CPOF, but the Danes' tactical satellite system lost connectivity due to the BN TOC's frequent movement and was unable to routinely share and receive a digital COP with adjacent U.S. and multinational units.

In spite of their technological advantage, the Danes ultimately relied on FM radio and analog map battle tracking techniques to maintain situational awareness and effectively link intelligence collection platforms with analysts at BDE and BN. While combat training centers continue to help test and develop the digital expertise required to make these systems functional, U.S. training units must still take simple and practical steps to solve intelligence interoperability issues in the multinational DATE scenario.

Best Practices for U.S. Units Operating in the Multinational DATE Scenario

Successful U.S. units operating in the multinational DATE scenario effectively blend analog, radio, and digital mission command systems during mission planning and execution, highlighting the strengths and mitigating the weaknesses of their multinational partners. Future JMRC exercise participants should continue to maintain proficiency with U.S. digital systems and equipment, including analog systems as a primary means of communication to achieve shared situational awareness. Best practices are listed below; many of these steps are already practiced by our multi-national partners and can be quickly leveraged by U.S. units to integrate multinational partners into operations.

- ◆ **Establishing an O&I FM radio network re-transmitted throughout the unit's area of operations and serving as the unit's primary means of intelligence communication.** Use a tactical voice bridge to link communications platforms employing different waveforms and COMSEC. FM radio communications techniques appears to be a lost art for many intelligence staff personnel, who are more comfortable using text chat programs as a primary means of communication at fixed sites, based on their experiences in Iraq and Afghanistan. The O&I net



U.S. Army photo by CPT David Schenk

The BN S2 NCOIC from the Danish 1st Armored Infantry Battalion Royal Life Guards gives an operational update to his commander during training exercise Combined Resolve III at JMRC. The Danish BN staff used analog battle tracking and written orders as their primary means of communication during the exercise, as the BN TOC was frequently on the move and not able to maintain digital communications with their BDE headquarters.

maximizes the abundance of FM radio communications systems and procedures in multinational units, which allows the training unit to distribute intelligence information throughout the formation without interfering with the unit's primary command FM network.

- ◆ **Using the FM O&I net to conduct periodic situation updates, distributing intelligence information across the force and facilitating current operations battle tracking.** U.S. units should establish a format for periodic FM O&I updates that includes current assessed enemy locations (at the company or platoon level), status and priority of reconnaissance assets, a review of notable intelligence reports, and changes to the assessed enemy course of action. These O&I net updates should be conducted at least every four hours in order to help subordinate units maintain situational awareness.
- ◆ **Creating named areas of interest overlays and the unit's collection plan for reconnaissance assets in hard copy using acetate overlays to be distributed at the OPORD brief or the unit's combined arms rehearsal.** Successful units can then issue updates to the reconnaissance plan during the planned periodic intelligence updates over the FM O&I net or identify a recurring procedure for hard copy graphic distribution. Successful units issue hard copy graphics, not just a PowerPoint slide but an actual acetate overlay, to ensure that subordinate elements have full access to the reconnaissance plan and can operate effectively without a digital connection.
- ◆ **Publishing a text based intelligence summary that minimizes file size to less than 1 megabyte of data in order to conserve limited digital bandwidth facilitates dissemination and integration of intelligence information among intelligence personnel at all levels.** Most U.S. units create a daily graphic intelligence summary in PowerPoint that contains embedded JPEG images and pictures, causing the file size to be too large to be shared effectively with multinational units operating with limited digital connectivity. Successful U.S. units rely on a text-only intelligence summary that is easily shared and downloaded by units with limited access to digital information using an HP-2C/185 CPN or a SIPR/NIPR Access Point (SNAP) terminal. This practice also forces intelligence personnel to provide succinct analysis and situational updates to their subordinate units without relying heavily on convoluted slides.
- ◆ **Training and certifying responsible leaders as foreign disclosure officers (FDOs) and foreign disclosure representatives (FDRs) before deploying to the component**

command area of responsibility to ensure that U.S. classified and unclassified information can be shared legally during training exercises. FDOs and FDRs should work to receive a Delegation of Disclosure Authority Letter that gives the training unit the authority to review and share information with their multinational partners.¹⁰ This is a process that can take several weeks to complete and must be accounted for in a unit's training plan in order to be successful.

Conclusion

Training in the multinational DATE scenario at JMRC requires that U.S. units update their approach to intelligence sharing and mission command. Too often, U.S. units focus their internal training plan towards digital (and often U.S.-only) communications platforms, like CPOF and DCGS-A, in preparation for a BDE or BN level training exercise or combat training center rotation. While these communications platforms often function well in the U.S.-only training environment, they prove ineffective as the primary communications platforms in a multinational training environment.

Successful intelligence sections in the multinational DATE scenario follow Army doctrine established in MI Pub 2-01.2 and carefully consider the capabilities and limitations of their multinational counterparts during mission planning in order to achieve the most efficient intelligence communications architecture, and enable situational awareness and the commander's decision making process. MI leaders at the tactical level should not ignore the tremendous power of digital systems, especially DCGS-A, which provide an unparalleled level of situational awareness and detail when employed effectively. However, MI leaders at the tactical level should also create a training plan that incorporates both digital and analog battle tracking techniques in order to produce well rounded intelligence sections ready to succeed in any environment.

In the multinational DATE scenario, U.S. units are most successful when they blend analog battle tracking, FM radio procedures, and digital mission command systems that provide redundant forms of communication and ensure that all units are capable of maintaining situational awareness. Successful units also update and rehearse their unit intelligence/situational awareness sharing SOPs in order to succeed in the multinational DATE. Finally, successful units train and certify a cadre of officers and NCOs in proper foreign disclosure procedures and become familiar with the foreign disclosure process in their component command area of operations. Following these lessons learned will prepare units for future conflicts where the U.S. fights together with partner nations to achieve a common goal. 

Endnotes

1. JMRC DATE exercises have included Army units from Austria, Bulgaria, the Czech Republic, Denmark, Estonia, Germany, Latvia, Lithuania, the Netherlands, Norway, Romania, Slovenia and the U.S.
2. JP 2-01, Joint and National Intelligence Support to Military Operations, III-1.
3. CW2 Bryce Bouwens and MAJ Ryan Burke, "Warhorse Brigade's Successful Employment of DCGS-A Enabling the Commander's Decisionmaking Process," *Military Intelligence Professional Bulletin*, April June 2014, 21.
4. MI Publication 2-01.2, 4 February 2014, Establishing the Intelligence Architecture, 1-3 to 1-4.
5. *Ibid.*, 1-14. This information sharing requires trained foreign disclosure representatives from the U.S. training unit to validate the sharing requirements.
6. The 1st Cavalry Division's Ironhorse Brigade successfully used a tactical voice bridge during the Combined Resolve III exercise to bridge U.S. and DEU communications platforms.
7. This statement is predicated on observations drawn during JMRC training exercises 14-08 (Saber Junction 14) and 15-01 (Combined Resolve 3) with Infantry Battalions from the Czech Republic, Slovenia, and Denmark.

8. JMRC exercises often include non-NATO nations, making it difficult to use the classified BICES network as a primary solution to enable automated data processing.

9. See NATO STANAG 5525 for further information on the Joint Consultation, Command and Control Information Exchange Data Model. This program allows bi-lateral sharing of COP information with nations' whose mission command systems are MIP compliant.

10. For further information, see AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, which implements Army policy established in DoD Directive No. 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, and DoD Directive No. 5230.20, Visits and Assignments of Foreign Nationals.

CPT Smith is a Maneuver Battalion Intelligence Observer, Coach, Trainer at the JMRC in Hohenfels, Germany. His previous assignments include HUMINT/SIGINT Platoon Leader, Infantry Battalion S2, and Company Commander. He has also served as the JMRC Intelligence and Operational Environment Planner. His military education includes the MI Officer Basic Course and the MI Captain's Career Course. He is an incoming student at the National Intelligence University and holds a BA in History from the University of Dayton.

Speaking With Intelligence

Speaking With Intelligence (SWI) is a **monthly, informal online talkshow presented by the Army Reserve Intelligence Support Center enterprise**. We bring exciting speakers from around the Intelligence Community to the warmth and comfort of your living room. We broadcast **live on the last Thursday of each month at 2000 central time**.

We've had a lot of **exciting topics**:

"I'll take INTELINK for 20, Alex!"

"Marines talking SMAT: Techniques for Improving Analytic Tradecraft"

"Cheat, lie, and steal your way across the internet!... How ransomware profits organized crime."

"Google Glass: Game Changer or Just Goofy?"

"Social Media in Mexico: Not tú mama's revolution."

To hear about future shows, nominate speakers, send us fan mail, or ask us a question please email from your .mil/.gov account:

usarmy.usarc.mirc.list.speaking-with-intelligence-swi@mail.mil



Why COIST Matters

by Victor R. Morris

This article was originally posted in Small Wars Journal, March 2015.

The views expressed in this article are those of the author and do not reflect the official policy or position of FORSCOM, JIEDDO, DA, DoD, the U.S. Government, any Government Agency, or Booz Allen Hamilton.

Introduction

“Do you even COIST, bro?” was the question a young command post NCO asked one of his Soldiers. The question arose during situational exercise lane training involving platoon level patrols in the company sector. The young soldier asked his leader how he knew about the enemy’s employment of improvised explosive devices (IEDs) and the “hot spot” locations, which are essential to countering asymmetric threats, maintaining situational awareness and contributing to bottom-up refinement.

There have been numerous debates regarding the applicability of Company Intelligence Support Teams or COISTs and the “way ahead” in future conflicts. Opinions such as “COIST is for COIN,” “COIST is not doctrine,” and “Intel is for analysts” have been widespread. In contrast, there have been positive reviews from specialist through brigadier general about the efficacy of COISTs in training and combat.

One of the current challenges involving COISTs stems from an overall military shift. This shift involves the reduction of counterinsurgency (COIN) operations world-wide, increase of Decisive Action Training Environment (DATE) rotations and global employment utilizing Regionally Aligned Forces (RAF). The DATE rotations support conducting Unified Land Operations in a Hybrid Threat Environment. There is a perception that COISTs are only relevant in an irregular warfare model during COIN and stability operations. Other challenges to COIST future applicability involve doctrine development and ineffective task organization.

The current company COIST model is not conducive to effectively engaging diverse combinations of regular and irregular forces simultaneously. Future security challenges will include multi-faceted, uncertain, complex and chaotic environments, and will require more support to information and intelligence requirements at all echelons. The initial, sustainment and pre-deployment training must be a command priority and must be formalized for future management during Army Force Generation cycles. Finally, teams must become better integrated into company command

posts during training and be better supported through more emphasis on overall mission command. COISTs must not only be maintained for future conflicts, but adapted to be better integrated and transitional within company mission command systems during Unified Land Operations involving a hybrid threat.

Background

The complexity of irregular warfare necessitated the need to have more enhanced intelligence capability at the small unit level. In conventional operations, intelligence is disseminated from higher to lower headquarters based on the presence of intelligence gathering resources. In COIN or other decentralized operations, information flows in the opposite direction, where small units gather raw information based on their operational environment (OE). Recent COIN operations assessed that company formations needed the ability to produce intelligence to drive their operations and support higher echelon common operational picture development.

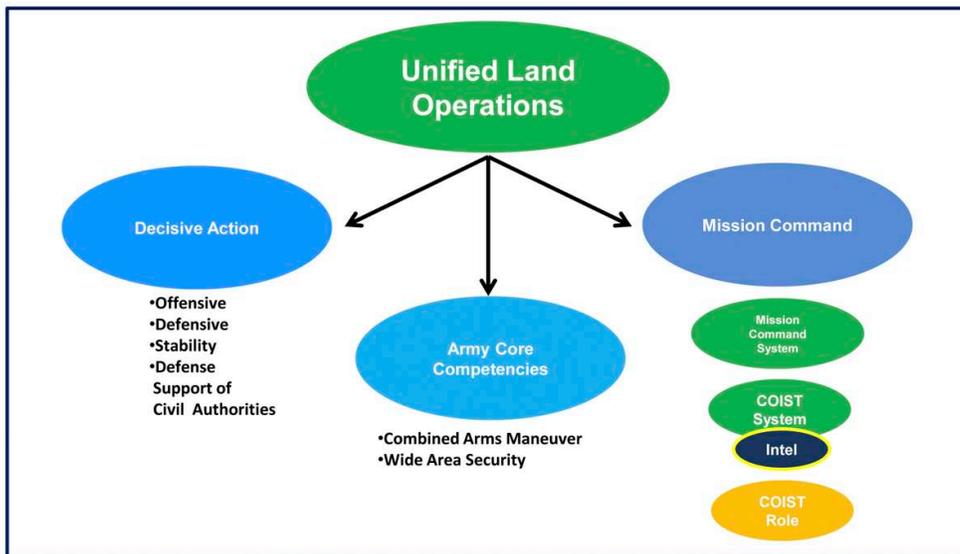
This assessment was refined and given the designation “COIST” with the following mission: *serve as the primary source of information and intelligence that the company commander needs to make timely accurate decisions* (CALL COIST Handbook No. 13-09, May 2013). Post-deployment after action reviews (AARs) and training assessments dictated the employment of COISTs and greatly enhanced the company’s ability to analyze, produce and disseminate accurate information and intelligence in a COIN environment. They also facilitated better situational awareness and more effective lethal and non-lethal targeting in support of the commander’s intent and overall mission.

The Shift: Unified Land Operations

In response to the current and future changes, the combat training centers and TRADOC collaborated on the development of a training model called DATE. The current model is designated as DATE 2.1 and differs from past training rotations and pre-deployment Mission Readiness Exercises utilized to prepare units for Iraq and Afghanistan. The model was designed to prepare tactical organizations to execute a wide range of operations as part of Unified Land Operations. The DATE model presents a complex training environment that is designed to train operationally adaptable units. The

ground operations provide the ability for the unit to build competency with mission essential tasks, while refining standard operating procedures (SOPs) from the last fourteen years of combat.

Next, the model drew on aspects of the contemporary OE, while incorporating aspects of emerging threats and security challenges. The threat to the brigade’s mission involves an emerging category of threats and activities that do not fit into the traditional understanding of conventional and unconventional war. Lastly, the DATE includes Joint, Interagency, Intergovernmental, and Multinational partners and a multifaceted host nation security force that presents the brigade with integration challenges and opportunities. This paradigm shift to encompass Decisive Action, Army Core Competencies, and Mission Command has created debate about the applicability of COISTs during Unified Land Operations.



COIST in Unified Land Operations.

The Doctrine Dilemma

There have been improvements during the last eight years involving the development and implementation of COIST doctrine, but the concept is still not formalized in many company formations. It is imperative that doctrinal references be used as the basis for COIST training, AARs and SOP development. A current doctrine review and its support to COIST operations is below:

◆ **25 November 2008:** FM 2-19.4, 1-24, Brigade Combat Team (BCT) Intelligence Operations. This section briefly mentions the need to form

COISTs based on capability requirements and access to perishable information. It also highlights the fact that these teams are ad hoc and optional.

- ◆ **23 March 2010:** FM 2-0 Intelligence fails to address COIST operations in detail.
- ◆ **9 November 2010:** TC 2-19.63 Company Intelligence Support Team. Aside from various CALL handbooks published May 2013, this is a very detailed doctrinal publication involving COISTs. Although it was published in 2010, it acts as the doctrinal foundation for our COIST, Attack the Network, COIN, and staff training courses.
- ◆ **15 April 2014:** The revision to FM 2-0 Intelligence highlights COISTs in BCT intelligence operations (Chapter 2). Paragraphs 2-7 through 2-10 provide an overview of COIST and their contribution to intelligence sharing, enemy assessment, troop leading procedures, and mission execution. The manual also states that the MI Company may augment selected maneuver companies with MI Soldiers to form the nucleus of the COIST.
- ◆ **10 February 2015:** ATP 2-19.4, 1-24, Brigade Combat Team (BCT) Intelligence Operations. This document has been updated from the previous 2008 version and clearly frames the COIST’s role and responsibilities.

Evaluating the Threat

Hybrid threats are not new and there are myriad examples throughout history of how adversaries organize into conventional and irregular forces. A hybrid threat (HT) is defined as the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefiting effects (TC 7-100). The term “hybrid” has recently been used to illustrate the increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict. Contemporary hybrid warfare involves a multiplicity of actors employing a combination of hybrid instruments and unconventional operations facilitated by 21st century technologies and combinations of conventional and irregular forces.

Hybrid threats are characterized by the combination of forces, which can further be defined as conventional military, insurgent and extremist networks or transnational organized criminal organizations. To be a hybrid, these forces cooperate in the context of pursuing their own internal objectives, which further complicate the unit’s mission and need for increased situational awareness and understanding.

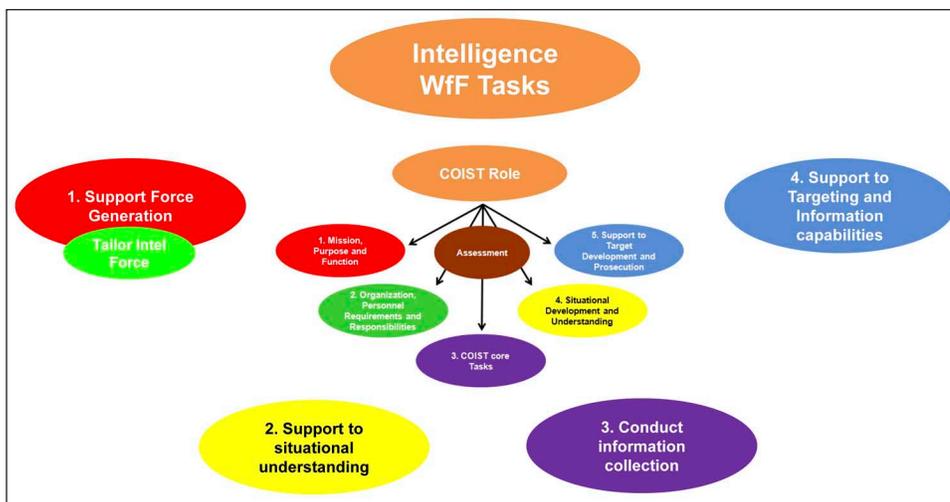
A recent example of this threat can be seen in Buenos Aires, Argentina. On August 10, 2014, Troops of Apolo Task Force, Third Army Division, discovered a complex illegal structure which operated in La Esperanza village, Buenos Aires municipality, Cauca. On site, troops fought against a group of guerrillas and when they retreated, troops searched the area and located a 200 m2 structure which had been adapted to manufacture explosives and process coca paste. This facility was reported to be the property of the Revolutionary Armed Forces of Colombia (FARC). This event is evidence of the close relation between drug trafficking and FARC, and the way this criminal structure intends to strengthen its capabilities by using explosive devices.

Some of the goals associated with hybrid threats:

1. Removal of forces from their area of operations.
2. Degrade and exhaust forces rather than cause a direct military defeat.
3. Use of a dynamic variety of conventional and unconventional methods to create multiple dilemmas.
4. Prevent opponents from segregating the conflict into easily assailable parts. In many cases military action is the least important of the hybrid threat's activities.
5. Rapidly form, transform, adapt and abolish cells based on requirements, environment and opponents.
6. Simultaneously inject themselves into all of the operational variables in the OE (PMESII-PT).
7. Adhere to ensuring security, accomplishing the task, maintaining adaptability, and remaining connected to the people.
8. Preserve bases to train, self-sustain, prepare for future missions and evolve organizational capability.
9. Initiate strategic consequences of denying an enemy a secure area, or making it politically untenable to remain.
10. Create a dilemma where an army is vulnerable to conventional attack when it disperses to combat irregular forces within the population, and cede control of the OE and population if they remain concentrated.

Training to Counter the Threat

COISTs must possess core competencies associated with engaging actors in a hybrid environment. The below tasks are associated with offensive, defensive and stability operations in a static or mobile command post during operations. The core competencies can also be aligned with a COIST framework consisting of the following spheres: Mission, Purpose and Function, Task Organization, Core Tasks, Situational Development and Understanding, Support to Targeting and Assessment. The framework is nested in the Mission Command and Intelligence Warfighting Functions for complementary effects.



COIST IWFF Integration.

This list is not all inclusive and is subject to change based on the mission and commander's discretion.

Traditional or conventional Threat: Military forces as a threat to the regulated armed forces of a state or alliance of states with the specified function of military offensive and defensive capabilities. These forces may have matching capabilities across all war-fighting functions.

◆ **COIST core competencies:** Intelligence Preparation of the Battlefield (IPB) involving detailed terrain analysis,

an awareness of various intelligence disciplines to include TECHINT, OSINT, SIGINT, GEOINT and HUMINT, template and company graphic management (analog and BFT), PIR, SIR, CCIR management, ISR program management, proper enabler utilization (task/purpose), planning on the move contribution and direct support to the orders process, which is condensed during high-tempo operations.

Irregular Threat: Irregular forces as armed individuals or groups who are not members of the regular armed forces, police, or other internal security forces (JP 3-24 Counterinsurgency). These forces include: paramilitary, special purpose forces,

insurgent, guerilla, terrorist and criminal elements. At the tactical level, they can apply tactics, techniques, and procedures common to regular forces but do so with asymmetric applications. The definition of irregular warfare highlights population centric engagement and intention to damage an opponent's influence over that population.

◆ **COIST core competencies:** IPB with an emphasis on understanding trends, patterns, human networks (to include criminal), culture and perceptions of the community within the environments, an awareness of various intelligence disciplines to include Weapons Technical Intelligence, OSINT with a social media emphasis, SIGINT, GEOINT and HUMINT. All of the above competencies support situational awareness and support to targeting.

Lessons Learned

James K. Greer's article from the Small Wars Journal, "*The Network vs. the BCT: Organizational Overmatch in Hybrid Strategies*," analyzes the concept of more modular approaches at the tactical level specifically involving "cellular companies." In summary, he suggests that we must become a cellular network in order to respond to future threats. This is accomplished through a deviation from the current relatively fixed company identity to a "cellular company" that operates off a rule sets enabled by a robust information and intelligence cell. This cell is an augmentation of the information mission command system. He also states that the company should be able to gain or lose modules many times in a day without losing the coherence of operations, as tasks and engagements are conducted simultaneously and sequentially.

As an Infantry Company Commander during OIF 09-10, we conducted operations in a similar model. For example, we had one platoon conducting route security patrols (C-IED), one platoon conducting host nation security force EOD training, one platoon conducting indirect fire disruption patrols in a targeted area of interest, and one platoon designated as a company or battalion quick reaction force. Based on the situation and operations tempo, these patrols could be happening sequentially or simultaneously. Additionally, each module has its own set of enablers, which had to be planned and managed properly.

The "dynamic retasking" occurred when host nation security forces required tactical support from U.S. forces. Typically, commanders were given six to eight hours to dynamically re-task the company to support host nation battalion level operations. This re-tasking meant consolidating and re-organizing the platoons or "cells" back at the operating base and finalizing the troop leading procedures. The majority of the time the mission was to conduct a company

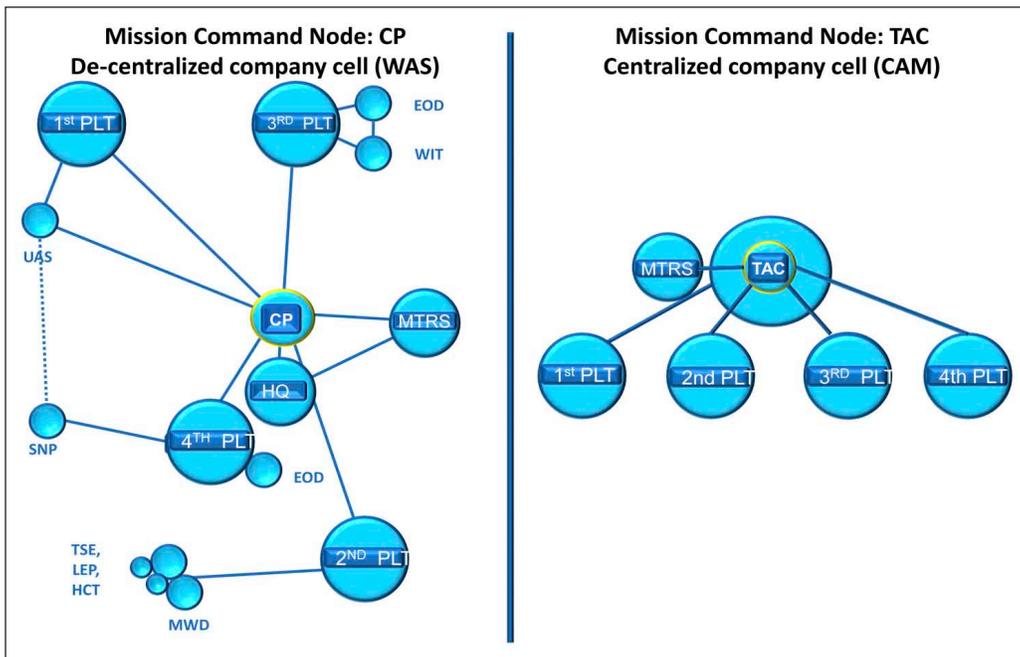
level clearance of an urban area. In other offensive terms, we conducted company movements to contact whilst partnered with host nation forces. The threat was asymmetrical at the time, but this can easily be applied to a more conventional or hybrid threat. The OPORD was completed and briefed within three to four hours of the company WARNO. The company essentially went from conducting decentralized stability operations to centralized offensive operations in six hours with direct support from the headquarters section. COIST employment begins with the company command team and the commander's mission command philosophy and system management.

Mission Command Systems: COIST 2020 Initiatives

The solution to effective and adaptable companies lies within mission command. ADP 6-0 defines Mission Command as the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations. Additionally, mission command system consists of five components: personnel, networks, information systems, processes and procedures, facilities and equipment. All of these components are contained in the company command post module. That module is contained in the headquarters section with the commander as the backbone of mission command.

Due to the nature of the future OE, the current state of company command posts and COIST cells are not effective due to a lack of effective integration. They should not only be combined, but augmented through experience and capability—not personnel. The efficacy of this technique comes from a synchronization of the five components of mission command in one module with intelligence as a centralized function. The module or node is the command post, the cells are the headquarters section/platoons, and the network is the company. One of the primary arguments with COIST training and employment involves creating cells "out of hide" and taking soldier from line platoons.

All the mission-command capabilities are already present in the headquarters section of a maneuver company/troop/battery, which includes the 35 series MOS intelligence soldier, Armored, Infantry, and Stryker formations. Mission command capabilities can also be modified or augmented in non-maneuver companies as seen in Chapter 9 of the CALL COIST Handbook No. 13-09. This is not to say that a soldier from the line cannot be transferred to or from the section, but the capabilities are already there and are adaptable. If you are conducting combined arms maneuver through



Company network, cells and modules/nodes.

high-tempo operations, the commander is fighting mounted through a multi-vehicle TAC or in a dismounted configuration. There is no “COIST vehicle” and those skill sets are executed via the personnel and systems present on the various TAC vehicles. If you transition to wide area security, the entire module along with the systems transitions to a tent or hard stand building.

Company intelligence must be synchronized with current operations and reporting, based on all of the preparation and assessments conducted prior to the mission. The emphasis comes from a previous planning knowl-

edge involving friendly maneuver, enemy courses of action, information requirements and enabler integration. Accurate reporting is decisive in high-tempo operations and must be concise for proper common operational picture development. Doesn't it make sense for the soldiers collecting and analyzing the information before the mission, to report it during and after the mission?

All modular configurations of the command post must be able to receive, distribute and analyze information. They must also be able to recommend courses of action and integrate resources. All of this is accomplished through one mission command module that includes the company intelligence aspect. Intelligence is innate at the company level based on recent combat operations. There is no longer a need to differentiate command posts from COISTs because their missions are synonymous. We need to train with increased capability in mind, in lieu of increased personnel or equipment. Strong companies with strong leaders have the ability to “do more with less.”

Conclusion

Companies have evolved from recent combat operations and must continue to evolve and adapt based on the future threats involving security. Time-honored concepts of conventional and unconventional war involving traditional methods have no meaning to a hybrid threat beyond their ability to be used against its opponents. The skill sets required to combat this threat must be standardized and maintained at the company level. Operations at the tactical level directly correlate to the success or failure of a campaign, where success is gained through enhancing the situational awareness in tactical units at the company/troop/battery level. All of the principles contained in this article are applicable to maneuver and non-maneuver companies alike. Whether you are utilizing COIST, Company-Level Intelligence Cell, Company Intelligence Cell, or Intelligence Support Team, you must be cellular and adaptive in order to support higher echelon requirements and the mission in a highly dynamic OE. ✨

Other References

ATP 3-90.37 Combined Arms Counter-Improvised Explosive Device Operations.

ATP 3-21.11, SBCT Rifle Company 3rd QTR FY 15 (pending).

John Lichfield, “Super-cities threaten to Swallow Humanity,” *The Independent*, August 2014.

Victor R. Morris is a former U.S. Army Captain and Stryker Company Commander. He is currently a civilian contractor and instructor at the U.S. Army Europe's Joint Multinational Readiness Center in Germany.



by Colonel Todd A. Megill (USA, Ret.) and Colonel Stephen P. Perkins (USA, Ret.)

For four decades, FORSCOM has delivered formations for employment by theater commanders or combatant commanders in lean and healthy resource climates, and we will lead this effort into the next decade.

-GEN Daniel B. Allyn, former FORSCOM Commander¹

The opinions expressed herein are those of the authors, and are not representative of those of the Department of Defense, the U.S. Army, or FORSCOM.

Introduction

The development and delivery of tactical intelligence capabilities will continue to be an important part of the U.S. Army Forces Command (FORSCOM) mission. The FORSCOM Intelligence Warfighting Function (IWfF) focuses on ten initiatives to deliver trained and ready Military Intelligence (MI) Soldiers and units per the Army Force Generation (ARFORGEN) model in support of Mission Command.²

- Foundry 2.0 Concept and Implementation
- Intelligence Readiness and Operations Capability Concept
- Intelligence Readiness Reporting
- Intelligence for Senior Leaders Training
- DCGS-A Training and Integration with Mission Command
- Combat Training Centers Modernization
- G2X and FORMICA Implementation
- GEOINT Readiness
- Language and Cultural Awareness Training
- FORSCOM LandISR Implementation

Figure 1. FORSCOM 10 IWfF Initiatives.

Simply put, “Understanding readiness is not a very sexy thing. It’s getting soldiers to the right place at the right time and getting them trained to a high level. It’s not finding the bad guy. It’s not providing the data that punches out a hard target.”³

Former FORSCOM Commander GEN David Rodriguez identified the challenge for the next decade when he stated, “As we build America’s Army to participate as a member of the joint force of 2020, we must strengthen our expeditionary force capabilities within a fiscally challenged environment. I

believe that the key to doing this is agile and adaptive leaders employing Mission Command effectively.”⁴ For the IWfF, there is nothing more important than creating the conditions for our MI Soldiers and units to train and to develop our MI leaders to support Mission Command.

This article discusses how the FORSCOM IWfF is addressing Mission Command requirements, including how the FORSCOM IWfF is *supporting the warfighter*, using the *Installation as an IWfF Platform*, and *training MI Leaders and Commanders*—and provides some recommendations on the way ahead.⁵

Supporting the Warfighter

“Ultimately, the goal is to ensure that every MI Soldier is fully trained, equipped, and engaged in the fight against a complex, agile, and adaptive enemy, whether deployed or at home (via intelligence reach). Thoughtful investments will ensure the Army intelligence warfighting function remains capable of supporting decisive action across the globe.”⁶

FORSCOM has worked unceasingly to sustain translator/interpreter companies in the active Army force structure as well as retaining a theater-level interrogation capability, which includes an interrogation facility to train Counterintelligence (CI) and Human Intelligence (HUMINT) Soldiers and Maneuver Commanders at Fort Bliss, Texas. FORSCOM has also worked with the Army G2, the U.S. Army Training and Doctrine Command (TRADOC), and the Intelligence Center of Excellence (ICoE) to transition the three Battlefield Surveillance Brigades to the Expeditionary Military Intelligence Brigade (E-MIB) concept. Each E-MIB will provide a headquarters and two MI battalions to support Corps operations and to downward reinforce divisions and brigade combat teams (BCTs).

Responding to the need to address new doctrinal changes in the geospatial intelligence community, FORSCOM issued FORSCOM Regulation 115-9, which addressed map requirements and the development of GEOINT Cells at Corps and divisions. They broke ground on the new Geospatial-Intelligence Readiness Center (GRC), which will become op-

erational in FY 2015 and supports both the Global Response Force (GRF) and FORSCOM units as a whole.⁷

In 2013, FORSCOM established a FORSCOM G2X, which is different from the doctrinal G2X, but allows FORSCOM to focus on CI and HUMINT readiness areas related to the ARFORGEN mission, focusing on manning, training, and equipping organizations in the ARFORGEN Cycle. It also works to enhance the Foreign Military Intelligence Collection Activities and CI Live Environment Training opportunities within FORSCOM and improves its partnership with the U.S. Army Intelligence and Security Command (INSCOM) functional expertise in these areas.⁸

The FORSCOM LandISR program is extending and sustaining Sensitive Compartmented Information (SCI) connectivity to FORSCOM Corps, divisions, and BCTs. Future FORSCOM LandISR program requirements maximize the Army Joint Worldwide Intelligence Communications System (JWICS) Enterprise capabilities by enhancing the quality of the network infrastructure and support. LandISR will support the Intelligence Readiness and Operations Capability (IROC) initiative and Soldiers' need for access to live Intelligence and Intelligence Community (IC) databases.

Finally, FORSCOM has become a valued member of the Army G2's Intelligence Senior Integration Group and the Intelligence Senior Steering Group (ISIG).⁹ FORSCOM has also taken the Army lead in translating Reach operations from the special operations forces (SOF) and INSCOM organizations into the general purpose forces (GPF). Understanding how SOF and INSCOM used Reach operations to support their missions in Iraq and Afghanistan will ensure Mission Commanders can see future potential deployment areas accurately and expand Intelligence support opportunities. FORSCOM's outreach to its subordinate G2s and senior intelligence officers (SIO), the Army Command SIOs (TRADOC and Army Materiel Command) and the Army Service Component Command G2s resulted in more efficiently linking our shared messages on security and networking issues.

Installation as an IWfF Platform

In her 2012 *Army Greenbook* article "Army Intelligence 2020," the Army G2 highlighted the importance of readiness and our ability to meet future challenges. "Among the greatest challenges we face is the pace of change, both in technology and in the conditions we find in each theater. As a result, even as we integrate the new capabilities into our intelligence force, we must constantly upgrade the equipment, the tools and the advanced skills training we provide to ensure our intelligence formations arrive in theater with

the right skills and equipment to remain on the forward edge."¹⁰

FORSCOM's top-to-bottom MI review (T2B-MIR), *FORSCOM G2 MI Readiness Review Results of Analysis*, validated the belief that FORSCOM installations needed to improve their capabilities and capacities to conduct IWfF training and to operationalize their training using IROCs.¹¹ The review evaluated four components, which were deemed critical to supporting training and operational reach operations: facilities, cadre, systems, and networks. It drew from the existing LandISR program architecture, which provided information on JWICS connectivity, SCIF facilities, and JWICS automation necessary for the Foundry and IROC initiatives.¹²

LTG Legere's mantra that to be ready for combat and contingency operations, Intelligence Soldiers and units must have the "the right equipment and the right skills." "No MI Soldier at rest and no cold starts" is the linchpin for FORSCOM Intelligence training.¹³



Photo by SGT Austan Owen

JBLM Intelligence Academy. Leaders of the newly organized Intelligence Academy, CPT David Miller, ACE chief and SFC Brian Gardner, ACE NCOIC, both with the 7th ID, demonstrate a few teaching methods they use while giving a class. The Intelligence Academy was developed in an effort to standardize intelligence training and introduce incoming soldiers to the Pacific Command AOR.

In that vein, FORSCOM is firmly committed to the Army's *Foundry 2.0* program, which adjusts the way the Army invests in MI Soldier and unit training.¹⁴ While the Foundry Program will remain the Army's premier intelligence training program and the cornerstone of the IWfF support to the ARFORGEN process in the future, many of the instructors will be Soldiers, not the civilians and contractors who have dominated the Foundry workforce over the past 10 years.

The Foundry 2.0 Program has significantly improved the MI Soldier's individual and collective training at home station. The Army cannot allow this capability to be lost. By applying the FY 2012 T2B-MIR's assessment, the Army can improve its capability at the Foundry Home Station training sites, formalize IROC requirements, and synchronize pro-

cesses and procedures with Army and combatant command policies. As an enduring Army IWfF requirement, Foundry 2.0 enables a long-term training capability where commanders are able to train units in critical IWfF skills at home station, using facilities and training methodologies analogous to tank and infantry gunnery.

Foundry/IROC allows Mission Commanders and leaders to be exposed to Intelligence operations and the need to synchronize Intelligence collection with the dynamic operational environment. Further, Foundry expands the Foundry Program from an *individual training* for readiness focus to mission support to readiness focus supporting Geographic Combatant Commands and Army Service Component Commands, especially theater security cooperation engagements.

This focus intuitively points to the importance of the IWfF in the Army's readiness enterprise. To better understand its place in the installation's process, we developed an Intelligence Readiness Relationships graphic to highlight the multitude of players in the Installation Senior Commander's IWfF Training Management System and the complex nature of training MI Soldiers and units at home station.



Figure 2. Building Intelligence Readiness Relationships.

Many examples explain how installation MI professionals work with others for MI Soldier and unit readiness, but all benefit from having a Senior Commander who sets priorities, issues timely guidance, and monitors the progress of their IWfF working within the context of Mission Command. LTG Legere, in her 2013 Army article, *“Army Intelligence in Support of a Regionally Aligned Army,”* shared five “best-practice” examples illustrating the IROC concept and how it

contributes to readiness.¹⁵ The best example of home station Intelligence training and operations-intelligence fusion in FORSCOM is how the Stryker BCTs at Joint Base Lewis-McChord used Reach operations on a recurring basis, and leveraged their Intelligence Operations Facility in an IROC-like role.¹⁶ When Senior Commanders see these results they gain a better appreciation of how they can leverage training at home station and take note of how they must integrate the IWfF into their Mission Command efforts either in a regionally aligned forces (RAF) environment or an overseas contingency operation.

Training MI Leaders and Mission Commanders

In his *Army* article, *“Building Readiness and Providing Responsive Landpower,”* GEN Allyn described the importance of training in the preparation for overseas contingency operations, noting, “Our success in deploying combat-ready units is a function of rigorous, realistic and innovative training conducted at home station/annual training sites and during post-mobilization training.”¹⁷ The FY 2014 FORSCOM Command Training Guidance (FCTG) Supplement 1 identifies five priorities, including #2—*Build and Empower Leaders*. “Our leaders, Soldiers, and units are exceptionally well trained with vast operational experience; however, our ability to efficiently plan in a resource-constrained environment, conduct effective training, or mentor our Soldiers and leaders demands our immediate command emphasis.”¹⁸ GEN Allyn emphasizes the need to create “learning leaders,” who use a deliberate program incorporating “continuous and progressive development.”¹⁹ At a recent FORSCOM Commanders Forum, MG Charles Flynn unveiled the FORSCOM “Leader Development” website, which “harnesses numerous tools and products from the broader Leader Development network across the Army, sister services, the interagency, and even civilian entities.”²⁰

The Army must integrate leader development into everything it does. “In training, successfully executing tasks under different, challenging conditions builds leader and unit confidence to operationally adapt to the environment. The Army must develop leaders who seamlessly integrate leader development into training management consistent with ADP 7-0 Unit Training and Leader Development.”²¹ The FORSCOM IWfF must leverage the full suite of resources within the Training Support System, including the Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT) and the TRADOC Training Brain Operations Center (TBOC).^{22,23} FORSCOM leaders must look for ways to maximize the available time and other resources. Current RAF missions and rotations to the combat training centers (CTCs) offer our Commanders and staffs the opportunity



Figure 3. Leader Development Toolbox.

to work Reach operations by working the IWfF into their Mission Command functions and priorities.

In his FY 2014 FCTG Supplement, GEN Allyn notes in his fourth priority, *Operationalize Army Total Force Policy and Shape the Force*, that we must reestablish partnerships between active and reserve formations.²⁴ As an example, active component units are leveraging the PANTHER STRIKE exercise, an MI training event hosted by the Utah National Guard at Camp Williams, Utah, to work multinational (Canada, the United Kingdom, Australia, and New Zealand) and interagency intelligence multidisciplinary issues.²⁵

FORSCOM MI leaders must master their understanding of TRADOC's *Operational Environment*, their own MI "weapons systems"—especially the DCGS-A platform—and the Army's training management system. Much as in the past, MI leaders and Soldiers must be the most knowledgeable people in the room when senior leaders need information on the adversary. Gaining this level of knowledge requires constant study throughout an MI leader and Soldier's career, including exposure to leading subject matter experts (civilian and military), exposure to operational areas that are less known, and discussions with Soldiers and units who have been deployed to various regions. Leveraging the relationship built through RAF, Intelligence professionals should conduct physical and virtual exchanges with forwardly deployed analysts and operators.

MI leaders must master the DCGS-A platform and ensure its capabilities are known by operators and integrated into the common operating picture that the Commander uses. The Army cannot bring analytical prowess to bear on tactical problems until MI Soldiers have mastered their "weapons." FORSCOM continues to work with DA G2, PM DCGS-A, and FORSCOM tactical units on "ease-of-use" initiatives, developing and documenting procedures for efficiently and effectively addressing analytical problem sets.

Intelligence professionals must not only be able to undertake Intelligence operations, but they must also be able to explain and integrate them within Commander's running estimate and Mission Command.

Charting the Way Ahead

Over the past forty years, FORSCOM has seen many changes, tried to adjust to the lessons of the past, and arguably have made some mistakes. Having said all of that, this

article takes a swing at five things the FORSCOM IWfF needs to enhance its performance.

- ◆ **First**, the Army needs to invest in the FORSCOM G2. It should assign a general officer (active or reserve) as the FORSCOM functional lead. From 1973 to 1994, the FORSCOM G2/J2 was a brigadier general. While FORSCOM's sister organization, TRADOC does not have a general officer as its SIO, it is led by a senior executive service (SES) member and has several SES-level civilians to lead its organization and interface with the Army Staff and the IC. To effectively influence tactical intelligence efforts in our Army, FORSCOM G2 must be a full partner in Army senior leader discussions.

When examining the Staff director billets at FORSCOM, it is easy to see that the Army, especially the personnel, operations, logistics, and communications communities, have recognized the value of investing in FORSCOM leadership.²⁶ One option might be to make the natural progression of the Commander of the MI Readiness Command (MIRC) to be the FORSCOM G2. Since the MIRC is a subordinate unit to FORSCOM, the MIRC commander is situated to understand the integration of multi-component formations and would be an asset to the FORSCOM Staff and to the Army IC.

- ◆ **Second**, the Army needs to continue investing in enabling MI capabilities focused on supporting the tac-

tical commander. There are three areas that come to mind: TICOs, MICOs, and E-MIBs. The two FORSCOM Translator/Interpreter Companies (TICO) provide a “go-to-war” capability that the Army has always needed, but had not until recently invested in this capability.²⁷



Photo by SSG Christopher Klurits.

Exercise SENTINEL SAGE. Soldiers with 201st BfSB and 3-2 Stryker BCT, 7th ID, participate in Gryphon Tomahawk MRX at Joint Base Lewis-McChord. The exercise was the largest MI exercise yet to occur at JBLM and involved civilian and military assets from across the U.S.

While The Army Language Program normally addresses the key language mix it recruits (SIGINT collectors and analysts, and CI and HUMINT operators), it never was able to systematically address the rapid deployment needs of the Army. Often the solution for the rapid deployment forces was to search its ranks to find the needed language speaker, often without a clearance and poorly vetted skills to conduct the mission.²⁸ In recent conflicts, the Army leveraged contract linguists, who were hired to address the shortfalls. The TICOs bridge this gap and provide a capability to support training and to be rapidly deployable to support Mission Commanders.

For the foreseeable future, the MICOs will remain the cornerstone of tactical Intelligence presence in our ground formations. The MICOs assigned to each BCT offer a multi-disciplinary intelligence capability for their Commanders. Providing both collection and analysis to the Commander, we need to continue to emphasize the connection of the unit to the greater Army Intelligence enterprise.

An E-MIB will be assigned to each of the Corps and provide reinforcing capabilities to the Corps and its divisions. The E-MIB will serve two purposes: it will give the Corps Commander the resources to “shape” the Intelligence effort, reinforcing collection efforts to solve critical priority intelligence requirements, and through its unique partnership between FORSCOM and INSCOM,

it will ensure the tactical Intelligence force remains connected to the operational-level and national-level IC.

Further, the Army needs to maintain a theater-level interrogation capability. While our current capability is an active duty battalion stationed at Joint Base San Antonio with an interrogation facility on Camp Bullis, Texas, the actual size of the capability could be a multi-COMPO solution with two reserve component battalions. The Army should retain organization with an O-5 commander and active duty staff that can be the focus for this capability, its employment, and continued doctrinal evolution.

- ◆ **Third**, the Army must use FORSCOM to build its next generation of Intelligence leaders. The inactivation of Division Combat Electronic Warfare and Intelligence Battalions left fewer opportunities for tactical MI O-5 commands. Additionally, it left a gap in the coaching and mentoring of junior MI officers.

While the Army did attempt to enhance the Division G2 position by making it a centralized selection board position, it also unencumbered the BCTs and their MI leaders from the Division G2s purview. In a 2013 decision, FORSCOM realigned its BCTs to divisions and divisions to Corps, which will help provide improved leadership and oversight across FORSCOM not



Photo by U.S. Army Sgt. LaToya Nemes

201st BfSB MRX. Soldiers with the 502nd MI Battalion observe a possible improvised explosive device threat during a training exercise. The Sentinel Sage exercise was conducted to prepare the unit for a scheduled deployment.

just the IWfF. An additional gap is the ability of Mission Commanders to integrate IWfFs capabilities and limitations into their planning and execution cycles. Using the “DIVARTY” concept that FORSCOM is championing, there could be a “division intelligence” cell added to the divisions’ staff that could assist with the training and readiness, and leader development of MI Soldiers and leaders at home station and as IWfF synchronization specialists during overseas contingency operations.²⁹

◆ **Fourth**, the Army needs to maintain its IWfF investment in FORSCOM tactical formations. Program Managers and TRADOC Capability Managers must ensure their systems are user-friendly and have the infrastructure to secure the equipment that allows adequate training access. The Installation as a Docking Station (IaADS) concept allows us to use our MI systems on the SIPRnet as would happen during field training and deployments.³⁰ We must build this same functionality into JWICS for our SCI systems. The use of an “IaADS concept for JWICS,” J-IaADS, would assist with units having the proper “authorities to operate,” which is essential to conducting operations on JWICS.

FORSCOM must continue to have MI systems that support its MTOE and employment TTPs. FORSCOM Soldiers must master their analysis “weapon system”, the DCGS-A. Our MI systems must be connected to the networks at home station and proper network authorities to operate must be maintained. Additionally, while the Army has tried to give its MI Soldiers in the field the best software version of DCGS-A available, it may have been doing them a disservice in the process. Specifically, is it better to have an older but still very capable weapon system that the Soldier has mastered or have the “best” weapon system that the Soldier has only familiarity with and lacks true confidence? Proficiency and confidence with the weapon is normally better. Efforts to stabilize software will go a long way toward improving readiness to the force by providing MI Soldiers with increased familiarity with DCGS-A and its associated networks. FORSCOM needs to maintain and expand its formal relationship with INSCOM in this area.

Tactical Intelligence operations cannot be conducted in isolation. The current and future operational environments are too complex for a single unit to direct, collect, and process all the Intelligence it needs to be successful. INSCOM serves the role of linking tactical Intelligence formations to the bigger national and Army ICs, which ensures the tactical Mission Commander and staff have the best Intelligence to incorporate into their common operating picture. FORSCOM and the Army need to ensure the linkages created during this current fight are not weakened, but expanded and made robust. The Army must continue to invest in MI Soldiers across all MI specialties to ensure integration of their capabilities into Mission Command and in the thought process of Corps, division, and BCT commanders.

◆ **Fifth**, the Army needs to invest in the modernization of the threat capabilities at the CTCs. The CTCs continue to

serve as the premier leader development and collective training venue in the world.³¹ FORSCOM and TRADOC commanders have expressed a need for the CTCs to provide a complex, challenging operational environment and for the opposing forces to replicate the latest adversary capabilities. GEN Cone, in 2012’s *Operational Environment to 2028: The Strategic Environment for Unified Land Operations*, noted:

“As our Army transitions from a decade of war, it is critical for us to focus on the future. Successfully preventing conflict, shaping the environment, and winning our Nation’s wars requires substantial preparation across our Army. We must strive to understand the complex future and prepare our Army to operate and adapt in any environment.”³²

In a recent TRADOC Threat Overmatch Assessment, the TRADOC G2 noted there are five areas where the U.S. has Overmatch on the Threat, three areas where there is a transition to Threat Overmatch, six areas where the Threat has Overmatch. An additional five areas have contested capabilities.³³ In FORSCOM’s assessments, culminating in an assessment of the National Training Center and the Joint Readiness Training Center, that overlapped with the TRADOC areas, FORSCOM G2 and G39 looked at four areas: the cyber threat, the EW threat, the unmanned aerial systems threat, and the denial and deception threat to tactical commanders.³⁴

While the FORSCOM assessment highlighted the CTCs’ efforts to challenge the IWfF capabilities and Mission Commanders against adaptable opposing forces (OPFOR) are making great strides, it also noted the two CTCs do not currently replicate many potential future threat capabilities. The Army must ensure the OPFOR at the CTCs replicate the operational environments deployed and RAF forces will likely encounter. Commanders must then incorporate them into their operational planning and train to the right standards at Home Station. We must improve our targeting procedures, and preparations for hostile forces employing EW and computer network attack, development of jamming TTPs to increase denial of communications, including the use of global positioning system jammers, and training to operate in an electro-magnetically compromised environment.

Conclusion

The Intelligence Organization and Stationing Study (IOSS) implemented in 1976 addressed many of the “stovepipe” criticisms Intelligence has faced since the end of WW I. “By the end of the 1980s, the Army had fully implemented the IOSS reforms. Army Intelligence had dedicated assets to support every level in the Army.”³⁵ While the past has been challenging for the FORSCOM IWfF, the last ten years dis-

played its potential and solidified its position in Army forums and discussions. Current Army plans are wrestling with “pooling” concepts in a time of declining resources, seeking to consolidate SIGINT and CI/HUMINT at echelons above Corps.

Despite declining resource, the Army must ensure Commanders at every level and echelon have access to the most current, relevant Intelligence and have adequate resources to influence their operations. There are some senior Army leaders who believe tactical Army units cannot train their MI Soldiers and units to standard and the Army and Department of Defense would be better served if they consolidated and focused on the national priorities. Soldiers and their leaders must remember the tactical fight has not ceased to be important. Speaking before a group of FORSCOM officers, Major General Oliver Dillard recalled the biggest challenge he had as a new Battalion S2 in Korea, in 1950, was the lack of Intelligence at the tactical level. He noted, “I fought to get Intelligence Soldiers out of the Suits and into Boots.”³⁶

While the lack of resources and the threat may seem to be driving the Army to consolidate Intelligence resources, it is also important to keep Soldiers in the Boots and with tactical Commanders, who are responsible for Mission Command. The Army cannot go back to the days where MI was viewed as technically proficient, but incapable of synchronizing its activities “outside the wire.”

Little doubt exists the future of tactical intelligence lies in the hands of the FORSCOM commanders and their SIOs. The use of IROCs to leverage the capabilities of the tactical forces cannot and should not be discounted. Involving Corps, division, and BCT commanders and their staffs in IWFF operational engagement will tremendously enhance the Army’s ability to conduct Mission Command. FORSCOM G2 must guide FORSCOM’s efforts to “prepare conventional forces to provide a sustained flow of trained and ready land power to Combatant Commanders in defense of the Nation at home and abroad.”³⁷ 

Endnotes

1. GEN Daniel B. Allyn, “Building Readiness and Providing Responsive Landpower,” *Army* 63, No. 10 (October 2012), 68.
2. For more information see COL Todd A. Megill, “Ready, Relevant, and Resilient: Ten Ways FORSCOM Builds Intelligence Capabilities,” *Military Intelligence Professional Bulletin* 40, No. 2 (April-June 2014), 10.
3. Henry Cuninghame and Allison Williams, *Elite Magazine* Online, “Forscom G2: Col. Todd Megill,” 1 January 2012. At <http://fbelitemag.com/articles/2012/01/03/1138808>. Accessed 26 December 2012.
4. GEN David M. Rodriguez, “Intelligence Considerations and Challenges from an Operational and Strategic Perspective,” Briefing, Fort Belvoir, Virginia, 20 September 2012.
5. FORSCOM Campaign Plan (January 2012), 8-19. The FCP contains two Intelligence and Security focused major objectives, and 19 critical tasks spread out among the four FCP lines of effort (LOE). The Intelligence manning, equipping, and training tasks are in the Prepare LOE. The Intelligence enabling tasks are in the Shape LOE. Intelligence (CI) support to Force Protection tasks are in the Preserve LOE.
6. MG Gregg C. Potter, U.S. Army, “Intel 2020: A Strategic Path for Army Intelligence,” *Military Intelligence Professional Bulletin* 38, No. 4 (October-December 2012), 32.
7. Dave Chace, FORSCOM Public Affairs, “FORSCOM Breaks Ground on Geospatial Readiness Center after Original Fell to 2011 Tornado,” 18 December 2013, at http://www.army.mil/article/117118/FORSCOM_breaks_ground_on_Geospatial_Readiness_Center_after_original_fell_to_2011_tornado/. Accessed 15 February 2014. The GRC is used by Soldiers from the 100th Engineer Company and civilian staff members to coordinate map and data transfers between NGA and U.S. Army units. While the GRC’s primary focus is supporting the SOF and the GRF located on Fort Bragg, it will also be used to support all of FORSCOM’s Corps and division headquarters.
8. In concert with INSCOM, FC G2X oversees FORMICA operations at three FORSCOM installations with a goal to expand the FORMICA program over the next year to include 100 HUMINT Soldiers across 11 installations.
9. The ISIG ensures the synchronization of the Intelligence Enterprise and expands Army Intelligence capabilities/capacities. It is focused on coordination of POR/QRC transition-National to Tactical training/system integration. Chartered IAW HQDA *General Order #3*, DA DCS, G2 is the ARSTAF lead for ISR integration issues, including plans, policies and architectures. The ISIG provides guidance and direction to meet requirements of the Army Intelligence Enterprise; informs and influences Army/Joint/Intelligence Community and Acquisition governance processes; and enables synchronized Army collaboration with foreign, Joint and National agency partners. The Intelligence Senior Steering Group synchronizes Army MI strategic planning/ Intelligence Community/Congressional Liaison external engagement; drives Army MI strategic planning and communications; provides collective visibility on IC initiatives; and enables unity of effort—full court press on Army MI for MI seniors.
10. LTG Mary A. Legere, “Army Intelligence 2020: Enabling Decisive Operations While Transforming in the Breach,” *Army* 62, No. 10 (October 2012), 169.
11. *FORSCOM G2 MI Readiness Review Results of Analysis*, SURVIAC Contract Number SP0700-03-D-1380, TAT 09-17, DO 314, 27 September 2012.
12. Stephen P. Perkins and William J. Willoughby, FORSCOM White Paper, “FORSCOM LandISRnet” (27 December 27, 2012).
13. USAICoE, *Intelligence 2020* (Fort Huachuca, AZ: 2 July 2012), 3.
14. AR 350-32 Army Foundry Intelligence Training Program, Draft 2013.
15. LTG Mary A. Legere, “Army Intelligence in Support of a Regionally Aligned Army: No Cold Starts and No MI Soldier at Rest,” *Army* 63, No. 10 (October 2013), 164.
16. SSG Chris McCullough, “209th MICO Conducts Comprehensive Training Exercise,” *Press Release* No. 131118-01 (18 November 2013). The 209th provides Intelligence support to 3^d Stryker BCT, 2nd ID.

17. Allyn, 68.
18. GEN Daniel B. Allyn, "FORSCOM Command Training Guidance (CTG)-FY 2014), Supplement 1," Memorandum for Commanders, Major Subordinate Commands/Units Reporting Directly to FORSCOM, Army National Guard Bureau, and Army Service Component Commands, 19 November 2013, 4.
19. Ibid., 4.
20. BG Charles A. Flynn, Email message to authors, "Leader Development Update and Staff Way Ahead," 30 January 2014. The Leader Development Toolbox has a public facing page (www.forscom.army.mil/leaderdevelopment) that seeks to grab your attention and route you to either CAC or non-CAC enabled sites.
21. GEN Daniel B. Allyn, "FORSCOM Leader Development Guidance," Memorandum for Leaders, 7 January 2013, 2.
22. The IEWTPT is the U.S. Army's only simulation system dedicated to training MI analysts in critical wartime skills. Tactical MI units need a means to simulate an opposing force on their ground stations and provide the soldiers operating the IEW systems a realistic picture of the battlefield.
23. TRADOC's TBOC replicates the complexities of the operational environment by leveraging real world data, information, and knowledge in order to enable continuous learning across all TRADOC LOEs.
24. Allyn, FORSCOM CTG-FY 2014, Supplement 1, 6.
25. SFC Brock Jones, 128th Mobile Public Affairs Detachment, "Panther Strike Evolves into New Animal in 2012," DVIDS Online at <http://www.dvidshub.net/news/91208/panther-strike-evolves-into-new-animal-2012#ixzz2tcBLGjDW>. Accessed 18 February 2014.
26. U.S. Army Force Management Support Agency, FORSCOM Headquarters Table of Distribution and Allowances, Document no. FCW3YBAA, E-Date: 16 November 2013, prepared 22 January 2014, 3, 9, 20, 23, 27.
27. The 51st TICO is stationed at Fort Irwin, California and the 52^d TICO is stationed at Fort Polk, Louisiana. These two companies have unique Soldiers assigned to MOS 09L Interpreter/Translator.
28. Author observation in September 1994 while assigned as the III Corps G2 Operations Division Chief. During the Operation UPHOLD DEMOCRACY, III Corps successfully found two Haitian-Creole speakers in 1st Cavalry Division to assist with translator/interpreter duties. One was a cook and the other was a supply specialist. Operation UPHOLD DEMOCRACY was an intervention designed to remove the military regime installed by the 1991 Haitian coup d'état that overthrew the elected President Jean-Bertrand Aristide.
29. Victor Bero, FORSCOM. Email message to LTC Brian Scott, "DIVARTY initiative," 20 February 2014. It is NOT the former Army of Excellence DIVARTY, rather it is a HQ only. However, to get at the atrophy of FA skills in the force, FORSCOM will attach the BCT fires battalions to the DIVARTY at homestation for training and readiness.
30. LTC Obediah T. Blair, Moderator, "Enterprise Network Panel: Installation As A Docking Station," Briefing slides, Fort Gordon, GA, undated, p. 6. <http://www.afceaaugusta.org/Resources/74.pdf>. Accessed 18 February 2014.
31. COL Michael Barbee, "The CTC Program: Leading the March into the Future," *Military Review* 93, No. 4 (July-August 2013), 16.
32. TRADOC, *Operational Environment to 2028: The Strategic Environment for Unified Land Operations* (Fort Eustis, Virginia, 20 August 2012), 1.
33. Mario Hoffman, TRADOC, "Operational Environment" briefing slides, Fort Bragg, North Carolina, 8 January 2014. Mr. Hoffman is the Director, G2 Training (Operational Environment/Opposing Forces) at TRADOC, Joint Base Langley-Eustis, Virginia.
34. Kirk Drennan, FORSCOM, Keep the Commander Informed Paper: *Combat Training Centers (CTC) Threat Modernization*, 3 December 2013.
35. Michael E. Bigelow, Command Historian, INSCOM, "A Short History of Army Intelligence," *Military Intelligence Professional Bulletin*, 38, No. 3 (July-September 2012), 59.
36. MG Oliver W. Dillard, (USA, Retired), telephone interview by Stephen P. Perkins, 23 May 2011.
37. GEN Daniel B. Allyn, "Mission, Vision, and Commander's Intent," Memorandum for Officers, Noncommissioned Officers, Soldiers, and Civilians, 10 May 2013, 2. This is an extract from the FORSCOM Mission Statement.

At the time of the writing of this article COL Megill was the Deputy Chief of Staff, G2, FORSCOM, Fort Bragg, North Carolina. COL Megill served in Operations DESERT SHIELD/STORM and JOINT FORGE and two tours in Operation IRAQI FREEDOM. A 1984 graduate of The Citadel, he holds graduate degrees in strategic intelligence, military art and science, and strategic studies, and is a 2005 graduate of the U.S. Army War College. He is also a graduate of the School of Advanced Military Studies and the Post-Graduate Intelligence Program.

COL Perkins is the Assistant Deputy Chief of Staff, G2, FORSCOM, Fort Bragg, North Carolina. He served the last 20 years of a 30 year career as an MI officer in the U.S. Army. He retired following his assignment on the Multi-National Force-Iraq staff from 2006-2007. A Project Management Professional®, he is a graduate of Cameron University, holds graduate degrees in public administration and strategic studies, and is a 2001 graduate of the U.S. Army War College.



Living Up to Its Legacy: GRCS PED Innovation for Complex Operational Environments

by Sergeant Michael Peralta, Sergeant Christopher Dake,
and Chief Warrant Officer Four Ross W. Glidewell
1st MI Battalion, 66th MI Brigade

Background

Warfighters and ground commanders have relied on the fast, accurate intelligence provided by Guardrail Common Sensor (GR/CS) in multiple theaters of operation. Guardrail was first utilized as an airborne intelligence, surveillance, and reconnaissance (ISR) platform in Germany in 1971, primarily to monitor Soviet, East German, and Czechoslovakian troop movements. After the fall of the Berlin Wall, GR/CS provided ISR support to troops during Operations Desert Shield/Desert Storm. After 9/11, Guardrail was again called upon to be the premier Signals Intelligence (SIGINT) platform in support of Operations Iraqi Freedom/New Dawn and Enduring Freedom/Resolute Support (OEF/ORR). In addition to nonconventional theaters of operations, GR/CS has been integral in providing continuous SIGINT support along the Korean demilitarized zone for over 30 years.¹

Classic GR/CS is defined as a Corps level ISR asset used with a fixed, definable forward line of own troops (FLOT). Multiple aircraft (three is desirable for the best coverage and technical performance) are flown at a standoff distance at the Corps front to peer into the battle space in order to predict and detect 2nd and 3rd echelon enemy schemes of maneuver. Collection was location focused over a wide area. Collected intelligence was fed to national level databases to be utilized by combatant commanders at a later date. This method of intelligence processing, exploitation,

and dissemination (PED) took a long time and did not always account for specific customer needs or timelines.

Legacy GR/CS intelligence PED offered less in terms of near real time (NRT) reporting, and was more successful at offering corroborating intelligence that could be used to develop operational products in conjunction with other types of intelligence. In other words, despite its accuracy, intelligence turn-around from legacy GR/CS systems was slow and therefore was not suited to an unconventional battlefield. From an aviation perspective, traditional GR/CS was flown on a set track with little deviation from the prescribed mission. Pilots had little to no contact with the intelligence professionals at the PED site, providing them with limited mission situational awareness (SA), which hindered their ability to be dynamically re-tasked or extend flight time to support ground operations.

Rewriting the Book on GR/CS Operations

Keeping with the proven mission sets, 1st MI BN and the 66th MI BDE set out to find new ways to employ GR/CS and capitalize on recent mission gear upgrades and new technologies added to the RC-129B. The unit analyzed ways to exploit these new capabilities with quantifiable results and today, GR/CS has evolved to operate in an asymmetric environment absent a known FLOT.

As the post-Cold War battlefield evolved from a traditional battle space to a post 9/11 environment characterized by

current conflicts, it became necessary for GR/CS to evolve into a versatile asset capable of providing both large-scale, strategic intelligence and accurate, NRT, tactical intelligence. 1st MI BN took the traditional GR/CS tactics, techniques, and procedures (TTPs) and developed new ones to better suit the needs of customers engaged in the asymmetric environment of OEF. In addition to the wide-area, large-scale collection that GR/CS is known for, 1st MI BN adapted key positions in the Home Station to provide intelligence at a significantly faster pace.

The battalion utilized Mission Managers (MMs) to oversee and filter collected intelligence, and began tipping in NRT to ground commanders using secure internet relay chat (IRC). In order for this new TTP to work for ground commanders, increased pre-mission coordination and planning was necessary. As an extension of the Guardrail “name brand,” the liaison officer (LNO) is the daily face of Guardrail to the Regional Command Collection Managers and to customers, responsible for fostering unit rapport. He or she is a hand selected, seasoned MM who is collocated downrange with the pilots. The LNO must balance strategic interests while working directly for the customers to establish pattern of life analysis, enemy network exploitation and development, etc.

The LNO is the relay to the Home Station during the mission planning process with customers and aircrews as well as providing GR/CS capabilities briefs to the customers. In a short amount of time, 1st MI BN was able to rewrite the book on GR/CS operations, adapting it to an asymmetric combat environment, and the creating the trust required to operate effectively in today’s combat space. This trust extends from ground units to 1st MI pilots and back to the Home Station.

Developing trust between forward deployed customers and GR/CS operators at Home Station proved to be one of the most difficult challenges to overcome. GR/CS MMs were forced to develop trust with ground commanders and troops via IRC. Without an in-person relationship to build on, the intelligence produced by GR/CS had to be reliable. Over time ground commanders began to recognize the qualities of Guardrail and it became an asset synonymous with speed and reliability.

The pilots, having historical tactical background seeing Troops in Contact, developing and learning NRT IRC threat tips during the Post Mission briefing, recognized a way to bridge communications from the cockpit. After seeing the effectiveness of this NRT tipping 1st MI BN took the Guardrail concept one step further, and began incorporating GR/CS pilots in the PED process by adapting the

“Aircrew Coordination Concept” from the aviation doctrine to fully integrate the pilots, MMs, LNOs, and operators into a working “remote aircrew” dependent on each other for complete mission SA. Unlike traditional aircrews, the intelligence professionals conducting the PED are not located on the platform, but instead are located at the Home Station. By incorporating GR/CS Pilots into the PED process, 1st MI BN was able to transform GR/CS from a solely strategic asset into an extremely valuable tactical asset.

Built into the architecture of the GR/CS hardware is a secure communications line between the GR/CS ground shelters, pilots, and MMs called Voice over Wire (VOW). MMs began utilizing VOW to pass pertinent intelligence to 1st MI BN pilots, who in-turn would pass that intelligence quickly via secure radio to Joint Tactical Air Controllers (JTAC) embedded with Special Operations Forces. This quick accurate intelligence turn-around from Home Station operators to units on the ground has been extremely effective in supporting tactical operations. In an environment where minutes can mean lives, 1st MI BN significantly reduced imminent threat tipping time to units on the ground. In a traditional GR/CS framework, ground troops would not see GR/CS intelligence until hours after it was processed and exploited, or 10 to 15 minutes later utilizing IRC. 1st MI BN has reduced that time to an average of 4 to 7 minutes, utilizing the “direct tipping” method through VOW.

The transition to a more customer focused mission, the incorporation of pilots into the GR/CS PED process, and the method of direct tipping identified an issue between two very different ideologies with little common ground. Army pilots come from a rotary wing background as Chinook, Blackhawk, or Apache pilots, and their tactical experience proved crucial to the success of 1st MI BN GR/CS doctrine. Many of the Military Intelligence (MI) professionals working in the Home Station, however, have limited tactical experience, and have spent most of their time supporting the strategic environment.

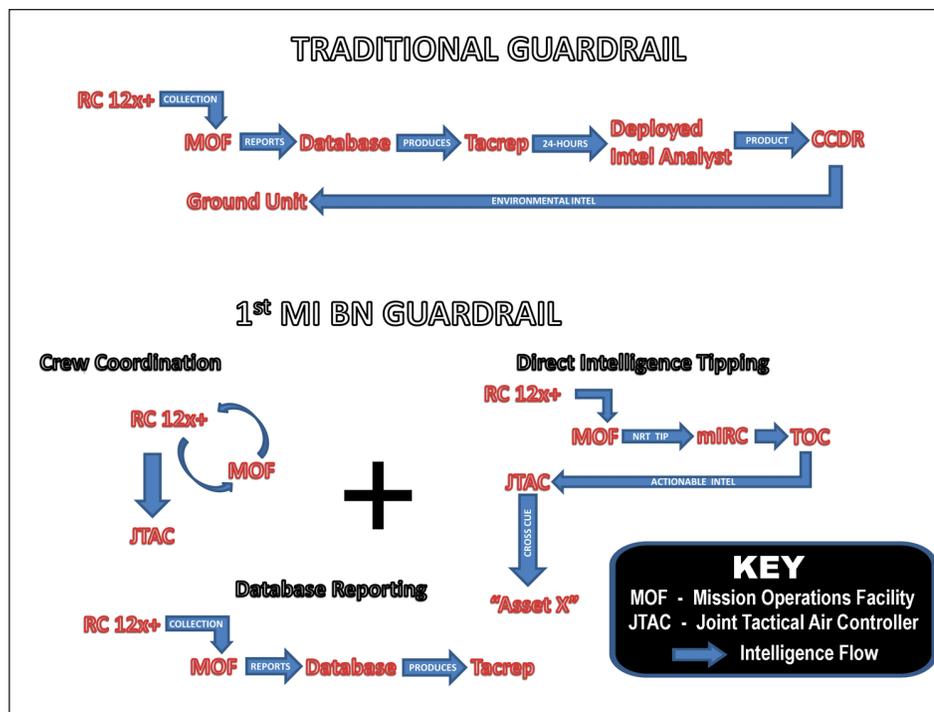
In order to make 1st MI BN’s version of GR/CS successful, it was clear that the pilots and MI professionals needed to learn to trust one another and also to communicate effectively. Upon further review of the pilot and Home Station integration, it became apparent that neither group really understood the other’s job and was unable to effectively communicate or discern the other’s needs or technical lingo. The pilots looked at the MMs, operators, and LNOs as uninitiated junior Soldiers with limited understanding of aviation, far from the actual conflict, and nothing personal at stake.

To break down the perceived divisions a concerted effort was made to educate GR/CS pilots on the intelligence process from the PED side, and the Home Station MMs were educated on the aviation principles and tactical communication. Communication barriers were overcome during educational training. Pilots and MMs began a dialogue on how to collectively improve product output and quality to the customer, and aviation crews began to appreciate the increased, interconnected SA and measurable gains in quality and productivity the new training afforded them. Over time, the full capabilities of the upgraded RC-12+ were realized

As a part of the education process during their initial training and unit integration, 1st MI BN pilots go through Home Station training before learning to fly the mission sets. They work with the MMs and operators during actual missions to cement intelligence collection concepts and theories. This gives the pilots a better understanding of the MM and operator's SA and identifies the operational gaps the pilots must fill for Home Station personnel. The training also puts a face to the voice on the radio. Instructor Pilots work with new MMs and operators to train on aviation TTPs, aviation terminology, weather criteria, performance impacters, and criteria for tip passage to ground troops. The training allows MMs, LNOs, and operators to ask the "dumb" questions they may be afraid to ask (e.g., the effects of thunderstorms, altitude physiology, airspace limitations). The training is designed to build trust and cooperation within the "aircrew" in order to best employ the RC-12X+ to achieve mission goals with the customer needs relayed transparently among all parties.

The "Aircrew Coordination Concept" started paying immediate dividends in combat operations. In addition to the pre-mission coordination and planning that allows 1st MI BN to act as a tactical asset, direct communication with the pilots allows GR/CS to be a more dynamic asset capable of quickly responding to the needs of theater and supported ground troops. Without mutual pre-mission education and constant communication between the "expanded aircrew," previous missions could easily be cancelled due to weather, airspace, or inactivity in targeted collection. Communication between elements, dictated by the OPTEMPO and significance of the event, determine how the pilots configure the plane to maintain the longest station time possible or, as necessary, to relocate for better collect on an event (e.g., troops in contact).

Pilots coordinate with MMs in order to revise or change mission flight tracks because of weather, TICs, or restricted operating zones. In other mission sets, operators will focus on predetermined targets and have the option to place the aircraft into an orbit around a target or vector the aircraft to achieve a high confidence location of the selected target. All instructions are verified by the pilots to prevent flying through significant weather, restricted, or controlled flying areas before the aircraft is relocated. It is difficult to overstate the benefits of this dynamic re-tasking. Not only does it maximize intelligence collection time, the trust between the "remote crew" allows GR/CS to maximize system capabilities to better support the war fighter, resulting in greater force protection and effective enemy neutralization.



The incorporation of 1st MI BN's new mission TTPs provided "name brand" recognition for ground commanders in Afghanistan. In the same way that the trust between 1st MI BN's remote aircrew proved a key ingredient to mission success, ground commanders needed to trust the intelligence they received from a relatively obscure asset in the tactical airspace. 1st MI BN pilots and MMs were persistent in passing quick effective intelligence, until eventually, Guardrail was no longer a secondary player in the tactical environment of OEF, but became a premier platform that commanders requested by name.

1st MI BN's "remote aircrew" concept helped save the lives of many American, Afghan, and Coalition Forces by provid-

ing ground troops early warning of enemy troop movements, attack preparations, ambush preparations, weapons possession and facilitation, IED locations, and enemy network development. In addition to its unparalleled force protection capabilities, GR/CS has also been integral in the neutralization of enemy High Value Individuals.

Conclusion

GR/CS has evolved from a legacy SIGINT platform used at the Corps FLOT to detect 2nd and 3rd echelon communication and movements into a premier SIGINT platform of choice by educated collection managers and customers. Our unconventional TTPs are proven in combat and based on adapting the “Aircrew Coordination Concept” from aviation doctrine. Committing to the principles of education and communication through mutual confidence and cooperation by pilots, MMs, and LNOs allows for collection in areas, around weather, and in airspace that previously would have cancelled the mission leaving the customer without SIGINT coverage.

Today, GR/CS simultaneously supports strategic initiatives and tactical objectives. Education and integration of Home Station personnel into the cockpit using the “Aircrew Coordination Concept” as the foundation allows us to simultaneously provide tailored, accurate NRT intelligence directly to the combatant commander, helping him or her shape the battle space before the first shot is ever fired.

These TTPs, however unconventional, have saved numerous lives in combat, helped to earn name brand recognition for 1st MI BN, and created an overwhelming demand for GR/CS coverage at both the strategic and tactical levels. ✪

Endnote

1. Brandon Pollachek, “Guardrail Turns 40, Modernization Keeps it Going,” ARMY.MIL, 8 July 2011. At http://www.army.mil/article/61251/Guardrail_turns_40_modernization_keeps_it_going/.

SGT Peralta is an MOS 35P, Cryptologic Linguist. He is a graduate of both the Defense Language Institute and the Persian-Farsi Cryptologic Basic Course. He is currently assigned to C Company, 1st MI BN (AE) in Wiesbaden, Germany where he serves as a Senior Mission Manager for Guardrail Operations. During his time at 1st MI BN, SGT Peralta also served as the Guardrail LNO while forward deployed to Afghanistan during OEF.

SGT Dake has been stationed at Fort Hood, Texas and Wiesbaden, Germany as well as having served in Iraq in 2010 and Afghanistan in 2012. He is currently assigned to the 1st MI BN having served as an LNO as well as supervising the Aerial Precision Geo-Location Section and was recently selected for Warrant Officer.

In addition to CW4 Glidewell’s initial service as a CH-47 Chinook pilot, he has served in Guardrail assignments in the 3rd MI BN (AE) and 1st MI BN (AE). He served as an Instructor Pilot and Maintenance Pilot at 3rd MI BN (AE), Camp Humphreys, Korea from 2010-2012. He is currently assigned to 1st MI BN (AE) in Wiesbaden, Germany as a Standardization Instructor Pilot. CW4 Glidewell has served multiple tours with 1st MI’s Guardrail detachment in Afghanistan in support of OEF and ORS from 2012 to present.

Fort Huachuca Museum



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





Enabling Decision Confidence by Mitigating Four Interacting Dilemmas Facing the Army Intelligence Enterprise

by Colonel Nichoel E. Brooks and Jami Forbes

Introduction

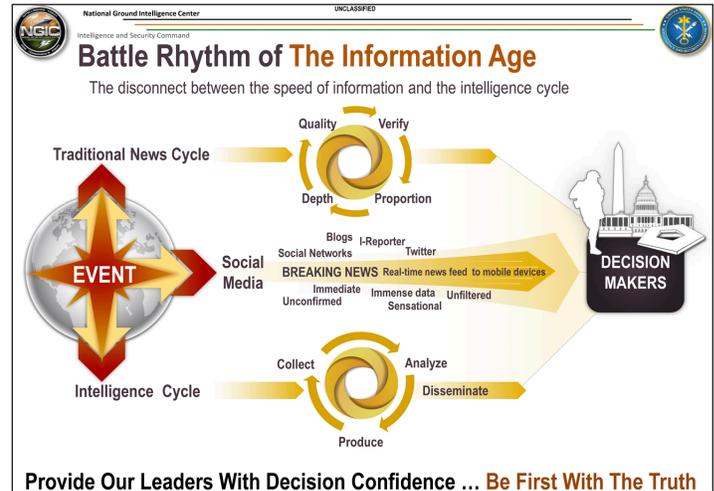
The intelligence enterprise is at a crossroads—it is facing an environment of shrinking resources while also being expected to meet growing responsibilities and requirements. In particular, the Army Intelligence Corps, seasoned by decades of war in Iraq and Afghanistan, must expand its focus to more complex and unpredictable global threats and issues.

Emerging adversarial forces, enabled in part by technological advancements and increased access to information, are becoming more adaptive, decentralized, and transnational than ever before. In addition, the developing missions of the Army’s Global Response Force (GRF) and Regionally Aligned Forces (RAF) require a greater understanding of not only unconventional and adaptive adversarial forces, but diverse human domains across the world. Intelligence must be agile enough to help win current and future contingencies, while also supporting efforts to prevent conflict and providing the information needed to shape the global environment.

Technologies and rapidly changing world conditions are creating unprecedented challenges for the intelligence process. The intelligence cycle—which has long centered on a hierarchical, regional, and centralized enemy—has traditionally spanned weeks and months. However, this process must change in order to meet current conditions and mission demands. The accelerated pace of conflict is limiting the amount of time Army commanders have to both shape the environment and form decisions, reducing the intelligence cycle to a mere days and minutes. Undoubtedly, the demand for timely, predictive, and accurate intelligence is more important than ever.

How will we ensure national security in this new environment? How will the Army Intelligence Corps foster trust and provide its leaders with decision confidence? How will we not only be first with information, but first with the truth? In order to evolve and meet these challenges, we must first recognize four basic interlocking dilemmas that are facing the broader Intelligence Community (IC) today. These dilemmas center on capacity, transparency, data, and time.

The Four Dilemmas Facing Army Intelligence



Provide Our Leaders With Decision Confidence ... Be First With The Truth

“Although the Intelligence Corps is faced with interlocking dilemmas involving capacity (increasing demand for intelligence during an era of declining resources), transparency (opaqueness between organizations), data (greater access to data than ever before), and time (the rapid battle rhythm of the information age), there are steps underway to help mitigate these issues”

Capacity. Declines in the Army’s end strength and shifting fiscal priorities are realities all Army pillars are currently facing. However, for the Intelligence Corps, the reduction of resources comes at a time when an increasingly complex operational environment is driving greater demand for analytical capacity.

Army intelligence must continue to support requirements in Iraq and Afghanistan, while also broadening its understanding of conflicts involving adaptive sub-state actors in the Middle East and North Africa, the expanding crisis and threat to regional stability in Syria, emerging missions and new allies in Africa, and growing cyber threats. In addition, intelligence professionals will be required to bolster support to RAF and GRF by providing information on local populations, political officials, power brokers, and the global human domain—all critical data points in helping to foster enduring partnerships around the world.

Transparency. Challenges relating to declining capacity directly interlock with dilemmas involving transparency.

Intelligence organizations are often opaque, and rightfully take steps to protect information from adversarial forces. However, these efforts also often extend to intra-organizational relationships, and inhibit potential avenues for collaboration and partnership between U.S. intelligence assets.

The lack of transparency among organizations makes it difficult to form efficiencies, and makes it especially challenging for intelligence consumers to route questions and requirements via the most effective method. For example, in order to answer critical intelligence questions, an Army customer may submit requests for information to several organizations at a time, causing multiple analysts to be occupied with answering the same requirement.

Given the increasingly austere conditions and dwindling resources, Army intelligence can no longer afford such redundancies, and must bolster efforts to federate intelligence production, improve collaboration, and continuously dialogue with customers and partners in order to stay responsive to changing priorities. As former Director of the Defense Intelligence Agency, LTG Michael Flynn once stated, “the single biggest threat to our national security is our inability to work together” as an intelligence force.

Data. The third dilemma is data. Technological advances have enabled intelligence professionals to have greater access to data than ever before. The increased use of social media both by adversarial forces and the human domain means that information can be diffused across a group, network, or even the globe within seconds. Events such as the September 2014 demonstrations in Hong Kong also reveal how significant social media can be in activating a population and influencing global political and social dynamics. It also reflects how important open source information and intelligence is to understanding environments around the world. Emerging sources of publicly available information enable new applications for network analysis, providing insight into narratives, locations, and personalities.

In addition, RAF initiatives will allow our forces to have unprecedented first-hand insight into events and the human domain across the globe. Regional forces, as part of joint, integrated, and often multi-national teams, will benefit from personal contact and direct observations. The information will enhance our understanding of the operational environment, and provide the background necessary for commanders’ awareness in an increasingly uncertain world.

However, while increased access to data provides greater sources of information to draw from, the volume of data provides unique challenges. Not only must intelligence officials develop mechanisms to keep up with the rapid pace of

data flows, but derive relevant meaning, and manage huge quantities of collected data. Information must quickly and efficiently be assessed in order to support leaders needs for competent decision making in today’s strategic environment, but must also stay within the constraints of intelligence oversight and ethical boundaries.

Time. The final interlocking dilemma is time. How do we process large amounts of data quickly, make the right type of information discoverable, and be “first with the truth” for decision makers?

In today’s information age, the battle rhythm is more demanding than ever before. Intelligence, which used to be processed in weeks or days now must be processed in days or hours (and in some instances, nanoseconds). Information is instantaneous and global, and the speed at which it now travels has created challenges for the traditional intelligence cycle.

What used to be a formalized requirements process based on pre-determined planning has given way to a more fluid progression driven by real time changing conditions. Today’s adversaries are unconventional, adaptable, multi-nodal, and global. The traditional method of doing things will simply not work in this environment.

How to Mitigate these Dilemmas

Fortunately, given the interlocking nature of the dilemmas, each one affects the other. Efforts to mitigate one dilemma will inherently work to impact the others. The first step in working towards this goal, however, is likely the most tenuous. Intelligence organizations, often bureaucratic and slow to change, must recognize that the traditional methods of conducting business will not work in the new environment. The business model for intelligence analysis has not fundamentally changed in 20 years, and must become more agile and adaptable than ever before. In order to meet current and future requirements, we must increase capacity through limiting redundancies and duplicative efforts, forging analytical partnerships, bolstering intelligence integration, and leveraging information technology to efficiently share products and knowledge.

Several initiatives are currently underway which are working to meet such challenges, including the formalization of the Army Program of Analysis, the creation of the Army Knowledge Gateway, the Theater Intelligence Brigade (TIB) as the Anchor concept, and emerging analytical models. In addition, the Intelligence Corps can look to mitigate the dilemmas through incorporating “quick win” and cost effective changes such as embracing innovative, disruptive, and creative thinking.

The Army Program of Analysis

For Fiscal Year 2015 the Army G2 provided guidance regarding the establishment of a Program of Analysis (POA). The POA is a process that synchronizes analytical production and planning of the Army Intelligence Corps. It also helps to close analytical coverage gaps, prevents duplication of effort and inefficiencies, and helps to provide timely and accurate regionally-focused intelligence products.

The cornerstone of the POA initiative is centered on input from Army Commanders, who have been asked to identify key areas of concern and intelligence gaps, and provide feedback to the current planned production.

In addition, by providing visibility on all-source and Geospatial Intelligence (GEOINT) production plans and efforts, the POA enables the Intelligence Corps to leverage analytical partnerships within its ranks, as well as among the Joint Force and the IC. No longer will there be ambiguity regarding what an organization is planning to work on—rather, there will be greater access and opportunity for federation, collaboration, and partnership.

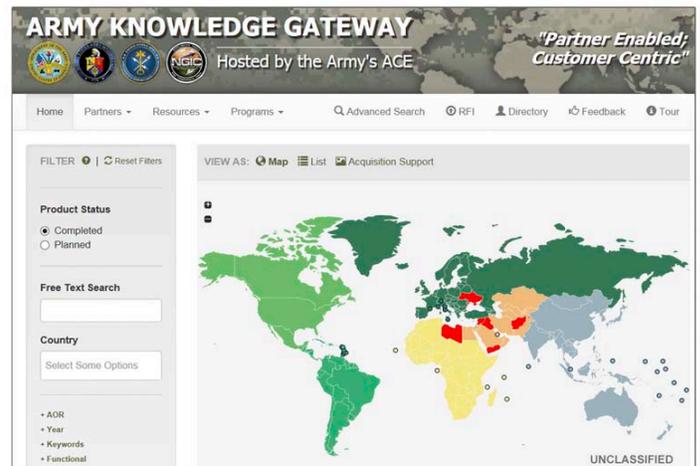
Because the POA is nested within Department of Defense and national intelligence production planning, it provides Army Commanders with an unprecedented opportunity to articulate their intelligence needs and priorities. Further, regular dialogue between decision makers and intelligence producers during POA crafting and implementation affords leaders the opportunity to quickly adjust production priorities based on shifting dynamics within their assigned geographic regions.

The Army Knowledge Gateway

In 2014, the Army National Ground Intelligence Center (NGIC) was tasked to develop an Army intelligence enterprise capability that would enable users to quickly discover and access all-source and GEOINT production from not only among the Army Intelligence Corps, but the broader IC as well.

The Army Knowledge Gateway (AKG) is a web-based interface available on multiple networks, and provides access to products based on geographic or functional areas of interest. For example, customers with intelligence requirements for a particular region can click on that country on the map and see not only finished products, but planned production and points of contact. When it reaches full operating capability, the AKG will reflect intelligence planning and production throughout the Defense Intelligence Enterprise, from the Defense Intelligence Agency and NGIC to the Army Service Component Command and Corps G2s. The AKG represents a significant step towards connecting

tactical and operational intelligence forces, while simplifying the means in which consumers of intelligence can find relevant information.



TIB as the Anchor Point

“TIB as the Anchor Point” is an Intelligence and Security Command (INSCOM) initiative that places the Theater Intelligence Brigades as the focal point for integrating Theater Intelligence Requirements. The TIBs are located around the globe, and are a key conduit for operational intelligence collection and collaboration, particularly with RAF units. In partnership with the INSCOM functional brigades and TIBs, NGIC serves as the Army’s enterprise lead for All Source Analysis. It also serves as the Army’s National Level ACE—and works to provide the foundational and strategic scene setter, helping to enable operational and tactical applications.

NGIC’s role in the “TIB as the Anchor Point” initiative will be to bridge the strategic environment and the broader IC with the TIBs. This will be achieved through developing intelligence communities of effort, producing foundational intelligence products (such as GEOINT, identity intelligence, weapons and systems, and emerging/disruptive technologies), and providing direct support to training and exercises. In addition, NGIC will help to increase discovery of operational intelligence by prominently displaying TIB data in the AKG.

Challenging Current Analytic Models—ABI and OBP

In conjunction with the POA and AKG initiatives, other efforts are underway within the IC that will help to mitigate the interlocking dilemmas as well as modernize analytical practices and business models. Two of the most innovative are Activity Based Intelligence (ABI) and Object Based Production (OBP). These processes help transform intelligence practices that have not been updated in decades.

ABI is an approach that will mitigate issues involving capacity, data, and time. ABI seeks to help analysts visualize vast sources of data both temporally and spatially so that they may interpret the information quickly, derive relevant meaning, and drive intelligence production. In essence, it helps an analyst see activities, how they relate to one another, and identify their significance within a broader picture.

OBP complements ABI in that it helps analysts parse a wide variety of data through the categorical and hierarchical organization of intelligence production. While ABI centers on the collective significance of activities, OBP is an organizing principle that organizes intelligence based on an object (a person, place, event, issue, etc.). In particular, it aids analytical tradecraft and consumers by helping to organize data and provide greater discovery of known intelligence information. OBP will help mitigate issues involving transparency by feeding data back into multiple analytic programs employed by the IC.

Open Source Research Capabilities

In addition, efforts are underway to harness vast new sources of information available through open source domains. The value of Open Source Intelligence (OSINT) is more important than ever and is a critical component of the modern information domain. NGIC is coordinating the establishment of an Army OSINT lab, which will provide a specially trained group of analysts with access to unique analytical and search tools to find the right information through the use of tradecraft while maintaining operational security and abiding by intelligence oversight requirements.

New Business Practices

Fostering change and adopting new practices is difficult in any organization, let alone government agencies—which are often large, horizontal, and rely on tradition. However, as John Kotter, Harvard Business School, outlines leading change must start with identifying a sense of urgency, and embracing initiatives such as quick wins. Allowing for “disruptive” and creative thinking are quick wins, and not only require little to no cost (an advantage in today’s era of budget cuts), but are necessary agents of change that will be required in order to meet upcoming challenges. The Intelligence Corps can begin this process through encourag-

ing collaboration and discussion, and fostering partnerships that will allow the greater intelligence enterprise to form communities of interest that will work together to solve problems.

Outlook

The changing operational environment is presenting unique and unprecedented challenges, particularly for the intelligence discipline. Emerging adversarial forces and mission requirements will be more complex and adaptable than ever before, while the information environment will be faster paced and more demanding. The future is a sharp break from the past, and requires new ways of thinking about the world.

Although the Intelligence Corps is faced with interlocking dilemmas involving capacity (increasing demand for intelligence during an era of declining resources), transparency (opaqueness between organizations), data (greater access to data than ever before), and time (the rapid battle rhythm of the information age), there are steps underway to help mitigate these issues.

In conjunction with its partners in the broader IC, the Army’s Intelligence Enterprise can work to identify new partnerships, leverage information technology, increase collaboration, and employ new analytical models and update intelligence business models. Initiatives such as the POA and AKG will help transform Army intelligence to meet new demands, answer critical intelligence gaps, aid RAF and GRF units, and enable leaders to have decision confidence. These efforts will be empowered by complementary initiatives within the IC to modernize processes such as ABI, OBP, and OSINT labs. Together we can find strength through collaboration and integrated capacity, and the Intelligence Corps will rise to the challenges of today’s complex environments and bolster our nation’s ability to prevent, shape, and win future contingencies. 

Colonel Nichoel Brooks is currently the Commander of NGIC. She has served as the Executive Officer of the Defense Intelligence Agency and as Commander of the 310th MI Battalion.

Jami Forbes is Department of the Army analyst currently assigned to NGIC. She specializes in studies on insurgency and has completed several deployments to Afghanistan.

Intelligence Support to CENTCOM Materiel Recovery Element



by Major Joshua J. Smith



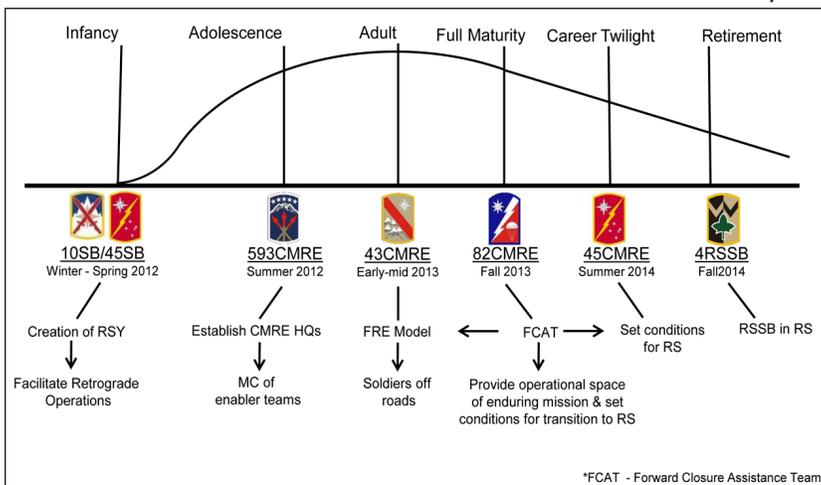
Introduction

The CENTCOM Materiel Recovery Element (CMRE) was first conceived in Afghanistan in 2012 from a realized need through lessons learned during the withdrawal from Iraq. The first unit to initiate this new mission was the 45th Sustainment Brigade (SB) starting with a retrograde sort yard (RSY) to emplace procedures for a deliberate retrograde and redistribution of materiel. Over the nearly three years of the CMRE mission three other SBs have executed the mission which came full circle back to 45th SB to evolve the CMRE mission into the Resolute Support Sustainment Brigade to support the changing mission in Afghanistan. Many changes have occurred, improving operations and procedures. These will be discussed in the context of intelligence warfighting function support to sustainment operations and the CMRE.

CMRE Mission—Sort, Retrograde, Deconstruct

The SB S2 focuses primarily on the main supply route/alternate supply routes (MSR/ASR), while the operational environment owner (OEO) S2 focuses on the larger area, or the urban areas and spaces in between and around the MSR/ASR. The CMRE has a focus on portions in both of these areas. As the CMRE pushes materiel out of an area, either to an RSY or through a ground line of communication (GLOC) the interest is on the flow of traffic and locally contracted white truck movement. The CMRE is also concerned with the installations and security zones around it as an installation is deconstructed.

The typical SB has a unique perspective of the OE. With the organic Quartermaster and Transportation units, and possibly also Engineer, moving over the road networks each day they are able to understand the normal conditions and recognize the subtle changes which provide the OEO with vital information and intelligence.



This hybrid intelligence mission focuses on how the CMRE views the battlefield, communicating in the Combined Joint Operational Area—Afghanistan (CJOA-A), supporting Force Protection (FP), and focus areas for pre-deployment training and preparation.

As the CMRE mission falls to the SB, so with it comes the limited personnel and minimal resources. As a result of this, it is key that an S2 must be an integral part of not only higher and lower headquarters but to each Regional Command (RC) or Train, Assist, Advise Command (TAAC). These commands and other government agencies provide much of the support required for awareness and analysis. The art of extracting the vital timely intelligence from the vast amount of information compiled and disseminated daily is a delicate process. The first step is to answer the question “What is needed now to aid in the military decision making process (MDMP) and provide the framework for relevant and timely decision support?” Defining the few key tasks and areas of focus to support the OEO until they have retrograded to the

point of the focus shifting to other areas and maintaining support to the CMRE is a unique facet of the intelligence mission.

The Battlefield through CMRE Eyes

Though each of the four SBs that were charged with the CMRE mission conducted operations differently to address the rapid changes of retrograding and supporting the closure of the Afghanistan Theater, root factors and concerns remained the same. An area of operations (AO) that spans an entire country, not an RC or two, is not the norm for the SB. Previously, two SBs would cover the CJOA-A. The AO becomes the specific installations and the area of interest (AOI) is now the MSR/ASR. Should the MSR status change or become impaired or the materiel is unable to pass, everything becomes backed up causing a "log jam" and the mission is hindered or delayed. The CMRE doesn't move the materiel and has little influence on the security of the MSR. The mission of the S2 becomes more predictive, defensive and forward looking to complete the mission. The analysis must focus on the future passability of an MSR or GLOC and less on the immediate threat of attack on the convoy. That analysis that will identify the event that will close a route or gate over a longer duration of time before the event occurs, rather than the improvised explosive device (IED) that will slow traffic today.

Information to predict reduced flow through an MSR, gate, or GLOC must be drawn from less common sources. The patterns of life and significant activities become less relevant and a more holistic view and approach must be taken. When conducting analysis, less of the Military portion of PMESII-PT must be looked at and a more in-depth look must be taken at the political, economic and social aspects.

The most effective intelligence an S2 provides a CMRE commander is the prediction of delaying circumstances giving the commander the knowledge needed to support decisions of flow and routes. Tactical level intelligence plays a small role in the intelligence support to the commander. In the traditional SB role a commander would most likely need more of this; for a CMRE a more operational, local, and/or strategic focus, as effects throughout a theater of operations will affect the movement and flow of materiel. It should be noted that, a CMRE may not be able to directly influence or affect decisions on what occurs but some foresight in reduced flow to an area may reduce the overall effect on the mission.

An example of this is the closure of a GLOC due to local government no longer securing the area and allowing its people to protest. This effectively closes the GLOC for rea-

sons the CMRE was not part of. It is the second and third order effects of a decision made by the OEO to execute (or the method of execution) the Theater mission that trickles down to affect the CMRE. In some cases this cannot be helped but the analysis must be provided to show a commander how (and the duration) this affects the flow of retrograded equipment. A closure for a day may not show much impact to the CMRE mission; a closure for 30+ days may back up holding yards to the point of over taxing the yard's storage space slowing its productivity.

One task the S2 always has is getting inside the planning and attack cycles of the enemy. The CMRE is able to do this by assessing political, social, and economic areas of concern as well as potential areas of engagement. At the initial onset of the CMRE mission all materiel was hauled by truck, (military and contracted white truck off an installation) and moved to a central hub containing an RSY. This process was not only costly but forced many Soldiers and equipment to be placed at a higher risk. As the process slowly morphed into how the mission is executed now, a series of RSY and forward retrograde elements (FRE) are set up across the CJOA-A like a spider web of retrograde support. One of the secondary effects of this is a disruption in the insurgency support base surrounding an installation. With actions pushed to a local area so also comes additional required local contractor support that would normally be filled at a large installation. With the economic benefits of contracting and sale of scrap material to the local community the enemy's ability to disrupt and destroy is reduced. A threat is still there but the forces on the installation were more a part of the local economic system than a threat.

The greatest threat on CMRE operations is indirect fire (IDF) or Green on Blue attacks. Often CMRE elements would be tied to local disputes over materiel or land. As time went on the focus of responsibility for causing these disputes turned away from the CMRE and more to the Afghanistan Government office that was levying the requirement. If an area was to be transferred to the Afghans (this was any government entity from the Ministry of Education building a school for women to the Afghanistan National Army establishing their own installation) the facilities were released through a Foreign Excess Personal Property (FEPP) or Foreign Excess Real Property (FERP) process. These were agreed upon between the land owner or recipient and a Coalition Forces' representative. Only that which is determined to be able to be maintained by the recipient and is demilitarized is offered.

An example of FEPP is used appliances that have little value (either because of condition or function) to the Army

supply system and are not deemed worth the risk or cost to have critical military assets, both Soldiers and trucks, move them across the country or the added expense of shipping back to the U.S. An example of FERP is something that can't be hauled away as a usable item (i.e., concrete pads, brick structures, or water and power infrastructure). FERP can also include buildings. FEPP items (i.e., heating and air conditioning units) inside buildings remain and become part of the FERP.

With the enacting of this process, enemy significant actions were greatly reduced. The few disputes over shares of materiel or control of land were minor in comparison to the previous frequency and severity of attacks.

Communicating across CJOA-A

No unit conducts operations in a vacuum. Communication throughout the unit's ranks and across the Theater, both higher and lower, is critical. Operating over the entire CJOA, the units and their daily business practices vary greatly. Each RC or TAAC will have their preferred systems for mission command and enemy threats. The Capital region will focus on magnetically attached improvised explosive devices and vehicle borne improvised explosive devices (VBIED); East region may add IDF also; South and Southwest will see IDF and IED before VBIED as the primary threat. Commonalities will always occur for threats, specifically Green on Blue threats and attacks. Where the specific unit or troops are at a given time will drive the focus of the S2. The RC intelligence sections provide a good indicator but the Task Force covering an installation is key to communicate with.

In effectively communicating with commands while conducting operations across the CJOA, the S2 must be fluid and capable of operating on an array of systems. Each region operates with their primary form of communication or platform for an intelligence common operational picture (COP). Some systems are part of an Army program of record; others will be third party. There is no longer a one-stop shop for communicating or gaining awareness of ongoing events in real time. The final submission of events or reports will be published on common databases such as multimedia message manager (M3). The process for finalization and publication is not timely enough for battle tracking and requires an S2 to be tied into live feeds and conversations.

Using programs such as Adobe Connect to Microsoft Internet Relay Chat (mIRC) to joint chat (J-Chat) or the Command Post of the Future (CPOF) over different networks battle tracking becomes a daunting task. The task is manageable if the initial communication is done with the OEO/base operating support-integrator (BOS-I) and work-

ing relationships are established. Without the relationship building of analyst to analyst connections, intelligence sharing and threat tracking can't be done in a timely manner.

Force Protection (FP) with Heavy Intelligence Injects and Support

FP is a high priority that is always built into each plan. Within the vast area (roughly the size of Texas) in which the CMRE operates enemy tactics, techniques and procedures (TTP) will change as open plains and desert in the East change to mountainous vegetated areas where the foothills of the Hindu Kush mountain range begin. When an element would go to a new area a threat assessment would be conducted along with an FP analysis. Upon arriving at a new area all FP would already be in place as these were mature installations. As the installation was reduced to the agreed upon transition size or back to the original state of the land prior to construction, the security threat to the installation increased. It is important to remain cognizant of not only the change in enemy TTPs across the RC/TAACs as mentioned previously but also the cultural aspects. An Afghan power base must be maintained for local political and military leaders as operations are conducted to ensure continuation once Coalition Forces leave.

A disruption in this hierarchy or natural economic flow causes devastating effects to Soldiers and equipment. Examples of this can be found in analysis of enemy attacks during the closing of installations. Attacks have occurred over control of land or the hand over and distribution of materiel and resources to the local population. The ownership and distribution of materiel and resources must be thought out. Is it best to give to a local elder or leader and let him decide or should coalition forces distribute everything equally? In some cases in small communities and rural areas, distribution done incorrectly causes a shift from a typical insurgent TTP to an attack directly on a weakened installation as opposed to a convoy.

In other more urban areas when local contracts or security forces became more involved we would see a natural Afghan economic flow occur. Local security commanders would gather waste (from the CMRE perspective) materiel and consolidate it for sale and construction. During the deconstruction of an installation the wood from razed buildings was collected by Afghans and consolidated until removal could occur. All of this was done by the order of the local Afghan commander ensuring equal distribution and preventing the monopolizing of materiel amongst local entities. Safety and security was maintained for U.S. Soldiers and the Afghan people, attacks decreased and no significant events or attacks occurred.

If an installation is transitioned, defensive capabilities are reduced with the size of the base. One of the most vital assets to an installation is an Aerostat. Installations where an Aerostat could be transferred to the Afghans had fewer threats than those that lost their “eye in the sky” to deter enemy activity, provide early warning, and identify hostile activity. It was identified that early forward positioning an FP Officer and an MOS 35F (Intelligence Analyst) to build relationships and tie into the base defense operations paid great dividends. Each installation base defense cell or TF along with the human intelligence and counter intelligence teams become our best source of intelligence. As the BOS-I leaves, only small security elements remain with maybe as little as concertina wire in the final days. Tracking subtle changes in enemy activity and constant adjustment of FP measures are essential.

The CMRE is not tasked, equipped, or placed to assume the traditional roles and responsibilities of any defense entity. It is not until the final weeks or days that this responsibility becomes critical for the CMRE to assume. With the reduction of the remaining barriers and walls it becomes incumbent of the CMRE to ensure security and awareness is maintained during operations. As BOS-I and integrated base defense controls and protects throughout the base security zone, the CMRE S2/FP becomes important and a contributor/enabler as all organic assets are moved or descoped.

Train up and Preparation

As the intelligence section began to prepare for this unique mission the leadership looked at what would be the most important tools and our primary weapon systems. In an SB the analysts primary weapon system is the Distributed Common Ground Station—Army (DCGS-A). Even with the utilization of other systems in-Theater such as Palantir, DCGS-A still plays a significant role. Receiving the latest upgraded hardware was critical to tying into the Theater intelligence architecture. Another key piece of hardware to have on hand is the Global Broadcast System (GBS). Even with all the other systems providing the same feeds and information, having a secondary system or one that does not draw from the same bandwidth the rest of the Brigade is using provides another key system to keep the unit tied into intelligence feeds.

Additional classroom training was conducted prior to the intelligence section’s deployment that resulted in gains of efficiency. Having little to no garrison requirement for a DCGS-A, skills are lost. The DCGS-A Pre-deployment Operator’s Course offered through Foundry becomes critical. This is also true for the GBS Users’ Course. Other non-system based training like the Green on Blue Train the

Trainer Course provided the ability to disseminate more effectively on awareness of insider threat to organic lower units, increasing awareness and survivor ability. The other intelligence related course that produced great dividends in the accuracy and effectiveness of intelligence operations and support is the foreign disclosure representative course. With the diverse groups, whether other North American Treaty Organization countries or Afghanistan, the CMRE provides many products at various classifications across multiple networks. This responsibility takes a marked amount of time and if not done correctly will initiate significant consequences. Training and guides are available but a close tie to the RC/TAAC Foreign Disclosure Officer is critical.

Non-Foundry or intelligence related courses worth considering are CPOF and Blue Force Tracker (BFT). Though not always associated with the S2 section, many commands will use CPOF and post SIGACTs or other pertinent information on these systems. The challenge of tying into all the needed data streams and locations is eased if you are able to observe the COP other commands in your unit or the BOS-I you are supporting are utilizing. By utilizing the CPOF you are also able to provide an enemy or threat COP in a format that can be easily transferred to the system those you are supporting are operating on and increase the flow and timeliness of information you are providing. The BFT becomes a tool for your awareness as convoys move along the MSR/ASRs. With the software already built into the BFT timely critical situational updates can be pushed to those convoys that may be directly affected. An example of this would be IED emplacing reports or engagements occurring further ahead on the MSR/ASR.

Conclusion

For the SB S2 section the intelligence duties and responsibilities are the same as other S2 sections but the focus changes rapidly and the section TTPs must be able to change rapidly and adjust with the changing focus and shift in responsibilities to maintain the flow of timely and accurate intelligence to support MDMP and the commander. The focus is not always military but more political, economic and social. The dynamic OE varies and changes from mature to austere conditions and expeditionary capabilities. The CMRE must be able to adapt to various systems and to areas with varying capabilities and requirements, whether it’s drawing support from the OE’s organic units or conducting additional analysis to support FP.

The CMRE mission from inception to its current operation has changed due to the changing environment and reduction in both forces and infrastructure throughout the Theater. The support to the mission by the S2 is fluid and

varies as the area the CMRE elements are operating in reduces and infrastructure disappears. To maintain the effectiveness and better complete the mission objectives the operation must merge with the diverse drivers in play in the region. By acknowledging and incorporating these unique drivers the S2 can play an improved role and better serve the overall operational effectiveness.

By utilizing the information at the lowest levels and assessing the situation around a FOB from the BOS-I and FP units, an S2 can better forecast the impact and threat to the CMRE personnel and remaining infrastructure or lack thereof if the land is returned to its original state. Further the S2 looks toward the local, political, religious, and cul-

tural aspects of the Theater of operation. Local opinion greatly impacts operations both positively and negatively and must be taken into account. As noted this non-traditional Sustainment Brigade intelligence methodology can pay great dividends to the overall mission by ensuring security is maintained. 

MAJ Smith currently serves as the Brigade S2 for 45th Sustainment Brigade. Previously he served as the 541st CSSB S2; MiTT Intelligence Advisor; Company Commander, 297th MI BN; Assistant S2, 2nd Brigade, 1st Infantry Division, and USARPAC Collection Manager. He has deployed in support of OIF and OEF. MAJ Smith holds degrees from Valley Forge Military College and King's College.

TRADOC CULTURE CENTER

Mission Statement: Established in 2004, TCC provides relevant and accredited cultural competency training and education to Soldiers and DA Civilians in order to build and sustain an Army with the right blend of cultural competency capabilities to facilitate a wide range of operations, now and in the future.

Request training through ATRRS
Course Number:
9E-F36/920-F30 (CT-MTT)

TRAINING AND EDUCATION



Available Training: The TCC provides training and education in cross-cultural competence skills, regional expertise, and functional topics in support of the CJCSI 3126.01A Language, Regional Expertise, and Culture (LREC) competency factors at the basic or fully proficient levels. The course is tailored to meet the requesting unit's cultural competence requirements in these areas.

Cross-Cultural Competence Skills Topics:

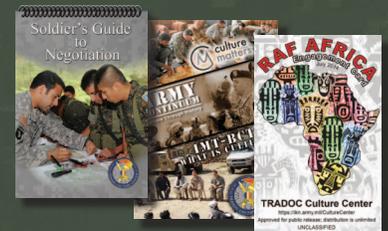
- What is Culture?
- Cross-Cultural Communication
- Cross-Cultural Negotiation
- Cross-Cultural Rapport Building
- Self-awareness and Perspective-taking

Regional Expertise:

- AFRICOM, CENTCOM, EUCOM, NORTHCOM, PACOM, SOUTHCOM
- Smart Cards and Smart Books are also available

Functional Topics:

- Key Leader Engagement
- Culture and Female Engagement Teams



Primary Training Focus:

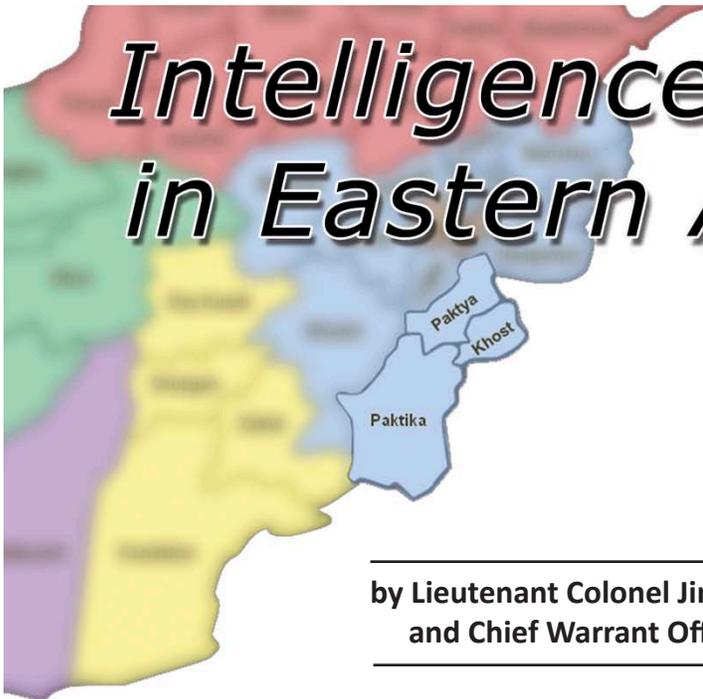
- OEF Pre-Deployment Training
- Regionally Aligned Forces
- Train-the-Trainer events
- Advanced Specialty Training



Search: TRADOC Culture Center | 

<http://www.facebook.com/pages/TRADOC-Culture-Center/155051471239990>

Intelligence Challenges in Eastern Afghanistan



by Lieutenant Colonel Jim Reed, Major Ken Wright,
and Chief Warrant Officer Four (P) Erin O'Hara



Part 1 of 2. Part 2 will appear in the July-September 2015 issue.

Introduction

In February 2009 the 4th Brigade Combat Team (BCT), 25th Infantry Division (ID) deployed for a 12 month rotation from Fort Richardson, Alaska, to eastern Afghanistan as part of Regional Command East, International Security Assistance Force. The BCT's area of operations (AO) included the provinces of Khowst, Paktika, and Paktia, all of which bordered Pakistan. The brigade headquarters was at Forward Operating Base (FOB) Salerno in Khowst Province. With the addition of a Military Police battalion, a National Guard Infantry battalion, an Aviation battalion, Provincial Reconstruction Teams, and Agri-Business Development Teams, the BCT took on the designation of Task Force Yukon.

During its deployment the unit encountered a number of interesting intelligence challenges—leading up to and during the deployment—which might serve as lessons learned and best practices for other intelligence professionals. The purpose of this article is to capture and share these experiences, so that others may use them to improve unit SOPs and overall unit effectiveness. While some issues presented here are useful only to Counterinsurgency (COIN) or Wide Area Security operations, many also have applicability to Combined Arms Maneuver missions.

Challenge #1—Only Six Months to Train Before the Unit Deploys. The biggest pre-deployment challenge we faced was time to train for the upcoming Operation Enduring Freedom deployment. The unit had returned from an Operation Iraqi Freedom rotation in December 2007. This

rotation, part of the Iraq War troop surge of 2007, had been 15 months in duration. During the summer of 2008 there was a turnover rate of approximately 50 percent of the intelligence personnel within the BCT. Soldiers who had been in the unit three or more years had departed and new personnel arrived. Almost the entire brigade staff changed out, with new officers arriving during June-September 2008.

During the summer of 2008, the BCT was notified it would deploy to Afghanistan in February 2009 for a 12 month rotation and that it would execute a rotation at the National Training Center (NTC) during November 2008. With the majority of new personnel not arriving until the end of July 2008, this left only three months to train before the NTC rotation (August-October) and six months before the unit deployed (August-January). Added to this lack of available training time was the requirement for all personnel to conduct quarterly airborne jumps and an Alaskan winter that made outdoor training very difficult during the November-January months.

Several things helped the unit to overcome this challenge. First, when the new brigade commander arrived in July, 2008 he immediately assessed that three months (August-October) was not enough time to properly train-up the BCT prior to its NTC rotation and issued orders that all leaders prioritize training for what was needed to succeed in Afghanistan. In other words, train for the deployment, not the NTC rotation.

Second, the G2 Section of our higher Headquarters, U.S. Army Alaska Command (USARAK), assisted us by taking

lead on the scheduling of intelligence mobile training teams (MTTs). Since there was no Foundry Training Site at Fort Richardson, the USARAK G2 Section, in coordination with the Brigade S2, focused on identifying MTTs (many from the Foundry catalog) which would most benefit the BCT, then scheduled nine to come to Fort Richardson between July 2008 and January 2009. The MTTs came from the National Ground Intelligence Center, ICoE/Fort Huachuca, the Defense Intelligence Agency, and TRADOC ISR TOPOFF. All were extremely important in getting the BCT's intelligence Soldiers trained and ready for Afghanistan.

Third, the decision was made to send all Signals Intelligence (SIGINT) platoon personnel to Hawaii to complete their pre-deployment training with the 500th MI Brigade instead of bringing them to the NTC rotation. The MI Company commander, Brigade Special Troops Battalion commander, and Brigade S2 were all in agreement when recommending to the Brigade Commander that the SIGINT Platoon go to Hawaii for 60 days of training. In Hawaii they received extensive SIGINT training, but by not going to the NTC they missed out on testing and honing the BCT's internal SIGINT collection, reporting, and analysis processes. This was a difficult decision, but the right thing to do given the circumstance of a looming Afghanistan deployment. We accepted risk that our SIGINTers would have to learn the tactical aspects of SIGINT collection once the unit deployed.

Challenge #2—Who to Turn to for Help? This can be a significant pre-deployment challenge for many units, especially those at remote installations such as Fort Richardson. The doctrinal answer should be for a unit to first approach its higher headquarters when looking for help. In this case, the 25th ID was unable to assist, as they were not our higher headquarters, USARAK was. In addition, the USARAK G2 did not have the large Analysis & Control Element normally found at a division. Rather, it had a small analytical cell (made up mostly of Army civilians) and a tiny Deployable Intelligence Support Element from the 205th MI Brigade. Additionally, the G2 was focused on maintaining situational awareness for the Alaska and Pacific regions, not Afghanistan. Bottom line, there was no single organization to turn to which could find solutions to difficult intelligence related questions. There was no one who could answer questions such as “Where do we get an SOP for Tactical Site Exploitation (TSE)?” or “How should we task organize our intelligence analysts to support high value individual (HVI) targeting?”

The solution of who to turn to for help came in the form of TRADOC's Asymmetric Warfare Group (AWG). Even before the BCT conducted its Pre-Deployment Site Survey to

Afghanistan, AWG personnel flew to Fort Richardson to spend several days briefing brigade and battalion leaders on how best to prepare for the upcoming deployment. They met with all interested leaders and answered all questions. In the case of the TSE SOP, they emailed one to the Brigade S2 within 48 hours. The AWG team's mission was to assist the BCT with all pre-deployment issues, and they were extremely helpful during the entire process. They also continued to provide assistance throughout the deployment. The AWG support was very impressive, in large part because they either provided immediate answers, or else wrote down questions and came back with answers within two or three days. This type of facilitation is crucial in today's complex and fast paced Army. Imagine if the MI Corps had its own version of AWG, albeit on a smaller scale—an organization that all G2s and S2s from across the Army could turn to for assistance?

Challenge #3—How to Create 19 HCTs? We were extremely lucky to have a Brigade Commander who was heading to Afghanistan for his third tour. Because of this, he knew exactly what he wanted when it came to battlefield Human Intelligence (HUMINT) collection. He wanted a 2-person HUMINT Collection Team (HCT) with every company that owned ground, so that each company commander had his own organic collection capability. He also wanted each HCT to operate as part of the company commander's Company Intelligence Support Team. He understood the fight in Afghanistan better than anyone, and explained that not only was it a decentralized company level fight, but that the role of the Brigade S2 Section was to ensure each company had a trained and capable HCT. The challenge was that with an estimated 19 battlespace owning companies, we would need 38 HUMINT Collectors. Given our 21-person HUMINT platoon, we would need more 35Ms.

Our solution was to use the MOS 92R Parachute Riggers from the brigade's Rigger Platoon as “HUMINT Assistants.” Since the unit did not plan to conduct airborne operations in Afghanistan, the entire Rigger Platoon would not be needed to do the limited amount of parachute rigging required to support periodic resupply drops. Using 92Rs was a highly unorthodox approach, but a practical solution. The Brigade S2X was given the mission of screening the records of all 92Rs, interviewing those with the best records, then selecting 19 from the platoon to serve as HUMINT Assistants.

The S2X then teamed each 92R with a 35M to form a 2-person HCT, attached each HCT to the company they would support during the upcoming Afghanistan rotation, and instituted a demanding training program to ensure each HCT was capable of executing its mission. MI Company

leadership were strong supporters of this approach and worked to educate the maneuver company commanders on how to properly utilize their HCT. The MI Company commander at the time, Captain Dave Beall, wrote an excellent article for the April-June 2009 issue of MIPB that outlines both the rationale for pushing HUMINT Collectors to the company level in a COIN fight and what it takes to make this approach successful.¹

Not surprisingly, the BCT encountered initial resistance during its NTC rotation. Due to the presence of non-HUMINT personnel (92Rs) working alongside 35Ms, several observers/controllers (O/Cs) initially refused to support the rotation. The S2X made it clear to the O/Cs that only 35Ms would be conducting Military Source Operations, and that the role of the HUMINT Assistant was to conduct analysis, Tactical Questioning (TQ) and TSE. Still, a handful of O/Cs continued to be unsupportive of this new approach and even threatened to have their chain of command pressure our BCT leadership to stop using 92Rs as HUMINT Assistants. It may have helped that this was the very first Afghanistan rotation at the NTC and the O/Cs were still a bit unfamiliar with OEF tactics, techniques, and procedures, or it may have been that our S2X folks were just very good at selling this newfangled concept of non-HUMINT personnel assisting 35Ms. In the end there was compromise, with the O/Cs agreeing to support.

During the Afghanistan rotation the decision to push 35Ms to the company level paid off. The BCT was able to provide HCT coverage over a far greater geographic area than the preceding BCT. Our higher unit, the Coalition Joint Task Force (CJTF), provided a CAT II Interpreter for each of the 19 HCTs. Employing company level HCTs also enabled the BCT to develop a larger number of human sources than would have been possible had the unit only employed HCTs at the battalion level. The quantity of daily HCT reporting coming out of the BCT was phenomenal. Most importantly, commanders at all levels—company, battalion, BCT, and CJTF—had good situational awareness of insurgent capabilities and intentions across the BCT's three provinces. However, based on personnel challenges, it was difficult to fully man all 19 HCTs during the deployment; the BCT was only able to maintain approximately 16 HCTs.

Challenge #4—Managing Biometrics Collection Operations. With the realization that Biometrics was playing an ever more crucial role in Afghanistan, we considered how to conduct effective collection operations across the extremely large AO the brigade would occupy in Afghanistan. There would be at least 19 FOBs or Combat Outposts (COPs), some of which would not have SIPR communications.

Biometric enrollments collected using portable Handheld Interagency Identity Detection Equipment devices were normally uploaded via SIPR to the Biometrics Automated Toolset (BAT) database. But how would we get the enrollments collected at remote COPs into the BAT database? The solution was what we called “Biometrics Digital LOGPAC”. Whenever a remote COP received a helicopter-delivered Logistic Package (LOGPAC), it would send a CD with its latest Biometrics enrollments to the battalion headquarters, so the S2 Section could upload the enrollments to the BAT database. In turn, the S2 Section was responsible for sending a CD with the download of the latest Biometrics watch list to each FOB/COP that did not have SIPR.

This “push” from the S2 sections took place daily during the NTC rotation, then weekly when in Afghanistan. This process worked well while at the NTC, but began to break down while in Afghanistan. The system depended on battalion S2s being proactive enough to keep the process rolling, regardless of all the demands involved in supporting daily combat operations. The solution was two-fold. First, the Brigade S3 published an order (endorsed by the Commander and written by the S2) directing that each battalion collect a minimum number of new enrollments per week (typically 150 per week). Second, the Brigade S2 began briefing the Brigade Commander on how many new enrollments the battalions had collected over the past week, as well as their total number of enrollments since the deployment began. The result was an increase in enrollments, as none wanted to be the battalion with the least amount of enrollments for the week.

Challenge #5—ISR Asset Integration. “Intelligence, surveillance, and reconnaissance (ISR) integration” is more than just integrating ISR assets into the unit's Collection Plan. It also includes integrating newly arriving MI units/assets into the BCT's task organization. Unless an asset has extremely long legs, such as Reaper Unmanned Aircraft System (UAS), it will be collocated with your unit; in other words, stationed within the BCT's AO. Often times there will be an airfield within the BCT's AO (expect the BCT HQ to be located there) which is where many of the aerial ISR assets will be stationed. During a real-world deployment, additional ISR assets will be allocated to the BCT, and while the brigade Collection Manager will normally be aware of inbound assets flowing into Theater (MI Force Flow), some intelligence units/assets will simply arrive at the unit unannounced. Regardless, upon their arrival, the Brigade S2 should recommend to the Brigade S3 the command relationship for the newly arrived unit/asset (Assigned, Attached, OPCON, TACON) and to which unit within the BCT.

Once the Brigade S3 makes a decision, the S3 Section adds the newly arrived unit/asset to the BCT's task organization (typically a PPT slide). The final step is for the S3 Section to publish a short statement in the next daily FRAGO that lists the command relationship of this newly arrived unit/asset along with an updated task organization slide. The Brigade S2 should be prepared to walk the S3 Section through this process, so that newly arrived units/assets are properly integrated into the BCT. For instance, a newly arrived Counterintelligence (CI) Team might be assigned to the brigade's Headquarters, Headquarters Company, so it is collocated with the Brigade CI Agent. On the other hand, a newly arrived Multifunctional Team might be assigned to the MI Company or attached to a maneuver battalion.

Challenge #6—Collection Management. Being a Collection Manager (CM) is not easy, as one must be an excellent planner, salesman, and teacher. The first challenge for a CM is to be a planner; specifically, to out-plan higher, lower, and adjacent units by determining collection requirements weeks or months in advance. Only by doing so is the BCT able to secure a commitment from higher to provide the external collection assets it needs to successfully execute its mission. This requires the CM to know more about adjacent unit future operations than anyone else in the entire BCT. Through this knowledge our CM was able to anticipate adjacent unit collection requirements and beat them to the punch by submitting requests for collection requirements before they did. This required having requests for ISR collection capabilities submitted to higher (CJTF) at least one month in advance. Requests had to show that: the BCT was fully supporting CJTF Commander collection priorities, and that the BCT was utilizing all of its organic assets.

Our CM was often able to get assets that adjacent BCTs could not get, because he figured out how to write our Collection Plan in such a way as to directly support the CJTF's top collection priorities. This is the art of the salesman. When our BCT collection requests clearly showed the linkage between BCT ground operations and the CJTF's top two collection priorities, we almost always got the asset/capability we were requesting. However, this required continuous, proactive engagement by the CM with battalion S2s and S3s to pull information from them about future platoon, company, or battalion level operations (task, purpose, where, for how many days, etc.), in order to submit the BCT's collection requests at least 30 days in advance. After this, the CM became the teacher, working with battalion S2s to help them determine their intelligence gaps and the ISR capabilities they could reasonably expect to receive to support these future operations. This took place prior to a bat-

talion staff conducting its Concept of Operation (CONOP) brief to the Brigade Commander, which typically happened one week before the start of an operation.

Electronic Warfare (EW) was another important consideration for the CM. The CM had to be aware of all EW missions planned to take place in or near the BCT's AO, as EW has the potential to interfere with certain ISR collection operations. Detailed knowledge of exactly when, where, and what type mission would take place (Electronic Attack or Electronic Support) allowed the CM to either employ an ISR asset which would be unaffected by EW, or at least minimize ISR asset downtime while the EW mission took place. It took effort for the CM to develop a written, synchronized plan that tracked EW missions, but it was worth the effort. An added benefit of having a written plan is that it can be used to defend the BCT in arguments with adjacent and higher CMs. Whenever our BCT was accused of causing EW interference with adjacent unit operations we were vindicated after referring them to our CJTF approved CONOP documenting our unit's approval to conduct the mission. The CM also had to be knowledgeable about adjacent unit EW operations, as operations taking place in an adjacent AO could have a negative impacted on operations in our AO.

Modern ground combat involves General Purpose Forces units sharing battlespace with Special Operations Forces (SOF). Coordination with SOF was an important function for the CM. Initial coordination efforts began with our BCT CM telling the SOF unit CM what ISR collections our BCT had planned. The SOF CM would then indicate if they (SOF) might be doing some activity that could potentially interfere. As the SOF planning window is typically no more than 72 hours out, this coordination had to be conducted daily. Even so, a CM must be prepared to hear that a SOF mission takes priority, and that the BCT's ISR asset must be moved to an area that will not interfere with execution of a SOF mission, whatever it may be. However, when this becomes excessive to the point of affecting multiple BCT operations, the higher CM should be notified. Only after our higher CJTF CM turned-away multiple SOF collection assets from our BCT battlespace did the SOF CM begin making a real effort to share information regarding SOF assets operating in our AO. As the relationship improved, we were even able to share ISR assets, which allowed the BCT to gain information on specific HVIs operating within our AO that SOF were attempting to target, HVIs we otherwise would not have known about.

Lastly, a CM must understand the limitations of the BCT's organic ISR assets. Armed with this knowledge, they are better able to argue the requirement (the need) for exter-

nal CJTF-provided ISR capabilities. For instance, use of the Shadow UAS in the high mountainous terrain of eastern Afghanistan was challenging. High winds impacted Shadow operations, as did extreme cold temperatures. There were times when cold weather prevented the Shadow from flying, due to the potential for wing icing. Engine failures in extreme cold weather were also a problem, although an improved engine has now been installed on the Shadow which greatly corrects this deficiency.

Another issue when flying in mountainous regions was that Shadow was unable to fly high enough to not be heard from the ground. Full Motion Video often showed individuals looking up at the Shadow. Improved engines and larger (extended) wings have now largely addressed this problem. If our CM hoped to get CJTF to give us the ISR assets we needed for an upcoming operation, especially one conducted in mountainous terrain, Shadow needed to be included on the Collection Plan, if only to make clear the reasons why it could “not” satisfy the collection requirement. Depicting Shadow and also listing its limitations on the Collection Plan (why it could not satisfy the require-

ment) helped our higher CM to understand its limitations, and often led to CJTF allocating us the ISR capabilities we needed. ✨

Endnotes

1. Captain David Beall, “The HUMINT Heresies: The Disposition of Human Intelligence Collection in Counterinsurgency,” *MIPB*, Apr Jun 2009, 32-37.

LTC Jim Reed served as Brigade S2 for 4/25 IBCT during 2008-2010. He is currently the XO of the Training Development and Support Directorate at Fort Huachuca, Arizona. Other assignments include G2 Operations Chief at ARSOUTH, BDE S2 for the 18th MP BDE, 11th ACR Assistant Regiment S2, and 96th CA BN S2 and HHC Commander.

MAJ Ken Wright served as Brigade Collection Manager for 4/25 IBCT during 2008-2010. He is currently the XO of TRADOC Capability Manager-Biometrics and Forensics at Fort Huachuca. Other assignments include Senior Intelligence Advisor to Saudi Arabia MoD and Battalion S2.

CW4(P) Erin O’Hara served as Fusion Cell Chief for 4/25 IBCT during 2009-2010. She is currently a Senior Doctrine Writer at Fort Huachuca. Other assignments include Senior Analyst at USARAK, Special Operations Intelligence LNO, Knowledge Manager for ARSOUTH G2, and Production Chief for CJTF-7 and V Corps.

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.





Use of SIMEX Can Maximize Training Opportunities for MI Soldiers



by Major James Welch and Chief Warrant Officer Two Kirk McKenney



Introduction

Simulation exercises (SIMEX) offer incredible opportunities and training value for Military Intelligence (MI) Soldiers. During field exercises, maneuver units give combat arms Soldiers ample planning, time, and resources to adequately train military occupational specialty (MOS) specific skills. However, during these same training exercises, time and/or resources are not always allocated towards training MI Soldiers in their MOS specific skills.

Therefore, leaders must also ensure that MI Soldiers are properly trained and prepared for whatever role they may be called upon to perform during the course of any mission. While an in-depth study of probable threats and an understanding of the operational environment are essential, it is imperative that leaders also train MI Soldiers to be able to put this knowledge into practice. Leveraging the use of SIMEX gives tactical leaders within the intelligence community an opportunity to overcome training limitations and sharpen critical skills.

Background

From February 2014 through February 2015, the 3rd Armored Brigade Combat Team (ABCT), 3rd Infantry Division, was assigned as the Northern Command (NORTHCOM) Regionally Aligned Force (RAF). As the NORTHCOM RAF, 3 ABCT was prepared to support missions within the continental U.S., as well as Theater Security Cooperation missions with Canada and Mexico. Prior to assuming the mission, it was imperative that MI Soldiers understood their role in defense support of civilian authorities (DSCA) missions, while also understanding the importance of intelligence oversight regulations during these operations. In an effort to emphasize the importance of this training, the unit

conducted a SIMEX in the Clarke Simulation Center at Fort Benning, Georgia. This exercise was designed to serve as a capstone training event prior to assuming the RAF mission and help mitigate any gaps in knowledge and experience of the brigade's MI personnel with regards to the intricacies of the NORTHCOM area of responsibility.

The Brigade S2 section worked with the Center staff to create a four day SIMEX specifically designed to train MI Soldiers in both homeland security and DSCA environments. The scenarios were brought to life using Virtual Battle Space 2 (VBS2) technology. VBS2 is designed to place a Soldier in a virtual world that mimics the terrain of a target area and provides situations that may be difficult to recreate in a traditional training exercise. The full scope of the exercise was broken down into four phases, discussed below:

Phase I, Preparation. The preparation phase consisted of concept and scenario development. Several in-progress reviews (IPR) were conducted in the months and weeks leading up to the exercise in order to discuss how the scenario would be carried out, which personnel would be tested, the footprint at the simulation center, training objectives, and the desired endstate. Concurrently with the IPRs, historical data was developed by Brigade S2 and MI Company personnel in order to present background information leading up to the scenario. Scenarios, target packets, and characters were created to give depth and realism to the scenario.

This detailed information provided the Soldiers with the ability to conduct Intelligence Preparation of the Battlefield as soon as the scenario began. The development of the scenario was a daunting task and required brigade personnel to work side by side with the simulation center personnel several days a week. Because the simulation center had not

created a scenario like this before, almost every aspect of the scenario had to be created from scratch.

Phase II, Script Development. The second phase of the operation transformed the concept into a script for the exercise. This script laid out the story, as well as how and when injects would be introduced. It was important to monitor how each element was progressing through the script so that each inject was launched at the correct time. If an inject was presented too early, the information may have been lost in a current task, or if too late, the element would be inactive for an extended period of time. Being dormant would lessen the intended stress on the Soldiers. To mitigate this issue, decision points were established so injects would appear precisely at the correct time.

Injects consisted of simulated videos within the VBS2 system, live actors, and message traffic between participating units. All injects produced information or issues to force the Soldiers to react in some fashion. Some injects would inform the Soldiers of something that was happening in the operational area, while others would cause the Soldiers to reassess a situation producing either a course change or to confirm their current azimuth. The live actors portrayed roles of various agencies the Soldiers might encounter if engaged in a DSCA mission. This presented a great opportunity to teach the Soldiers how to communicate and coordinate with civilian organizations. The actors portrayed the role of various organizations such as law enforcement, civilian agencies, and first responders.

These use of injects and the collaboration with civilian entities were deliberate schemes meant to prepare Soldiers for DSCA operations. In most cases, they reiterated to Soldiers that civilian entities are in charge during these types of operations. Soldiers deployed for a DSCA mission are in a support role and this was to be stressed throughout the SIMEX.

Phase III, Refresher Training. The third phase of the operation took place during the two weeks leading up to the exercise. During this phase, Soldiers participating in the exercise were provided with refresher training on the systems they would be using during the duration of the SIMEX, including Command Post of the Future and Blue Force Tracker, in order to simulate a real world environment. These systems were the primary means of communication used throughout the exercise. Additionally, Soldiers received instruction on the VBS2 system, learning about the controls to manipulate the angle of cameras and the communication program integrated in the system.

In addition, this time period was used to familiarize the exercise observer/controller (O/C) teams that would be grad-

ing the participating units. The O/Cs were broken down by battalion and were instructed to grade both the Battalion S2 section and their respective company intelligence support teams (COISTs). For this reason, it was critical that each O/C had a thorough understanding of the SIMEX scenario, as well as an understanding of DSCA and intelligence oversight regulations. To assist in this effort, ARNORTH representatives reviewed the scenario material and provided feedback to the SIMEX administrator. ARNORTH personnel were also on hand prior to, and during the SIMEX, in order to provide subject matter expertise and help O/Cs in their efforts to mentor and train participating Soldiers.



3rd BDE ColST Teams used CPoF and FBCB2 to conduct IPB and maintain C2 awareness of their assigned AO which was constructed inside a Virtual Battlespace2.

Phase IV, Execution. The final phase of the operation began with the execution of the exercise. The unit was notionally deployed to the area of operations in accordance with the scenario. A mission brief was given laying out the situation, an operation order with annexes was provided, and all historic data was distributed to each unit. Up until this point, the Soldiers had not been briefed about any aspect of the exercise. Each COIST was separated from its Battalion S2 and worked almost side by side to their sister COISTs from the same battalion. This helped achieve the effect of being separated geographically. Although, there was limited space in the facility, it worked in favor of the O/Cs, allowing them to have better command and control throughout the exercise and readily observe the actions of Soldiers.

In the end, the DSCA SIMEX achieved our desired endstate, ensuring that all MI Soldiers within 3 ABCT had a thorough understanding of our NORTHCOM RAF mission. In addition to understanding the role that Soldiers play in a DSCA environment, Soldiers became well versed in intelligence oversight issues that they might encounter during the course of DSCA missions. The utility of SIMEX extends beyond preparation for operational assignments such as deployments or RAF missions. Units can also use these types of exercises to prepare for other missions or training events.

Simulations to Prepare for CTC Rotations

During the course of our Brigade's RAF mission, our unit was notified that we would be taking part in a rotation at

the National Training Center (NTC). With limited preparation time, there would be few opportunities to adequately prepare MI Soldiers for the upcoming rotation. To compound this issue, the vast majority of MI Soldiers had no experience with NTC nor did they fully understand the idiosyncrasies of the hybrid threat to be faced during our rotation. Once again, the use of a SIMEX offered our team the best opportunity to overcome training deficiencies and limitations.

While our previous SIMEX required our team to create a scenario and work with the simulation center staff to bring the exercise to life, the majority of preparation for this exercise could be completed solely by the simulation center staff. Once we decided upon a specific geographical area and the array of our forces, the simulation center staff was able to construct the simulation with relative ease.

Unlike the DSCA SIMEX, we did not train Soldiers from Battalion S2 sections or COISTs during the NTC SIMEX. Rather, we used this opportunity to train analysts from the Brigade MI Company and the Brigade S2 section. In addition to establishing a better working relationship between these two entities, the exercise introduced Soldiers to the NTC terrain and landmarks that are often referenced in after action reviews. The exercise was broken down into two phases, with our forces serving in a defensive role for two days, followed by the offense for two days. Throughout the course of this exercise, simulation center staff used a computer program to auto-generate significant activities reports and other information. Although much smaller in scope and size than the DSCA SIMEX, the NTC event proved its worth and further validated the use of SIMEX to train MI Soldiers. The event increased cohesion between the Company and the Brigade S2 section, helped validate internal standard operating procedures, and increased the knowledge base of Soldiers.



3rd BDE S2 and MICO Sections used CPoF and FBCB2 to conduct Intelligence IPB and maintain situational awareness.

Lessons Learned, the Way Forward

As valuable as the training exercise was in preparing MI Soldiers for future missions, it will never take the place of conducting exercises in a field environment. The Soldiers were able to concentrate solely on the mission at hand, but

did not face the obstacles that a field environment often produces. While in the field, Soldiers must overcome the unfamiliar environment, lack of sleep, and additional requirements such as set up and tear down of equipment. Additionally, sitting in a climate controlled work environment and having the adjacent units nearby removes elements of reality they would face in a more traditional exercise. Some notional situations had to be explained in advance to prevent questions later.

Despite the incredible return on investment, units using SIMEX must go to great lengths in order to ensure the event occurs seamlessly. In the case of our DSCA SIMEX, there were some glitches in the VBS2 system and the scenario execution. Simulation center personnel worked extremely hard when it came to technical issues, but the scenario sometimes needed to be paused or restarted. Having these restarts and pauses in the middle of the scenario halted momentum which detracted from the training. However, the professionalism and skills of the simulation center staff helped overcome these issues.

Looking ahead to future simulation training exercises, it is suggested that several dry runs should be conducted to make sure the scenario makes sense; O/Cs have a thorough understanding of the event timeline, and that there are no technical glitches that would halt the training unexpectedly. Therefore, continuous communication must be maintained, along with several checks on the progress throughout all the phases. When the exercise begins, it may be too late to change the scenario. Further, the exercise should be developed using existing simulation scenarios from the myriad of databases available. With a multitude of options for acquiring a wide array of scenarios, most units should not have to construct a scenario from scratch.

Conclusion

Using SIMEX, MI leaders have the ability to tailor simulations to mirror scenarios their units may face while supporting any number of possible missions. Simulations can also be used by MI leaders to train in preparation for rotations at the Army's combat training centers and for conventional overseas deployments. Since many tactical training events may focus on operational forces, SIMEX offers MI leaders a venue to hone the skills of their Soldiers and better support the commander. 

MAJ James W. Welch currently serves as the Brigade Intelligence Officer for 3rd ABCT, 3rd Infantry Division.

CW2 Kirk McKenney currently serves as the 3rd ABCT Brigade S2 HUMINT Technician.

Vigilant Pacific: 205th MI Battalion Enhances FVEY Partnership and Interoperability in the Pacific

by Captain Brian Vaeni



Introduction

From 3 through 16 November 2014, the 205th Military Intelligence (MI) Battalion (BN) hosted the 19th annual joint, “Five-Eyes” (FVEY) Counterintelligence (CI) and Human Intelligence (HUMINT) exercise, VIGILANT PACIFIC at Bellows Air Force Station in Hawaii. VIGILANT PACIFIC has long been the premier CI and HUMINT exercise in the Pacific and is unique for its FVEY construct. However, this most recent iteration made substantial leaps forward in refining and testing a growing body of multinational, and joint doctrine and establishing an integrated intelligence sharing architecture. Additionally, the exercise furthered the deep and historical friendship amongst the FVEY partners.

The output of these efforts is a burgeoning multinational intelligence enterprise in the Pacific that is highly interoperable and able to meet the partnership demands of Army and Joint doctrine and future force concepts. After operating side-by-side for more than a decade in Iraq and Afghanistan, exercises like VIGILANT PACIFIC help maintain post-operational momentum by reaffirming our partnerships and the need for interoperability in our own area of responsibility.

The aim of VIGILANT PACIFIC nests with Army and Joint principles for multinational operations expressed in recent conceptual documents such as the *Capstone Concept for Joint Operations: Joint Force 2020* and *The U.S. Army Operating Concept: Win in a Complex World*, the latter of which was published just days before last year’s exercise began. According to the Army Operating Concept (AOC), the future Army force will “engage regionally to ensure interoperability,

build relationships based on common interests, enhance situational awareness, assure partners, and deter adversaries.”¹ The AOC itself nests within the Joint Force’s *Capstone Concept for Joint Operations (CCJO)*, specifically within the concept of “globally integrated operations.” The CCJO lists partnering as one of the eight key components of globally integrated operations and describes how the joint force must identify partners with whom they will most often work and develop standards for interoperability.² Partnering is essential because it provides enhanced capacity by combining assets, increases situational awareness through intelligence sharing and enhances capabilities with regional expertise.

One of the most tangible ways in which VIGILANT PACIFIC enhances joint and multinational interoperability is through the refinement of a Combined Joint CI and HUMINT Staff (CJ2X) Manual. This manual codifies the structure and processes of the combined, joint 2X staff. Many authors from different services of all the FVEY partners contributed to the document throughout the history of VIGPAC. Each year, the exercise steering committee determines which aspect of the manual to focus on for validation and builds the field training exercise (FTX) around those targeted training objectives. This year the FTX made significant strides in validating management processes at the CJ2X and Operational Management Team levels.

In addition to exercising staff roles, the FTX engaged CI and HUMINT teams in a collaborative manner by building teams comprised of multinational partners. This forced teams to share best practices and develop standard operating proce-

dures at the tactical level. Combining teams presented certain challenges, one of the foremost of which was sharing tactics, techniques and procedures (TTPs) within the limits of FVEY releasable doctrine. One way the exercise planners helped overcome this challenge was by requiring capabilities briefings from each country that had been cleared for release by foreign disclosure officers at the outset of the exercise. This ensured participants had a base line understanding of how each other trains and operates along with the parameters for sharing TTPs.

VIGILANT PACIFIC 2014 also showcased a significant step forward in FVEY intelligence sharing by unveiling the first-of-its-kind Distributed Common Ground System-Army (DCGS-A) FVEY Intelligence Fusion Server (IFS). The DCGS-A FVEY IFS became fully operational in September 2014, and analysts in Australia and Canada have been beta-testing the system since then. Presently, the DCGS-A FVEY IFS enables partners to conduct data searches and pulls from 13 sources of information. In the future, as DCGS-A capabilities become more widely available to FVEY partners, it will enable a larger degree of multinational intelligence federation. The federated intelligence enterprise in the Pacific expands analytical capacity by distributing the work load while simultaneously maximizing functional and regional expertise. The federated nature of the enterprise is enabled by integrated information systems and the expanding use of DCGS-A in the theater is working to satisfy a task set out in the CCJO to “create the information environment that will facilitate partner integration.”³

Although enhancing interoperability through doctrinal refinement and information technology integration was the focus of the FTX and DCGS-A demonstration, the exercise also encompassed many other activities that further solidified the bonds amongst the FVEY partners. Each morning a different country led the physical readiness training (PRT). The U.S. taught everyone the precise execution of preparation drills in accordance with FM 7-22, followed by some competitive team races. The Australians took advantage of VIGILANT PACIFIC’s picturesque location by leading beach PRT, consisting of relay races in the ocean and sand. There was also an organized sports day and leader professional development (LPD) tour of Pearl Harbor towards the end of the exercise.



Photo by SFC Joseph Hamilton, 205th MI Battalion

Members of each of the FVEY nations who participated in Exercise VIGILANT PACIFIC visited the USS Arizona during a Pearl Harbor LPD tour during the exercise’s cultural excursion day on 15 November 2014.

Sports day featured a cookout hosted by the Battalion’s family readiness groups and the Pearl Harbor tour provided important historical context to the partners’ shared security responsibilities in the Pacific. Additionally, the exercise happened to occur over Veterans Day (recognized as Remembrance Day by Australia, Canada, New Zealand and the U.K.), and the partners took the opportunity to gather for a solemn remembrance ceremony on Bellows Beach. The ceremony reminded the partners of the history of shared service and sacrifice made together by the FVEY partners in conflicts over the past century.

The informal interactions that occurred throughout VIGILANT PACIFIC through events like sports day, the remembrance ceremony, Pearl Harbor LPD and others are in fact an important component of multinational relationship building and even nest with joint doctrine. Joint Publication 3-0 contains considerations for *Phase 0-Shaping* that include conducting “actions (that) enhance bonds between potential multinational partners.”⁴ Through the activities associated with VIGILANT PACIFIC, the FVEY partners built valuable personal connections and a fostered a sense of shared history and destiny, strengthening our willingness and ability to work together in multinational operations.



Photo by SFC Joseph Hamilton, 205th MI Battalion

Participants in Exercise VIGILANT PACIFIC pause during a Remembrance Day Ceremony on 11 November 2014. The ceremony included reflections from representatives from each of the FVEY nations, a reading of the poem, “In Flanders Fields,” and a lei toss into the ocean.

Overall, VIGILANT PACIFIC 2014 succeeded in achieving the desired outcome of enhanced partnership and interoperability amongst the FVEY



Photo taken by 205th MI Battalion

Exercise VIGILANT PACIFIC participants pose for a group photo at Bellows Air Force Station, Hawaii, upon conclusion of the two-week exercise.

partners in CI and HUMINT operations and intelligence sharing. The FTX led to significant progress in validating the CJ2X Manual and truly tested combined operations at the CJ2X and OMT level. Meanwhile, the DSCG-A FVEY IFS demonstration showcased an important capability that will continue to grow and benefit the entire theater's intelligence enterprise for real world intelligence analysis. Future iterations of VIGILANT PACIFIC will see the final validation of the CJ2X manual with increasing operational applications, and exercises like TALISMAN SABRE offer the opportunity to further advance our analytical and system interoperability. 

Endnotes

1. TRADOC Pamphlet 525-3-1 *The U.S. Army Operating Concept: Win in a Complex World* (Fort Eustis, VA, 2014), 17.
2. Office of the Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020* (Washington D.C., 2012), 6.
3. Capstone Concept, 13.
4. JP 3-0, Joint Operations, 2011, xix.

CPT Brian Vaeni is the Company Commander for Charlie Company, 205th MI Battalion. He has served in variety of positions including an Infantry Reconnaissance Platoon Leader and Battalion S2, including one tour in Iraq (2009-2010). He holds a BA in Political Science and International Relations from Northeastern University.

The Army Publishing Directorate authenticated and released ATP 2-22.7, Geospatial Intelligence, dated 26 March 2015. ATP 2-22.7 provides doctrinal guidance concerning geospatial intelligence (GEOINT). It complements guidance provided in ATP 3-34.80, Geospatial Engineering. ATP 2-22.7 focuses on the fundamentals of GEOINT as well as specific tasks and techniques for performing GEOINT activities. The principal audience for ATP 2-22.7 is commanders, intelligence officers, engineer officers, staff planners, and GEOINT cells at brigades, divisions, corps, theater armies, and the Army Special Operations Command.

This manual supersedes TC 2-22.7 dated 18 February 2011.

This publication is available to Soldiers and Department of the Army Civilians at https://armypubs.us.army.mil/doctrine/DR_pubs/dr_c/pdf/atp2_22x7.pdf

Online Radicalization



Introduction

Undoubtedly, the rise of global *internet* connectivity ushered in a new era of *human* connectivity. International economic trade, diplomatic relations, entertainment and social interaction are just a few of the aspects of human life enhanced by the internet. Particularly, political, religious and social belief systems of all types now have the opportunity to influence and impact people in all corners of the globe. Such interconnectivity is invaluable for the advancement of cultural understanding and enrichment, but it comes with a dark side.

International radical groups also have the same tools of communication at their disposal, and are willing to use these tools to influence and motivate, or conversely, manipulate and coerce people from all walks of life into taking extremist and violent action. With the rise of global internet connectivity, radical groups of all types no longer need purely physical assets to recruit and influence individuals for their cause. Because of the far reaching capabilities of radical groups online, homegrown terrorism may be the greatest emerging threat to American national security.

This article is intended to present a framework for understanding online radicalization, some of its components, indicators and the threat that it poses to American national security. The discussion will not focus on one particular extremist group as the goals, processes and targets of online radicalization may extend across many ideologies and belief systems. Moreover, a further intent is that this will spur further dialogue within the counterintelligence community, forcing community members to have uncomfortable discussions about the real dangers posed by the internet. Indeed, there is disagreement among scholars as to what defines

and causes radicalization in general, leaving the door open for continued analysis and research.

Achieving Ideological Goals

Essential to success and longevity, radical groups achieve their ideological goals by gaining and keeping the attention of their targets. Once a radical group has a target's attention, the target must then be manipulated into acting at the will of the manipulator.¹ Such manipulation begins broadly through the use of media, a long time tactic of radical groups seeking to expand their recruiting base and instill fear in a given population. Radical groups understand that leaders in liberal democracies are unable to ignore press coverage and the subsequent effect press coverage has on public opinion.²

However, traditional media mediums like television and newspapers do not offer radical groups the greatest access to and means of instant communication and information updates. With the internet comes a unique opportunity for violent extremist groups to exercise more control over their message and audience, and such groups have embraced this opportunity with enthusiasm and vigor.³ Of importance, and unlike traditional forms of media, the internet allows extremist groups to conduct two-way communication with their audience, likely facilitating the flow of ideas, a sense of true membership on the part of new recruits and the opportunity for extremist leaders to task recruits over time. The targeted nation or population is left with no choice but to conduct an active counteroffensive to maintain the initiative.

Brigitte Nacos, who wrote in the mid-1990s on the use of the media by terrorist organizations, keyed in on the desire of terrorist organizations to ultimately shape not only pub-

lic perception within a target nation, but eventually foreign policy as well. Nacos references James Madison, specifically Madison's "contempt for the public's tendency to base political judgments and actions on passion rather than reason." She argues that as communications technology has developed, the public's *interest* in foreign affairs has increased, but the same cannot necessarily be said for the public's *understanding* of foreign affairs.⁴

As such, American political leaders are making increasingly complex and difficult foreign policy decisions based (at least partially) on the will of an ill-informed electorate. Arguably, this is what extremist groups want initially, forcing the target nation or population to make mistakes in foreign policy decisions and relationships. However, and understandably so, Nacos did not account for the rise of the internet and its use by extremist groups. Essentially, the manipulation of foreign policy through traditional media is an attack by radical groups from without. Perhaps then, targeting individuals for radicalization through the internet is the next step in the evolution of radical ideology, creating an attack on the target country from within.

Robyn Torok, in describing the process of online radicalization, draws from the work of historian and philosopher Michael Foucault, applying Foucault's analysis on the importance of institutions in forming and changing the psyche of human beings. In this context, some examples of institutions are schools, prisons and the internet.⁵ Torok asserts that traditional extremist institutions, such as training camps, are continuously targeted by national governments. As a result, such institutions are becoming less desirable for radical groups, forcing radical groups to turn elsewhere to recruit and train new members.⁶ The internet is an institution, one that has permeated our lives and reshaped the course of humanity. More importantly, especially to radical groups, the internet is an institution that knows no physical boundaries, requires fewer resources and can reach every corner of the globe.

The Process

The rapid expansion of extremist material online coincided with the meteoric rise of visual media online, namely internet sites such as YouTube. Drawing from the U.S. campaign in Iraq as an example, the use of video by terrorist and insurgent groups was key to the success of the media battle waged by these groups against American forces. Insurgents sought to portray themselves through video as fearless and superior, and conversely, portray the supposed weakness of western nations.⁷ YouTube began uploading videos to its site in 2005, and by May 2012, uploaded an average of 60 hours of video every minute.⁸ As YouTube's content ex-

panded, so did its audience. Naturally, extremist material began appearing on sites like YouTube as radical groups saw an opportunity to quickly and effectively spread their message to a large audience.

Radical groups create the message they wish to convey, and the means through which to convey that message. The next step is to develop the themes in which the message will be couched. Extremists never portray themselves as the aggressors online; rather, they attempt to persuade their audience that they are merely responding to and battling against an oppressive and aggressive government or culture. Extremist figures are depicted as heroes, and for those who have died for the cause, as martyrs.⁹ In this vein, the sense of unity offered by radical groups is designed to attract those looking for belonging and purpose. Extremists also attempt to bait their target country or culture into speaking out against the extremist cause, further adding to the alienation and frustration of the extremist, and further fueling the extremist's desire for violence.¹⁰

According to some scholars, Torok's focus on extremist narratives and online institutions is only part of the online radicalization equation. Drawing from the work of Salma Belaala, Cristina Archetti describes some of the influencing factors that help put individuals at risk for radicalization. Belaala's work, supported by Archetti's analysis, points to one's relationship with the local community as contributing to one's susceptibility to radicalization. Belaala writes specifically that:

"radicalisation is both an individual and collective process of identity construction that involves a social rupture in the relationship of the individual with his/her fellow citizens. The radicalized young people reject others on a cultural and political basis. They oppose their values and even develop antagonism towards their own families and local communities. They equally reject other cultural groups both locally and in the rest of society: Jews, Hindu, or moderate Muslims."¹¹

Archetti, in moving beyond the idea that the existence of extremist narratives is the sole catalyst for radicalization, further describes how the role that an individual's relationship with his or her environment plays a factor. According to Archetti, the mere existence of extremist content online does not guarantee that internet users will access this content, let alone embrace it. Rather, once viewed, individuals must then appropriate the extremist content through the "interpretive prism of the beliefs and worldview that result from the individual's constellation of relationships."¹² Essentially, the extremist narrative is combined with the individual narrative; an individual narrative comprised of personal beliefs, one's relationship with his or her environment and the individual's interpretation of the extremist message.

Whether online radicalization is caused by the strength of the extremist narrative, the disenfranchisement of young people, or a combination of both is a matter for further debate. Each case of online radicalization is different, with different motives and circumstances spurring an individual on to adopt an extremist ideology. From the extremist's perspective, the process of recruiting new individuals does not end with simply projecting the extremist message. Extremist recruiters actively roam the internet, seeking interested or capable potential recruits in online forums and issue-specific chat rooms, targeting young people specifically.¹³

However, active recruiting is not the only means by which new members are brought into the extremist fold. Revealing just how dynamic the online radicalization process really is, some potential recruits initiate contact with extremist organizations, advertising their willingness to assist extremist organizations. One such example is Ziyad Khalil, who in 1995, became a Muslim activist while enrolled at Columbia College in Missouri. During his time at Columbia College, Khalil began operating a website that supported Hamas and ultimately connected him with other radical actors. Al Qaeda later recruited Khalil, tasking him with the procurement of electronic communications and surveillance equipment within the U.S.¹⁴ Individuals like Khalil, who volunteer their service to extremist organizations, further the danger of online radicalizations. The means by and motivation through which individuals become radicalized online differ, making the entire process of online radicalization more difficult to conceptualize.

The Target for Recruitment

Extremist groups choose many different types of individuals to recruit, seeking young people in particular who are receptive to the extremist cause.¹⁵ Recruits radicalized online are also targeted based on the particular skills and talents that benefit the extremist organization. Khalil, discussed previously, serves as one such example. After offering his services, Al Qaeda recruited Khalil because of his proficiency in computer technology. With Khalil's story in mind, it is important to remember that not all extremist recruits become the so-called "lone wolf" attacker. Rather, recruits are placed in roles that best exploit their talents. Recruits radicalized online can be placed into leadership, operational or support roles, serving in positions that vary from intelligence gathering to financing and translating. In essence, the structure of an extremist organization may mimic that of a military organization, with online recruiting serving as an anonymous and effective means of filling the ranks.¹⁶ In addition to the extremist message and the socio-cultural factors that make individuals susceptible to recruitment, extremist groups will use talents and experience to entice

or manipulate individuals into pledging allegiance to the extremist cause.

Going beyond skills and talents of individuals, there are other characteristics that contribute to one's radicalization online. Of importance, the sheer amount of isolated, uninterrupted time that one spends immersed in extremist content online affects one's view of the acceptability of the content. As individuals spend more time interacting with others who are seemingly of like mind, discussion of committing violent acts becomes normalized acceptable behavior.¹⁷ The internet also creates the opportunity for personality-related role playing, allowing individuals to portray characteristics of themselves online that do not actually exist in reality.¹⁸

Over time, individuals realize the discrepancy between their real and online selves, causing personal pain and depression. Individuals will attempt to reconcile the differences between their real and online selves by living out the persona they have created online; that reconciliation manifesting itself in the form of violent acts or other actions loyal to the extremist cause.¹⁹ Such instances of isolation and image crafting represent social and emotional needs within an individual; needs that an individual may actively seek to fulfill through extremist means, or needs that may make an individual susceptible to extremist recruitment. The difference lies only in who initiates contact first; the individual or the extremist recruiter.

Zachary Chesser, an American-born convert to Islam who is now serving 25 years in prison for his connection to Islamic extremism, represents an intriguing case study in online radicalization. Chesser converted to Islam in the summer of 2008, and within two years, pled guilty to three felony charges, including attempting to provide material support to the terrorist group al-Shabaab.²⁰ Chesser not only represents how rapidly one may radicalize through online means, but also a combination of phenomena in which extremist views initially sparked his interest, *and* he later chose to act on them. Chesser initially converted to Islam while playing on a soccer team organized by a member of Hizb ut-Tahrir, an Islamist political organization. By the Fall of 2008, Chesser posted online material supporting jihadist activities to include acts of violence. After two years of posting extremist material online and activities including an unsuccessful attempt to travel to Somalia, authorities arrested him in 2010.²¹ After his conviction and subsequent incarceration, Chesser wrote several letters to the U.S. Senate Homeland Security and Governmental Affairs Committee explaining his motivations, actions and intentions.

According to his own testimony, Chesser's motivations stemmed from his initial conversion to Islam, and his sub-

sequent search to apply jihadist ideals to the world as he saw it. He saw jihad as an obligation; a mandatory extension of the religion in which he placed his faith. As such, the extremist material Chesser posted online, including blogs, videos and other media “tied things back to Islam rather than ‘revolution,’ ‘oppression,’ and ‘violations of international law.’”²² With this in mind, Chesser’s motivation extended beyond a simple desire for social connection or the cognitive dissonance caused by the realized divergence between the internet and reality. In Chesser’s case, his motivation came from a very real belief in the mandates of jihad, the evidence of which he clearly displayed in his desire to fight for the cause.

Chesser serves as yet another example of the complexity of online radicalization, particularly in understanding the type of individual typically targeted by extremist recruiters. Some individuals volunteer their services, and some are targeted because of their skills and experiences. Others are emotionally withdrawn and socially isolated, looking for a sense of belonging and purpose. More complicated yet, some individuals may exhibit a combination of all these characteristics.

The Way Ahead

Peter Neumann suggests a few methods that can be used by law enforcement and intelligence agencies alike to combat online radicalization. One such method involves building awareness in local communities, where local communities are taught and understand the concept of online radicalization and the associated warning signs.²³ He also suggests the concept of “countermessaging,” a form of information operations that is designed to counter the appeal of online extremism. Countermessaging uses the same media platforms of blogs, videos, social media and other forms of online communication. Ultimately, the intent of countermessaging is to mock, ridicule or somehow undermine the perceived legitimacy of the extremist message.²⁴ Of course, these methods only represent a small portion of the options available to counterintelligence elements, and are just the beginning of an effective campaign against online radicalization.

Conclusion

As the internet becomes an increasingly pervasive part of our lives, so too will the threat of online radicalization and subsequently, homegrown terrorism. Given the internet’s accessibility and the virtual anonymity that it offers, discovering instances of online radicalization will continue to be a challenge. However, the counterintelligence community must be prepared to handle this threat as extremists continue to find new ways to reach out to and recruit individu-

als. In general, the U.S. must remain steadfast in protecting the First Amendment rights of U.S. citizens while continuing to stay ahead of future terror plots. In light of the complexity of online radicalization and the subsequent adaptability of online extremists, the counterintelligence community must remain adaptable in defending against and ultimately stopping the threat. ✨

Endnotes

1. Brigitte Nacos, *Terrorism and the Media: From the Iran Hostage Crisis to the World Trade Center Bombing* (New York: Columbia University Press, 1994), 8.
2. *Ibid.*, 10.
3. Peter Neumann, “Options and Strategies for Countering Online Radicalization in the United States.” *Studies in Conflict and Terrorism* 36, (2013): 431-459, doi: 10.1080/1057610X.2013.784568.
4. Nacos, 18.
5. Robyn Torok, “Developing an Explanatory Model for the Process of Online Radicalization and Terrorism.” *Security Informatics* 2, no. 6 (2013). <http://www.security-informatics.com/content/2/1/6>.
6. Torok, 1.
7. Carol Winkler and Cori Dauber, *Visual Propaganda and Extremism in the Online Environment*, ed. Carol Winkler and Cori Dauber (U.S. Army War College Press, 2014), 2.
8. *Ibid.*, 5.
9. Torok, 3.
10. *Ibid.*, 4.
11. Cristina Archetti, *Understanding Terrorism in the Age of Global Media: A Communication Approach* (New York: Palgrave Macmillan, 2013), 106.
12. Archetti, 123.
13. Gabriel Weimann, “How Modern Terrorism Uses the Internet.” United States Institute of Peace, 2004. <http://www.usip.org>.
14. *Ibid.*, 8.
15. Weimann, 8.
16. Senior Counterintelligence Instructor in discussion with the author, 27 January 2015.
17. Neumann, 6.
18. *Ibid.*, 7.
19. *Ibid.*, 7.
20. Majority and Minority Staff Senate Committee on Homeland Security and Governmental Affairs, “Zachary Chesser: A Case Study in Online Islamist Radicalization and its Meaning for the Threat of Homegrown Terrorism”, February 2012. <https://www.hsdl.org/?view&did=701274>.
21. *Ibid.*, 9 and 10.
22. *Ibid.*, 41.
23. Neumann, 15.
24. Neumann, 17.



THE JOINT LANGUAGE UNIVERSITY



DEFENSE LANGUAGE INSTITUTE
FOREIGN LANGUAGE CENTER



Lessons Learned: Managing Linguists



A Collaborative Effort by Corporal Thomas Warden, Specialist Cameron Severts, Captain Matthieu Ruiz, Captain Lauren Nowak, Mr. James Marcil, Major Jonathan Beckmann, Major Timothy Hunt, and Lieutenant Colonel Jay Haley

Introduction

Language skills atrophy if not continually trained. Linguists face challenges such as deployments, rigorous battle rhythms and a resource-constrained environment. At times, it seems nearly impossible to maintain or improve linguist skills, and self-study is not enough. A linguist must have the same structured training in their Control Language (CLANG) as an infantryman does for rifle marksmanship or squad level tactics. Units with linguists must be proactive in maintaining and improving a linguist's abilities. Commands should understand the resources available and be creative in how they use these resources.

Part of this improvement includes an operational application of the linguist's CLANG, noncommissioned officer (NCO) mentorship, and dedicated training embedded within the training schedule. Mentorship needs to envelop institutional study; experience gained operationally, self-study, and practical immersions. Commanders must resource the training, NCOs ensure training is done to standard, mentors facilitate structured training, and individual Soldiers take personal responsibility for their studies.

In an intelligence battalion with a 24/7 mission at the National Security Agency/Central Security Service (NSA/CSS), the chain of command decides how they will push a 2/2 linguist to become a 3/3 or 4/4 linguist. The following is a list of lessons learned while developing 3/3 linguists:

- ◆ The responsibility for developing a linguist lies with an engaged commander, a functioning Command

Language Program (CLP), the mentorship and guidance of an NCO, and the individual Soldier.

- ◆ A commander needs a Command Language Mentorship Program that provides a structured environment for the linguist.
- ◆ A program must have the benefit of a thoroughly engaged CLP Manager (CLPM) at the battalion level.
- ◆ The overall goal is to produce competent, confident Soldiers capable of utilizing their language in support of operations.
- ◆ Culture creates context for the language. It is difficult to maintain or excel in a language without cultural knowledge or cultural interest.
- ◆ Language learning cannot be attained with brute force. Speaking the language has an added benefit of helping a linguist think in their CLANG.
- ◆ There are more resources available than most commands realize.
- ◆ Collegiate level English vocabulary and grammar skills are sometimes the difference between a 2/2 and a 3/3 linguist.
- ◆ Commands should be open to the possibility of attaching a Soldier to other units executing recurring military exercises with partner nations. Additionally, the Army as a whole should consider a rotation that affords linguists multiple opportunities during their careers to be stationed at bases where units execute military exercises with partner nations.

Linguist Training—Not Solely DLI

Training begins in Monterey, California at the Defense Language Institute (DLI). DLI structures training for a Service Member who has no knowledge of the CLANG and strives to train service members to pass the Defense Language Proficiency Test (DLPT) with a 2/2 or higher. The training is rigorous—the work and schedule are on par with leading universities. Daily, the linguist completes 8 hours of classroom study, followed by two hours of study hall, and assigned homework which includes memorization of an extensive vocabulary list. DLI supplements the study with a barrage of tests (Defense Language Institute). Upon completion of DLI, Soldiers begin Advance Individual Training (AIT). AIT trains Soldiers to use their language operationally, and upon completion of AIT, Soldiers must maintain proficiency in their CLANG (DA Pam 611-21).

Responsibilities—Engaged Commander, CLPM, Linguist, NCO

There is a shared responsibility for each linguist to maintain proficiency in their CLANG. Soldiers have a personal responsibility, NCOs are responsible for sharing their institutional knowledge by teaching, coaching and mentoring linguists, commanders are responsible for facilitating training, providing resources and enforcing disciplinary standards, and CLPMs are responsible for managing language resources.

The role of a mentor is vital. Mentors act as an advocate for the linguists to the chain of command. They effectively map out an appropriate course of study, provide motivation, track progress, and readjust a linguist's training to improve weaknesses.

A command team's role is to be the honest broker. The unfortunate reality is not every DLI trained linguist is proficient enough to maintain their language skills outside of the school environment. According to MILPER Message Number 14-083, Soldiers sub-proficient in their CLANG will have an immediate reenlistment prohibition, are not eligible for promotion, and can be separated or reclassified. Additionally, commanders must address current language proficiency scores on the NCO evaluation report. Although there are some exceptions, the standard is clear. Keeping a sub-proficient linguist does nothing to help the Army or the Soldier. Commands must give their linguists every opportunity to succeed, and then honestly assess the retainability of the Soldier with deference to the Soldier's overall performance.

Command Language Mentor Program

The program the 717th Military Intelligence Battalion utilizes has the benefit of a thoroughly engaged CLPM at the

battalion level. The CLPM manages the funds required to provide Soldiers with opportunities for CONUS or OCONUS language immersions and other language training. The CLPM also publishes the current and subsequent fiscal year's language training based on the training available, and works in conjunction with the brigade headquarters and the NSA/CSS Associate Directorate of Education and Training. The CLPM at the battalion level provides companies with the resources; however, a company-level CLPM is necessary to manage the commander's program. The CLPM should be an NCO highly proficient in their CLANG and show the qualities of a professional Soldier. Proper management of the Command Language Mentorship Program is key to the program's success and will pay dividends for every linguist in any language.

Daily Mission

The overall goal is to produce competent, confident Soldiers capable of utilizing their language within operations. Slang and colloquialisms can make even the best linguists second guess their abilities. Experienced language mentors offer insight into the target language that a classroom or self-study guide cannot provide. Focusing solely on passing the DLPT will only improve the linguist's DLPT score. The DLPT is intended to assess the general language proficiency on a foreign language and is meant to examine how well a Soldier will fare in real-life situations. A 2/2 linguist shows an advanced level of proficiency; however, linguists need to strive for superior proficiency. Most linguists will work, at some time or another, in a mission for NSA/CSS. In this capacity, it is paramount the Army provide the NSA with superior linguists who are experts in their field. It is the opinion of some senior leaders that the Army is behind other military services when it comes to providing superior linguists. The lack of a large pool of high caliber linguists is understandable given the last decade of conflict the Army has endured.

However, as deployments decline, commanders should refocus their attention on their language program. This attention cannot afford to be myopic in scope and must cover the spectrum of resources available to linguists. In a battalion with different mission sets requiring different languages, Soldiers are afforded the added benefit of having the opportunity to work with their CLANG on a daily basis. On the occasion a linguist does not understand something, there will be time to sit and decipher the problem or work with someone who may be more proficient in the language. The Army and the intelligence community does not need mediocre linguists but experts.

Education in Culture and History

In order for linguists to excel in their language, they would benefit from a genuine interest in the culture of that language (ACTFL). Examples of significant cultural connections are family, the arts, or history (Peterson and Coltrane). Finding the connection for a linguist can be difficult. In a resource constrained environment, the command must identify Soldiers who not only show aptitude, but also a desire to excel. Once identified, the command should seriously consider sending three to five Soldiers on an immersion. Upon return, these Soldiers have an “ink-blot” effect on the rest of the linguists. Their improved language skills and heightened cultural awareness are infectious to the rest of the linguists and instill in them a desire to improve and to earn the opportunity to later attend an immersion.

If an OCONUS immersion is not possible, there are CONUS immersions available. For example, Serbo-Croatian linguists could attend a CONUS immersion program where they will spend 18 days speaking the language with native speakers all day. These opportunities are temporary duty assignments and provide the linguist a cost-effective opportunity to disconnect from the daily tasks of the unit and focus solely on improving the CLANG.

Speaking the Language

Speaking the language has an added benefit of helping a linguist think in his CLANG. Thinking in a different language is an acquired ability that provides additional exercise to improve their proficiency (Jackson and Malone). This exercise may be accomplished by giving a group of linguists the opportunity to come together and hold an event in which they only speak in their CLANG. Events such as dinners or pot-lucks, a movie night, a game night, or participating in a training event in the CLANG can be sanctioned by the command and added to the training calendar. A 2/2 linguist may be forced out of his comfort zone, and start to build and reinforce his language skills.

Other Resources

In units in close proximity to external resource centers, commanders can send Soldiers to five week refresher courses before their DLPT. This training gives the linguist structured, focused training and improves their confidence before the DLPT. However, self-study is sometimes the only option. Linguists have access to dictionaries, flashcards or Rapid Rote’s flashcard phone application, electronic language applications, music, games, Rosetta Stone, the Joint Language University (JLU), and the Global Language Online Support System (GLOSS).

English Class

One thing many linguists do not realize is that if they are not proficient in English they are unlikely to achieve a 3/3 in their CLANG. Although there are exceptions, English classes can be just as important in improving a foreign language as classes in the CLANG. English is the basic foundation to learning a foreign language. If a linguist has poor English skills, it is as if the foundation is set on sand (MLA). Graduate level English skills are what will help foster a 3/3 in the CLANG. A brigade-level CLPM can sometimes contract an English teacher if this need is identified. However, Army Education centers provide English lessons for free if the classes are remedial and not for credit hours. Additionally, Soldiers can attend SEFLA (Spanish English Foreign Languages of America) if they are limited in their English, even if English is their native language. This could be applicable to Soldiers who are raised in the U.S., but their parents are immigrants and speak their native language inside the home. A Soldier can also attend GRE or GMAT improvement classes at a reduced cost through the Army. These exams will ultimately serve to improve linguists confidence and aptitude in their CLANG.

Attach to Another Unit

Commands should be open to the possibility of attaching a Soldier to another unit executing recurring military exercises with partner nations. Furthermore, the Army, as a whole, should consider a rotation that affords linguists multiple opportunities within their careers to be stationed at bases where regionally aligned forces execute military exercises with partner nations. In cases where the command is unable to immediately and directly effect the latter, they should facilitate programs that allow linguists to participate in exercises such as Red Flag, Tiger Meet, Cobra Gold, and the Exercício Cruzeiro do Sul (CRUZEX). Such opportunities are invaluable to a linguist to not only improve language ability and how well they deal with real-life situations, but they also improve their understanding of the military jargon of their CLANG.

These opportunities would also provide an avenue of fostering the cultural connection often required to make a career linguist passionate about his CLANG (Jackson and Malone). In any case, any Army spouse would say that learning the military jargon of their service member is confusing, and it seems as if the Army has an acronym for everything. The same applies for the militaries of other nations. An understanding of military jargon would be a valuable asset, and would pay dividends within the intelligence community when understanding the military capabilities of nations around the globe.

Summary

A superior linguist is the product of an engaged commander, functioning CLPM, experienced noncommissioned officers, and individual discipline. Cultural awareness of the language, resource management, and some creativity help to develop a competent and confident linguist. Units need a mentorship program that provides structured and thoughtful training for the linguists with the goal of a superior linguist that can use their skills operationally. ✨

References Cited

National Standards in Foreign Language Education Project (1996). Standards for Foreign Language Learning: Preparing for the 21st Century. Lawrence, KS: Allen Press. At https://www.actfl.org/sites/default/files/pdfs/public/StandardsforFLLexecsumm_rev.pdf.

Defense Language Institute at <http://www.dlilfc.edu/about.html>.

Peterson, Elizabeth Peterson and Bronwyn Coltrane. "Culture in Second Language Teaching." EDO-FL-03-09 (December 2003). At https://media.startalk.umd.edu/workshops/2009/SeattlePS/sites/default/files/files/CAL_%20Digests_%20Culture%20in%20Second%20Language%20Teaching.pdf.

Jackson, Frederick H. and Margaret E. Malone. "Building the Foreign Language Capacity We Need: Toward a Comprehensive Strategy for a National Language Framework" (2009). At <http://www.nflc.umd.edu/pubcatalog#.VRCWcl7whdd>.

Modern Language Association. Foreign Languages and Higher Education: New Structures for a Changed World (2007). At <http://www.mla.org/fireport>.

DA Pam 611-21 The Enlisted MOS Smartbook (2004).

CPL Warden is a Cryptologic Language Analyst assigned to B CO, 717th MI BN. He attended school at Southern Oregon University and is a graduate of the Defense Language Institute in Monterey.

SPC Severts is the A CO, 717th MI BN Serbian/Croatian language mentor and is the company's alternate CLPM. He is also the 2014 INSCOM Linguist of the Year. He holds a BA in Latin-American studies from Brigham Young University.

CPT Ruiz recently relinquished command of B CO, 717th MI BN. His previous assignments include S4 of the 14th MI BN, and NSA/CSS Texas Watch Officer. He is currently assigned to the 201st MI BN as an Assistant S3.

CPT Nowak is the Commander, A CO, 717th MI BN. Previous assignments include Commander, HHD, 14th MI BN, and Assistant S3 470th MI BDE. She received a BS in French with a minor in Spanish from the U.S. Military Academy.

Mr. Marcil is the 717th MI BN CLPM. He is a retired Cryptologic language Analyst with over 10 years working as a CLPM. He received his BSBA and MBA from TUI.

MAJ Beckmann currently serves as the operations officer for 717th MI BN. He is a graduate of the Junior Officer Cryptologic Career Program.

MAJ Hunt is the 717th MI BN XO. His previous assignments include BN S3, Assistant BDE S3, Command and General Staff College, CORPS Intelligence Planner, Task Force S2, CO CDR and Infantry PL. He received an MA in Business and Organizational Security Management from Webster University.

LTC Haley is the Commander of the 717th MI BN. Previous assignments include Commander A CO, 312th MI BN; Commander, HHC/1st Cavalry Division; S3 and XO of the 715th MI BN and the USARPAC ACE Chief. He received a BS from the University of Arizona in Chemistry.

A Special Mission unit on Fort Bragg is looking for qualified 35F/X, 35G, 35M and 35Ls for potential assignments. Serving as a Special Operations Intelligence Sergeant is a unique and challenging assignment. This assignment requires an individual who is highly motivated, confident, intelligent, and capable of working without direct supervision. You will be provided the opportunity to work with many national agencies and state-of-the-art systems in order to execute a unique mission of highest importance. Soldiers assigned here have a great opportunity to seek advanced training, be it civilian or military, and also be offered additional pay and accelerated promotion rates for the increased responsibility we place upon our analysts. We are looking for the right Soldier to be a part of the Army's top intelligence innovators who desire the challenge of conducting analysis for strategically directed operations.

Assignment prerequisites:

- Volunteer
- CMF 35F/X, 35G, 35M, 35L
- Minimum 22 years old
- Minimum GT Score of 110
- Rank of SGT – MSG
- Minimum of 4 years - Time In Service
- Must be able to pass an APFT – permanent profiles are considered on a case-by-case basis
- U.S. citizen
- Airborne qualified or volunteer for airborne training
- UCMJ / Financial: No recurring adverse actions
- Security Clearance: Secret; eligible for upgrade to Top Secret

If you have any questions or are interested in applying please contact Jody at (910)643-0689/0649 or at army.sofsupport-recruiter@mail.mil.



Ensuring Operational Readiness through Mission Command Principles

by Captain Douglas W. North

Introduction

As a Company Commander, it is important to first understand, and then assess the processes by which your unit operates. Headquarters and Headquarters Company (HHC), 717th Military Intelligence Battalion is under operational control of the National Security Agency/Central Security Service (NSA/CSS) Texas. This fact requires a number of additional vetting procedures for all personnel requiring access than your typical Army unit. Because of these additional vetting procedures, it was necessary to create a platoon sized element capable of receiving, in-processing, and integrating each Soldier, warrant officer, or commissioned officer into the site. For HHC, these Soldiers became Second Platoon or the Reception and Integration (R&I) Platoon.

Two principles of Mission Command were essential for this element to be successful. HHC had to build a cohesive team, create a shared understanding of the mission, and allow the platoon to exercise disciplined initiative.¹ When R&I platoon initially began operating it took some time to understand the process by which an individual soldier could effectively gain site access. Numerous Military Occupational Specialties (MOS) are typical to HHC and due to their differing training regimens for Advanced Individual Training, each Service Member arrives needing different amounts of assistance to integrate into the site. For example, Signals Intelligence Analysts (MOS 35N) have a longer AIT period during which they typically complete a Counterintelligence Scope Polygraph as part of their training regimen prior to their arrival. A Cryptologic Linguist (35P) however is focused on learning his assigned language and does not complete the polygraph prior to becoming certified in the MOS. This singular difference between initial training processes can extend the integration process for 35P Soldiers by 4 to 6 weeks.

Unit Personnel Security Processes

In the post-media leaks era, the vetting process for allowing personnel access to government facilities, classified

information, and Sensitive Compartmented Information Facilities has become incredibly important. Combat arms battalions and brigades typically accomplish this vetting process by using systems of record such as the Joint Personnel Adjudication System and the Personnel Security Investigation Center of Excellence to efficiently manage personnel security. Security Officers (S2) monitor their personnel and work with the Office of Personnel Management (OPM) and unit commanders to ensure personnel are cleared and have proper access credentials for classified information. S2 personnel are also required to assist commanders when access is to be revoked due to disciplinary action. Understanding and enforcing the security and vetting processes in any Army organization are key to success in maintaining a high level of mission readiness.

The personnel security process for a battalion S2 is learned primarily through “on the job” training. Understanding of the process has typically been limited by a lack of training at the Military Intelligence Officer Basic Course. Additionally, OPM does not advertise its processes very well. Similar to most processes and procedures, the personnel security process requires vigilance in attempting to communicate with the organization operating it to be successful. When navigating the investigation request process, it is important to use tracking systems that provide dates and situational awareness to the S2. This tracking allows the S2 to actively communicate with the proper personnel at each stage in the process and expedite any speed bumps.

An initial assessment of HHC led to the understanding that many of the problems it was having with integration were primarily tied to leaders not having awareness of the process or enforcing the procedures. Developing subordinate leaders was essential in this process.² By knowing how many days each individual remains in R&I platoon, HHC was forced to adhere to the Mission Essential Task List by integrating every Soldier into site in under 40 days. This requirement or MET of averaging a less than 40 day integration timeline was one of the standards to assess readiness of the

company to operate. Adhering to this standard was not an easy task, but as a former Battalion Commander used to say, "Do routine things routinely well." By establishing routines, HHC was capable of optimizing the process and integrating new soldiers at such a high rate that at one point R&I platoon was down to nine personnel, including the Platoon Sergeant and two Squad Leaders.

Vetting Process and Procedures

After understanding and assessing the process, the next step is execution. For HHC, the S2 shop, Platoon Sergeant, Squad Leaders and First Sergeant deserve the bulk of credit for executing this mission at such a high level of success. Vetting each individual who has a Notification of Foreign National Association (NFNA) is the biggest roadblock to accomplishing integration. The NFNA is Security's procedure for notifying the mission element of the foreign national association(s) that is/are reported by the individual during security processing. The intent is to notify the gaining organization of these foreign ties and to request input as to whether it will cause the individual to be unsuitable for the position due to a potential conflict of interest. The problem that occurs is that occasionally the individual needed to approve this request is unavailable due to a temporary duty assignment or leave of absence. Roadblocks such as these continue to be frustrating, but necessary in light of recent media-leaked security breaches that received the national spotlight. They are not any less infuriating when they block the path to efficiency. By consistently tracking these actions, the unit can mitigate roadblocks. The battalion S2 shop created a flow chart that depicts the vetting process from arrival at the unit to integration into site to effectively communicate this process to the battalion and brigade commanders.

To coordinate effectively, the S2 must understand the various entities and personnel they are to communicate with every day. The S2 shop for the battalion coordinates on a daily basis with the Military Affairs Desk Office (MADO) to ensure vetting procedures are executed properly. Additionally, they contact each individual in the chain required to approve NFNAs. The MADO is the branch in the Office of Personnel Security that coordinates with all Service Cryptologic Components to ensure military affiliates assigned to NSA/CSS sites worldwide are properly vetted, cleared, and indoctrinated to NSA/CSS standards. By maintaining oversight into this process, HHC has been capable of more quickly traversing the process.

The S2 shop then adds the Soldier's Security Clearance, Polygraph, and NFNA status to the tracker to determine where in the process the Soldier stands. The tracker is then

sent to the First Sergeant and Company Commander for review. This synchronization of effort between the battalion S2, R&I platoon, and the company command team increased efficiency in the process. Essentially, this is the use of Collective Leadership: synergistic effects achieved with multiple leaders aligned by purpose.³ As soon as a Soldier comes close to the 30 day mark in R&I, the Company Command team begins checking with S2 and R&I platoon leadership to confirm the individual will be scheduled for indoctrination to the site within the next 10 days. It is at this point that most individuals complete their integration and are indoctrinated. The vast majority of those that are held longer than 30 days in R&I are held because of a NFNA conflict of interest.

Conclusion

Soldiers accomplish what leaders enforce. This concept is not a new one for our Army, but it is an apt description of what has led to success in HHC, 717th MI Battalion. The reception and integration process for the battalion has improved dramatically due to the efforts of the NCOs of the organization, and the takeaways apply to many processes within the Army:

- ◆ Communicate effectively.
- ◆ Enforce standards.
- ◆ Establish routines.
- ◆ Maintain situational awareness.

Developing a Mission Command System at the company or platoon level is not an overly complex task as long as subordinates within that system share in the vision for success.⁴ Commanders must communicate their intent clearly for subordinates to execute effectively and enforce the standards within this system.⁵ Routines are established through repetition of the process, and the utilization of trackers helps to maintain situational awareness at all levels. This shared understanding enables leaders and subordinates to establish mutual trust and operate effectively. 

Endnotes

1. ADP 6-0 Mission Command, May 2012, 2.
2. ADP 7-0 Training Units and Developing Leaders, August 2012, 8.
3. ADP 6-22 Army Leadership, August 2012, iii.
4. ADP 6-0, 11.
5. ADP 6-0, 3.

CPT North is the Commander of HHC, 717th MI Battalion. He was previously the Battalion S2 for 4-70th AR Battalion both in garrison and forward in Afghanistan. He graduated from the Counterintelligence Officer's Course and the Signals Intelligence Officer's Course.



Enhancing Adult Learning within the MI Warrant Officer Advanced Course

by Chief Warrant Officer Three LaMesha Craft and Mrs. Rose Phillips

2012/02/01

Tell me and I forget, teach me and I may remember, involve me and I learn."

—Benjamin Franklin

Introduction

The Military Intelligence Warrant Officer Advanced Course (MIWOAC) has arguably been at the forefront of making considerable progress in implementing the Army Learning Model (ALM) 2015. This has been a monumental effort by the MIWOAC cadre, the Chief of the Warrant Officer Training Branch, and the leadership within the U.S. Army Intelligence Center of Excellence (USAICoE). The following is a discussion of how the application of adult learning theories, innovative methods of instruction, and continued education has led to a dynamic shift in the learning experience of mid-to-senior level MI Warrant Officers. This shift in educational design and application can serve as an example for other professional military education (PME) programs.

The MIWOAC is part of the Military Intelligence Warrant Officer Training Branch (MIWOTB), which also teaches the MI Warrant Officer Basic Course. The MIWOTB is part of Bravo Company, 304th MI Battalion, 111th MI Brigade and USAICoE at Fort Huachuca, Arizona. The Advanced Course is a six-week long and employs a multiple module approach to training. MIWOAC trains all MI WO military occupational specialties (MOSSs) in the latest applications of doctrine, technological changes, and concepts within the operational environment.

Adult Learning Theory

The best known adult learning theory is Malcolm Knowles' *Andragogy* (Merriam, Caffarella, and Baumgartner, 2007); however, it is also the most questioned and refuted as to whether it is truly a theory of learning or one of teaching. Within andragogy, Knowles made six key assumptions that delineate the differences between adult and pre-adult learning. The premises behind Knowles' assumptions include:

- ◆ Adults are internally motivated.
- ◆ Adults leverage their knowledge and life experiences when learning.

- ◆ Adults are goal oriented and practical.
- ◆ Adults need to know how what they learn can help them to achieve their goals.

Many of the tenets of andragogy are represented in the MIWOAC to meet the needs of the students. Additionally, by incorporating the various principles of adult learning within the program of instruction (POI), the course has steadily become compliant with ALM 2015, ensuring that the 21st Century Soldier Competencies are met and remain relevant to the U.S. Army as a whole.

Despite some criticisms of ALM 2015, the key benefits to this concept involve the facilitation of experiential and peer-to-peer learning. The MIWOAC consists of mid-to-senior level WOs between the ranks of CW2 and CW3 with an average of 16 years of service by the time they attend MIWOAC. This student population possesses a wealth of knowledge derived from military education and on the job training. Therefore, they require a level of instruction that supersedes the Army's traditional approach to training and education.

According to John Dewey, adults learn through connecting what they have learned from current experiences to previous experiences. This enables them to foresee future implications through interaction (Merriam, Caffarella, & Baumgartner, 2007). The second principle of interaction cites that "an experience is always what it is because of a transaction taking place between an individual and what, at the time, constitutes his [or her] environment (Dewey, 1938, 41 as cited in Merriam, Caffarella, and Baumgartner, 2007). For David Kolb, the primary goal of experiential learning is to obtain "a fully integrated personality" (Kolb, 1984, 164 as cited in Merriam, Caffarella, and Baumgartner, 2007). Based upon the course redesign, MIWOAC students not only learn from the instructor/facilitator in the course, but also through personal reflection and peer-to-peer communications, all of which significantly contribute to higher rates of content retention.

Warrant Officer Advanced Course Redesign

In early 2014, the MIWOAC underwent a significant course redesign to increase its rigor, and challenge the intellect of mid-to-senior level MI Warrant Officers from eight intelligence disciplines. Inherent in this process was the incorporation and application of experiential and peer-to-peer learning techniques to teach doctrinal processes to a population whose understanding of said processes spans a wide spectrum of familiarity. The new course curriculum facilitates cross training to ensure that today's mid-to-senior-level MI Warrant Officers understand how all intelligence disciplines support the intelligence warfighting function (IWfF) and the primary tasks inherent in the IWfF. Students develop a comprehensive understanding of how their intelligence discipline contributes to the larger military operations process.

The first and second weeks of the POI consist of common core training requirements as well as student briefs on their current or future units, overviews on DCGS-A and the U.S. Army Intelligence and Security Command, a briefing from their DA Branch Manager(s), MI MOS capability briefs from the perspective of the students, briefs on leadership and mentorship by well-respected senior Warrant Officers, and overviews of several educational services provided by resident organizations.

During the third and fourth weeks, students receive threaded instruction within a two-week Decisive Action Training Environment (DATE) scenario that includes Analytic Tradecraft, the Military Decision Making Process, Unified Land Operations, Information Collection, and Intelligence Support to Targeting. Throughout the DATE scenario, students utilize experiential and peer-to-peer learning to develop a mission analysis brief, an information collection/management brief, an Annex B (Intelligence) and Annex L (Information Collection) with supporting appendices. The fourth week culminates with a staff ride to Fort Bowie in which students provide information briefs on key aspects of the Battle of Apache Pass at various points along the foot path to Fort Bowie.

During the fifth week, students attend a one-week seminar offered by some of USAICoE's best instructional programs. This one-week seminar allows students to choose from the following topics: DCGS-A, Information Collection, Infrastructure and History, Violent Extremism, and Weapons Intelligence. The students utilize the information they learn

to become better intelligence professionals, mentors, and leaders.

The sixth week culminates with additional instruction on leadership and management such as training and leader development, managing civilians, the future of MI, and a mentorship session led by the WOTB cadre. Throughout the course, the cadre hold the students accountable for their learning experience by utilizing a self-assessment metric.

Application of the Self-Assessment Metric

In an effort to increase student responsibility for learning, the MIWOAC requires all students to maintain a self-assessment metric (See Figure 1) for the duration of the six-week course. On the first day of class, students receive instructions for filling out the metric that has three sections entitled, "What I know or think I know," "What I want to learn," and "What I have learned." Students are instructed to annotate what they know about their MOS and about MI by the end of day one. Furthermore, they are highly encouraged to fill in the "What I have learned" column on a daily basis.

Self-Assessment Metric			Rank/Last Name: _____
What I know (or think I know)	What I want to learn	What I have learned	

As Warrant Officers much of what we learn (aside from PME) are things that we have determined we need to know (or should know) based on our MOS, our position, or our interdependency on other disciplines or agencies within MI. Please fill in this sheet as you progress throughout this course. We will likely ask to see your sheets periodically throughout the course

Figure 1. Self-assessment Metric for MIWOAC Students.

The MIWOAC cadre requires all students to submit a copy of their self-assessment metric at the end of the third week (the halfway point of the course). The cadre then collects, codes, and analyzes the student data. By the end of the fourth week, the cadre presents the aggregate themes from the "what I want to learn" column. They discuss the data from two perspectives: Where in the remainder of the course the students will receive some of the information they want to learn and to solicit feedback on how the cadre can improve the course to provide additional information on topics they already received.

- ◆ **Demographics:** The data represented in Figure 2 was obtained from four recent MIWOAC classes (138 students). The average size of a MIWOAC class is 36 students. The average age of the students in this study is 38 with 81 percent of the student population having a college degree (50 percent of which have a Bachelor's Degree). The students have an average of 16.5 years in military service.

Self-Assessment Metric		Rank/Last Name: _____
<p>What I know (or think I know)</p> <p>Synopsis</p> <ul style="list-style-type: none"> • The majority of students (~85%) were modest when annotating what they know. <ul style="list-style-type: none"> • An average of three to five data points. • Data point typically focused on: <ul style="list-style-type: none"> • Individual intelligence disciplines (INTs) • Experience working on a staff. • Experience working as a section/team leader. • Current unit's structure (e.g. BCT, BfSB COCOM). • Areas they need improvement. 	<p>What I want to learn</p> <p>Top 14 Topics</p> <ul style="list-style-type: none"> • Better utilization of INTS: 93 • INT specific training: 55 • Senior WO Responsibilities: 43 • MDMP: 40 • The future of MI: 31 • Mentorship qualities: 30 • DCGS-A Interoperability: 22 • Methods to improve promotion potential: 21 • Integration of intelligence technological systems: 20 • Information collection / collection management: 18 • Joint Operations: 18 • Cyber Operations: 11 • Networking Tips: 11 • Better integration of all INTs in the intelligence cycle: 8 	<p>What I have learned</p> <p>Synopsis</p> <ul style="list-style-type: none"> • The majority of students (~85%) listed two to three times more data points in this column than the first column. <ul style="list-style-type: none"> • Likely a reflection of information they unexpectedly learned. • Other students (~15%) captured information that they deemed most valuable in this column. • Students acknowledged they learned 85-90% of what they listed in the "want to learn" section. <ul style="list-style-type: none"> • Students were generally pleased with the information learned, but wanted more specifics.
<p>The data represented was obtained from four MIWOAC classes (138 students). Collectively, each class listed an average of 36 topics under the "What I want to learn" column. Of the 36 topics, there were 14 reoccurring themes.</p>		

Figure 2. Data analysis of self-assessment metric for MIWOAC students.

◆ **Data Analysis:** Collectively, each class listed an average of 36 topics under the "What I want to learn" column. Of the 36 topics, there were 14 reoccurring themes across the four MIWOAC classes (See Figure 2).

Instructor Benefits from USAICoE SFDB Courses

Given the knowledge of the students, the Chief of the MIWOTB ensures the MIWOAC cadre has the requisite experience and technical skill-sets to facilitate experiential learning. These

skills are developed and continuously improved upon by attending a variety of professional development courses taught by USAICoE's Staff and Faculty Development Branch. Courses such as the Learner Centric Teaching Method (LCTM), Small Group Instruction (SGI) and Advanced Instructional Methods (AIM) provide insight into a myriad of ways to enhance instruction and facilitation skills within an adult learning environment. LCTM delves into Kolb's Experiential Learning Model, allowing facilitators at the MIWOAC to manage a classroom with diversified experiences. SGI explores numerous small group techniques that can be implemented within the classroom, allowing the facilitator to more accurately assess individual contributions and group cohesion. Finally, AIM stresses the importance of student reflection, and critical thinking within the classroom environment through the sharing of experiences through the development and implementation of case studies.

The Way Ahead: Capitalizing on the Full Circle of Adult Learning at USAICoE

The MIWOAC has made significant strides over the last year to increase the rigor of the course curriculum. However, the MIWOAC continues its efforts to improve the course, leaning heavily on the extensive feedback from the students of today to stay ahead of the requirements for the students of tomorrow. The cadre within the MIWOAC seeks to increase MOS disparity within the cadre to enhance the experiential learning that students can leverage. Additionally, MIWOAC cadre actively seeks additional SFDB courses to attend in between MIWOAC classes to enhance adult motivation to learn. 

References

Merriam, S. B., Caffarella, R. S., and Baumgartner, L. M. (2007). Learning in Adulthood: A Comprehensive Guide. San Francisco, CA: Jossey-Bass.

CW3 LaMesha Craft is a Master Instructor assigned to the MIWOAC, WOTB. She has been assigned to the Warrant Officer Training Branch since July 2013 and was the MOS 350F Track Course Manager within the WOBC. Additionally, she was the USAICoE Instructor of the Quarter, 4th Quarter, FY 2014. She is a PhD candidate with Walden University's School of Public Policy and Administration.

Mrs. Phillips is a Master Instructor working within the SFDB as Deputy Chief. She was a Training Specialist from December 2009 to December 2011 with the MOS 35F10 Intelligence Analyst Course, 305th MI BN. Mrs. Phillips transitioned to an Instructional Systems Specialist position in January 2012 as she became part of the SFDB team. She is a PhD candidate with Capella University's School of Professional Studies in Education.

Training Development and Support Directorate



The Intelligence CoE's Self-Development Program: Intelligence Leader Development Resource

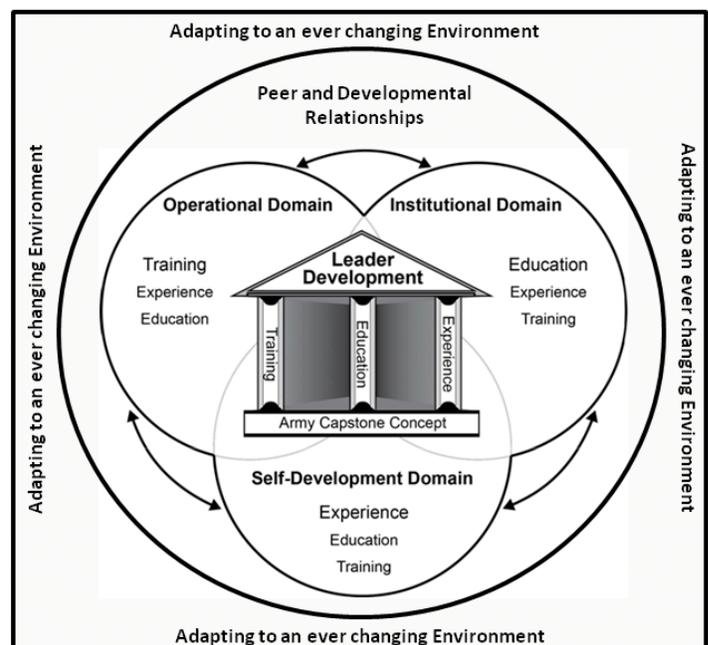
by Major Josef Thrash III, Captain Jennae Tomlinson,
and Sergeant First Class Nakisha Matthews

"In today's complex, rapidly changing, and increasingly competitive environment, we must LEARN—faster, better, and more deeply than our competitors and adversaries."

—General Ray Odierno

Every leader at every echelon throughout history has put an emphasis on the importance of leader development. Major General Robert Ashley, then the Commanding General of the U.S. Army Intelligence Center of Excellence (USAICoE), recognizing the need for a Career-Long learning program that utilized the limitless potential of social networking as a platform, directed the development of the Intelligence Leader Development Resource (iLDR). The iLDR project facilitates easy, open access to effective professional and self-development solutions by connecting intelligence professionals with resources, leaders, peers, academia, and private sector community on a variety of topics crucial to leadership development, intelligence studies, and issues related to geopolitics pertinent to regions of national and strategic importance.

The Army Leader Development Strategy 2013 provides a comprehensive approach to developing leaders to meet the security challenges of today and tomorrow. The strategy outlines the framework for the strategic vision as a mutually shared responsibility between institutional Army, the operational force, and the individual. It further requires leaders to help individuals realize that individual commitment to career-long learning is essential to their development as leaders. iLDR is a leadership tool that provides a robust and relevant platform to enhance any development model.



The Army Leader Development Model establishes three distinct, yet overlapping, domains that encompass leader development: Operational, Institutional, and Self-Development. Common to every domain are Education, Experience, and Training, which are paramount to how leaders develop, no matter their unit of assignment. iLDR provides a network capable of fusing and threading these tenets throughout the domains. It serves as an easy access to a professional, self-development domain through an open access and dynamic website that serves as a uni-

versity model, integrated self-study program that promotes the 21st Century Soldier Competency of the life-long learner.

"iLDR's intent is to support leader development and provide materials for mentors to use while engaging their Soldiers. Mentorship and leader development have and will always be our asymmetric advantages. When we think about the monumental task of managing the human dimension and cognitive development of thousands of Soldiers...sometimes the solution is simple as the campfire chats between then Colonel Fox Conner and a bright young Major named Dwight Eisenhower. iLDR is meant to provide those tools to inspire leaders to continue their self-development and take on the mentorship role as Fox Conner did with Dwight Eisenhower, George Marshall, and George Patton."

—MG Robert Ashley

In order for iLDR to be successful, we are asking for your assistance to build a cache of leader development resources to be shared and utilized across the force. You and your unit are doing outstanding things, we need you to consider sharing those leader development lessons learned, experiences, and success stories with the rest of the force. If you have successfully completed your time in a leadership position, such as First Sergeant, share that with us by filming a 10-to-12 minute video detailing your experiences and relaying insights that you believe will prepare the next NCO to assume that leadership role. Tell us what a new Commander may need to know to develop an effective command team and climate. If your unit has an effective leader certification program, share that with us in the form of a white paper that provides the details of the program with quotes, metrics, and even pictures. Allow us to share your leader insights and lessons learned to enhance the MI force as we continue to develop resilient and adaptive leaders.

The iLDR website is divided into three MI-related topic pages: Leader Development, Intelligence Studies, and Geopolitics. Each topic will have subsequent topics underlying key discussion points. The topics will provide an article for discussion, reflection questions and additional resources such as books, articles, videos, and more designed to enhance the discussion amongst intelligence professionals. Leader Development will focus on development, attributes, competencies, mission command and the profession of arms. Intelligence Studies will focus on intelligence fields, current and future threats, the future of the Army and the Intelligence Community (IC), outside operations and relations, self-development, and cyber operations. Geopolitics will be led by the TRADOC Culture Center (TCC) with information and research into countries in each of the Combatant Commands.

Currently, the iLDR website is live and each topic page has a main topic article. The Leader Development topic page

concentrates on leader development programs. It discusses the importance of these programs as well as bringing attention to some of the current programs throughout the Army. The Intelligence Studies topic page focuses on the building and developing of intelligence professionals with articles from academia as well as the military. The articles examine the intelligence professional by building an integrated and cohesive leader development program. The Geopolitics page shares TCC's mission and the new Army doctrine, Culture-Regional Expertise and Language. The focus is on knowing how the cultural terrain can help Soldiers become adaptive leaders. The website provides opportunities for MI professionals to connect with leaders and peers, as well as academia and private sector professionals, through open discussion forums related to trending leader development topics. This interactive mentorship opportunity will enhance Soldier and leader development, while reinforcing existing developmental programs at every command level.

iLDR hosts the USAICoE CG and CSM reading lists, a monthly newsletter, and personal video. It advertises upcoming leader development opportunities, such as the schedule for the MI Senior Mentor Symposium, which is delivered over Defense Connect Online. iLDR will augment Initial Military Training and Professional Military Education curriculums to enhance individual learning as well as incorporate leader development tactics, techniques, and procedures and lessons learned from the field. In a future release of the website, Soldiers will also be able to receive advice from peers, IC professionals, private sector leaders, and USAICoE instructors through secure, open access discussion forums.

The iLDR is not the first site of its kind. There have been several forums developed specifically for collaborative knowledge sharing and the information exchange within the military community. These sites have tools available for users to enhance their knowledge and minimize on-the-job training requirements. In many cases users have arrived at their next assignment more informed and ready to perform based on their utilization of these sites, gaining them instant respect from subordinates due to their level of preparedness. Self-development remains an important and powerful tool for job performance.

iLDR is not focused on any one aspect of being an MI Professional. It is a developmental tool and resource that can be used throughout your career; an additional asset in a resource constrained environment. It serves as a home base for collaboration with peers and other leaders, a reservoir of online tools, training recommendations and videos, and an interactive forum to share experiences. Most impor-

tantly, regardless of what duty position you hold or where you are stationed, iLDR will prove to be a dynamic and relevant resource in your kit bag.

An example, SFC Murphy has been tasked to develop a Leader Professional Development (LPD) session for his platoon. SFC Murphy visits the Geopolitics page of iLDR and decides to have the session focus on how terrorist groups are targeting military personnel and spouses utilizing social media. SFC Murphy reads the lead article, views the supporting videos, and then reads two of the supporting journal articles. By using the reflection questions that accompany each main topic article hosted on iLDR to facilitate group discussions, SFC Murphy is prepared to lead and host the LPD. iLDR can also be utilized to enhance a unit's existing LDP.

"A thorough knowledge of your profession is the first requirement of leadership and this certainly has to be acquired. Observing others is important—trying to determine what makes them stand out. That's why I think we can learn a lot by studying past leaders."
 —GEN Omar Bradley

Visit the website (<https://www.ikn.army.mil/apps/iLDR>) and provide the iLDR Team with your feedback. Whether a

link needs to be added or you want to write a future article about a certain subject, no contribution is too big or too small. We are eager to hear comments and will make the appropriate changes necessary to make this self-development tool a success for years to come. 🌟

MAJ Thrash is the iLDR Program Manager for USAICoE, Fort Huachuca, Arizona. He has served in a variety of operational assignments including Battalion XO, Battalion S3, and multiple deployments to Iraq as Brigade S2 and Company Commander.

CPT Tomlinson is an iLDR Site Manager. She has served in various MI assignments at the company level in garrison and while deployed to Afghanistan to include SIGINT Platoon Leader and MICO XO.

SFC Matthews is an iLDR Site Manager. She has been in numerous leadership positions at Brigade and Corps level staff. Her most recent position was the BDE S2 NCOIC while deployed to Afghanistan.

The 2014-2015 issues of MIPB can now be accessed on the outside of IKN (no CAC login required) at <http://ikn.army.mil>. Both regular and e-reader versions are available.

To access archived back issues, logon with your CAC and click on the MIPB icon under IKN Community Sites. Go to past issues to select the issue.



Culture Corner



TCC Support to USAICoE's iLDR Initiative

by Christopher Clark

The TRADOC Culture Center (TCC) is pleased to participate in the iLDR initiative, USAICoE's first public website. Each month TCC highlights geopolitical aspects of culture in a given country or region, providing guiding questions to assist leaders in exploring relevant aspects of culture, how it applies to them as leaders, how they can transfer this knowledge to their subordinates, and how culture can be integrated into the mission planning process. Geopolitics is a broad concept that encompasses many areas of study to include geography, economics, politics, history, demography, and many other aspects of a given country or region. Further examination into the cultural aspects of geopolitical factors will reveal that culture is present throughout all of these factors.

One may ask, how does culture fit into these aspects of Geopolitics? The answer is that culture provides the context in which many geopolitical factors exist. Culture dictates whether there is a formal or an informal economy, centralized or decentralized government, and whether there is a linear or circular perspective of their history. Many think that culture exists outside the influence of these geopolitical factors when, in reality, there is very little that exists within a culture that has not been shaped to meet the current needs or requirements of the culture.

The screenshot shows the USAICoE iLDR website interface. At the top left is the U.S. Army logo, and at the top right is the 'ALWAYS OUT FRONT' logo. The main header reads 'GEOPOLITICS'. A navigation menu on the left includes: HOME, LEADER DEVELOPMENT, INTELLIGENCE STUDIES, **GEOPOLITICS**, LINKS, PROFESSIONAL DEVELOPMENT TOOLKIT, FORSCOM LEADER DEVELOPMENT TOOLBOX, and CENTER FOR ARMY LEADERSHIP. The main content area is titled 'Topic: North Korea' and lists several bullet points:

- Democratic People's Republic of Korea (DPRK), Independent from Japan in 1945
- Government: Juche, Socialist State, Single-party State
- Supreme Leader: KIM Jong Un, designated successor Sept 2010, current leader as of Dec 2011 (after death of previous leader and father Kim Jong Il)
- Population: 24,851,627 (July 2014 est.)
- Military Branches: North Korean People's Army Ground Forces, Navy, Ari Force; Civil Services (2005)

 A quote follows: "Independence is an attribute of man, the social being; it should not be viewed as the development to perfection of a natural, biological attribute of living matter. This is, in essence, an evolutionary viewpoint. Of course, we do not deny evolutionism itself. Science has long established the fact that man is a product of ages of evolution. Man is a product of evolution, but not his independence. Independence is a social product. Independence is an attribute given to man by society, not nature; it is not a natural gift, but has been formed and developed socially and historically"- North Korea's longtime leader, Kim Jong Il (deceased)", Dec 2011. Below the quote are 'Main Articles' with links to: 'The cultural life of North Korea by Tania Branigan', '7 Strange Cultural Facts About North Korea by Stephanie Pappas', 'Civic vs. Social: How politics holds back Seoul's North Korean human rights law by Subin Kim', and 'North Korea and nukes: It's not all bluff by Andrei Lankov'. A 'Culture:' section begins with: 'Despite the existence of two distinct countries today, North and South Korea share a common cultural base. Most aspects of their traditional culture were formed and fully integrated into Korean society well before the split of the countries following World War II. Thus, 2015 not only marks the 70th anniversary of the end of WWII, it also marks the amount of time since the Korean peninsula has been ruled under one government. In fact, one would have to go all the way back to 1910 to find a time when one central Korean government controlled the entire peninsula. From 1910 to 1945, Japan occupied the peninsula and actively sought to destroy Korean culture to replace with Japanese culture. Despite Japan's best efforts, most Korean values and beliefs survived this period. It would then be reasonable to assume that the cultural identities of North and South Korea are very similar today since their cultural identity has survived despite extensive turmoil, right? The answer to that can be found in exploring the concept of *juche* and how *juche* exists in both countries today. *Juche* roughly translates to "self-reliance." It was this self-reliance that allowed their culture to survive through the Japanese occupation, but with the split between the North and the South, each country has shaped *juche* a little differently to...' On the right side of the page, there are sections for 'FEATURED VIDEOS' (with a video titled 'MY ESCAPE FROM NORTH KOREA'), 'DOWNLOADABLE CONTENT', 'FEATURED BOOKS' (with books like 'NORTH OF THE DMZ' and 'GETTING YES'), 'ARTICLES & JOURNALS', 'GEOPOLITICS LINKS', and 'PROFESSIONAL REFERENCES'.

The influence of culture on these factors is what gives each country and region throughout the world its own unique identity. This is why the TCC trains and educates Soldiers on the fact that culture exists within all aspects of a society and not in its own separate space. Based on the concept that culture is interwoven through geopolitics, the optimal way for the TCC to support the geopolitics section is to highlight the cultural aspects of geopolitics for the specific country being featured each month.

A recent feature addressed North Korea. The primary focus of the content provided by the TCC is the concept of *juche* in both North and South Korea and how this concept has evolved differently for the two countries over the last 70 years. In both countries, *juche* translates roughly as "self-reliance." North and South Korea have used *juche* to meet their politi-

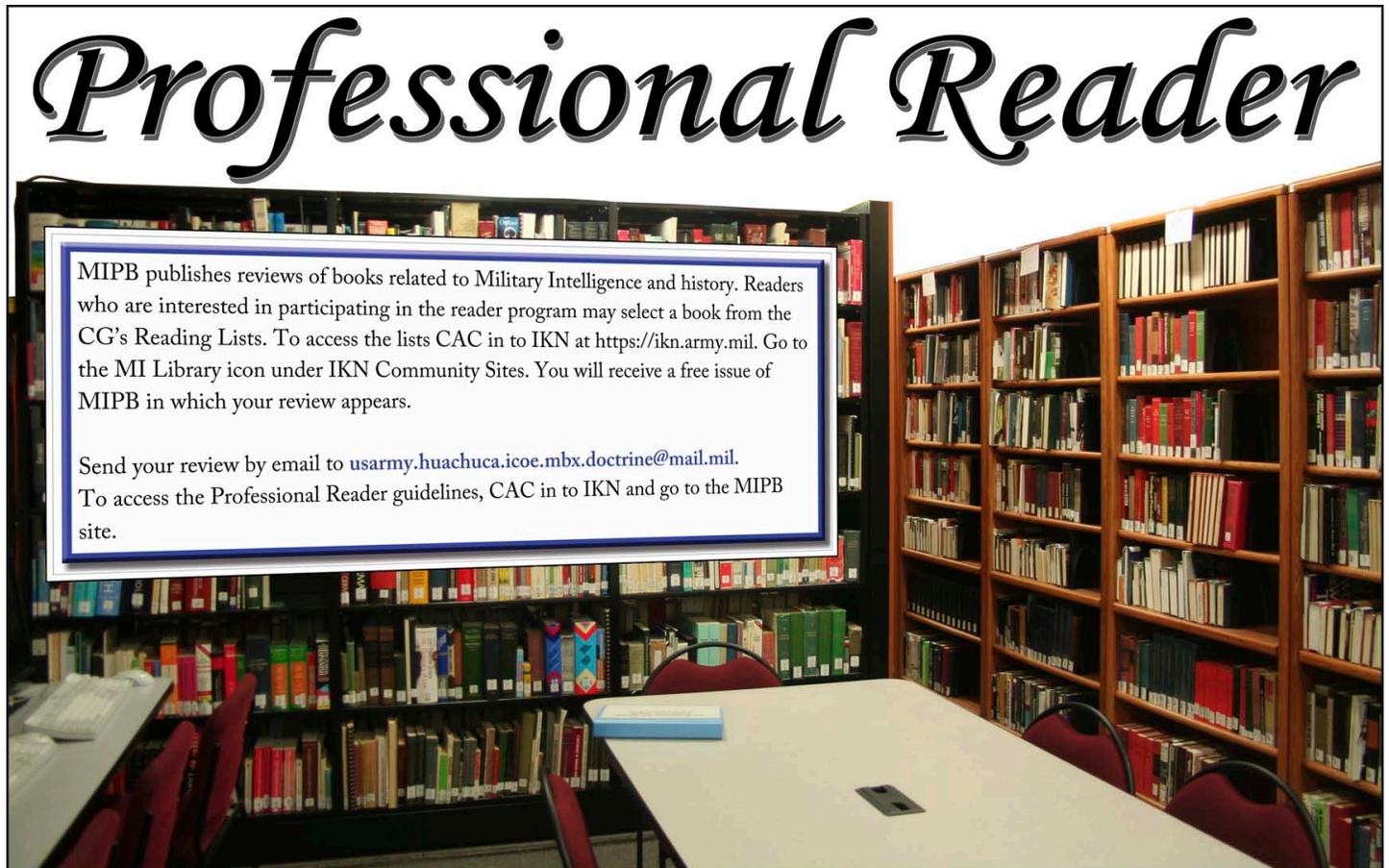
cal and economic needs, but in much different ways. In North Korea, *juche* was used to justify one-man rule which led to the installation of Kim il-Sung as the Supreme Leader and has kept the country under a strict dictatorship since the North/South split. South Korea used *juche* to serve as a motivating factor to modernize the country and strengthen the economy, resulting in South Korea becoming a global economic power with the 12th largest economy in the world (CIA Factbook).

This is just one of many examples of how culture has shaped the geopolitical makeup and collective mindset of a country. Further analysis into both North and South Korea also highlights that geopolitical institutions have a reciprocal influence on culture. Differing geopolitical factors within each country have influenced permanent and lasting cultural change, creating two unique cultural identities. These diverse identities would make reunification a highly challenging prospect.

Through use of similar case studies and exploration of the relationship between culture and geopolitics, the TCC will continue to support the iLDR initiative for the foreseeable future. It is important to continue to not only illustrate the influence of culture on geopolitics, but also how understanding culture enables MI professionals as leaders and supports their life-long professional development path. An iLDR user can look forward to the cultural perspective of geopolitics on countries in the PACOM, EUCOM, and AFRICOM regions. ✨

Mr. Clark is a TCC Training Specialist. He retired from the U.S. Army with 20 years of service as an Intelligence Analyst. He served in numerous locations to include Iraq, Germany, England, Japan, and South Korea. Assignments of note include member of a Military Transition Team for the 1st Mechanized Brigade, 9th Iraqi Army Division; instructor for the MOS 35F10, Intelligence Analyst Course, and Chief Instructor for the MI Senior Leaders Course. He earned a BA in Business Administration from Franklin University and a Masters of Business Administration with a minor in Technology Management from University of Phoenix. As part of the TCC Professional Military Education team, he develops culture education and training products for use in professional development courses for the enlisted and officer cohorts. Mr. Clark also develops products and training for Soldiers deploying to the PACOM area of responsibility.

Professional Reader



MIPB publishes reviews of books related to Military Intelligence and history. Readers who are interested in participating in the reader program may select a book from the CG's Reading Lists. To access the lists CAC in to IKN at <https://ikn.army.mil>. Go to the MI Library icon under IKN Community Sites. You will receive a free issue of MIPB in which your review appears.

Send your review by email to usarmy.huachuca.icoe.mbx.doctrine@mail.mil. To access the Professional Reader guidelines, CAC in to IKN and go to the MIPB site.

Moments In MI History

JSTARS in Operation DESERT STORM

by Lori S. Tagg, Command Historian, USAICoE

On January 14, 1991, the Joint Surveillance and Target Attack Radar System (now referred to as JSTARS, but at that time stressed as the "Joint" STARS) had its first operational mission as part of Operation DESERT SHIELD in the Persian Gulf. The air offensive was scheduled to begin two days later, and the US Central Command (CENTCOM) was desperate for targeting information. Up to this time, the Army lacked a long range, near all-weather, night and day intelligence, surveillance, and reconnaissance (ISR) and targeting capability. JSTARS was meant to fill that gap.

The JSTARS was comprised of an E-8 platform and several ground station modules (GSMs). It could provide wide-area surveillance through a moving target indicator (MTI) and two- or three-dimensional imaging through synthetic aperture radar (SAR). Both the Army and Air Force had parallel development programs for similar systems in the 1970s. In the early 1980s, however, Congress ordered that the two programs be integrated into a single system and a joint program office was established.

As a joint program, both Army and Air Force operators flew onboard the aircraft. Although they looked at the same real-time radar data, each had a different perspective of what it meant and where it would be most useful. Air Force operators looked for immediate targeting data for attack aircraft and could track moving targets in real time. Army operators manipulated the data differently, especially in the GSMs, to look at changes through time to predict enemy ground movements.

In September 1990, JSTARS conducted a successful Operational Fielding (Feasibility) Demonstration for both American and allied personnel in Europe. It was tasked with locating and targeting three 25-vehicle convoys moving at night. JSTARS easily passed the test. Shortly thereafter, a team of Army and Air Force program and system managers traveled to Saudi Arabia to brief the system capabilities and status to General Norman Schwarzkopf, the CENTCOM commander. Earlier in the summer, GEN Schwarzkopf had requested, then cancelled JSTARS deployment to Southwest Asia because the system was still in its testing phase and

its maturity for use in wartime was in question. By the December briefing, however, he had reconsidered and immediately requested deployment of the system to be operational by January 15, 1991.

In less than a month, the Army needed to form a unit, standardize all the equipment, identify and train personnel, arrange for the shipment of the GSMs, and develop a concept of operations for how the system would be employed in theater. At this time, the Army had no policy or procedures for integrating developmental systems into a theater of operations. No provisions existed for authorizations to form a provisional unit. The Commanding General at the U.S. Army Intelligence Center, Major General Paul Menoher, personally worked with the Department of Army Staff to get a provisional JSTARS detachment manned, equipped, and trained in time for deployment.

The whole process was contrary to policy and an exception to standing procedures. Colonel Martin S. Kleiner, the U.S. Army Training and Doctrine Command Systems Manager for JSTARS, formed the JSTARS Operational Detachment One and recruited and trained personnel from the Intelligence Center to operate the GSMs. The Air Force established its own 4411th JSTARS Squadron. Preparation time was so compressed that integrated training with USAF and Army personnel was still ongoing during the 17-hour flight to Saudi Arabia.

By January 12, two E-8A aircraft and five GSMs (a sixth came later) arrived in Saudi Arabia. Two days later, JSTARS was flying its first mission. COL Kleiner remembered that first mission as a learning experience: "The aircraft was airborne, it was down-linking radar and the ground stations were receiving it. Quite frankly, we had no idea what we were looking at. Our application of the system was pretty much being developed on the fly. This was a revolutionary capability. It wasn't simple evolution moving from one capability to incrementally something better. No matter how much you test or how much you postulate, until you actually get into an operational environment, you don't know what you are going to see."



The JSTARS E-8A aircraft, one of the GSMs, and its development crew. The developmental aircraft proudly proclaimed itself as a joint Army-Air Force asset.

The first mission began as an engineering test flight to determine what the system could produce but quickly became an eight-hour intelligence-gathering mission. Although initial plans called for the system to be used exclusively for targeting, JSTARS eventually was used to locate and track enemy units, especially those dug in along the Iraq and Kuwait borders with Saudi Arabia. Throughout the course of Operations DESERT SHIELD/DESERT STORM, JSTARS flew 49 consecutive, successful missions, mostly at night, tracking and targeting fixed and mobile enemy forces and Scud missile launchers for Coalition forces.

JSTARS proved critical during the first ground engagement near Khafji in Saudi Arabia, which the Iraqis had attacked on January 29. JSTARS was able to identify the location of Iraqi troops, when and where they were moving, and confirm the absence of any reinforcements en route. This convinced Coalition ground commanders that the engagement was not part of a much larger battle and allowed them to focus their assets accordingly and not disrupt the established campaign plan. JSTARS also detected Iraqi efforts to resupply its troops, and U.S. attack aircraft destroyed 70 percent of the vehicles and dispersed the rest.

After the war, COL Kleiner stated unequivocally that the JSTARS system contributed significantly to the war effort in the first Gulf War. Both the Army and Air Force were in agreement that the system proved its worth. Brigadier General John Stewart, the G2 for Army CENTCOM, stated, "The JSTARS was the single most valuable intelligence and targeting collection system in DESERT STORM....JSTARS was instrumental in making every 'key read' during the ground war." Air Force Chief of Staff General Merrill McPeak predicted, "We will not ever again want to fight without a JSTARS kind of system."



The JSTARS prepares to take off for one of its 49 successful missions for Operation DESERT STORM.

Perhaps the only complaint about JSTARS during the campaign was there were not enough present in theater to satisfy all requirements. Although initially planned for dedicated support to the Corps, the two available systems had to adopt a larger theater support concept.

In hindsight, the battlefield in Kuwait and Iraq was certainly ideal for employment of the system, the largely armored enemy was moving in mass formations over clear and uniform terrain with little civilian presence. In addition, the Coalition enjoyed air supremacy, which led

to its capability to immediately destroy JSTARS-identified targets. Indeed, the next employment of JSTARS as part of the peacekeeping Operation JOINT ENDEAVOR in the more mountainous Bosnian terrain would prove to be much more challenging.

Still, in the years following the first Gulf War, JSTARS enjoyed unmitigated support and Congress increased its funding. It had proved itself a critical targeting and intelligence asset. From the beginning it represented something even bigger. Major General Robert Noonan, Commander of U.S. Army Intelligence and Security Command, captured that sentiment in 1999 when he said, “This integration of Army

operations and intelligence soldiers with Air Force targeters and battle management officers represents the cutting edge of joint warfighting.”

Interestingly, the JSTARS had been used operationally in two theaters before the first production aircraft was even delivered in 1996. The final aircraft was not delivered until 2005. The system has conducted hundreds of missions in support of Operations IRAQI and ENDURING FREEDOM, and NEW DAWN. By 2014, funding issues were preventing the Air Force from replacing the fleet, but it was projected to remain in service until nearly 2030, albeit with updated sensors and electronic equipment. ✨



USACOE History Office photo

This destruction of Iraqi military vehicles along the “Highway of Death” was a direct result of JSTARS targeting capability. The Iraqis used school buses to move its ground troops.



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; 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. 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.
- ◆ 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 republication 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 (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.
- ◆ 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 contact information:

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

**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: 105293-000