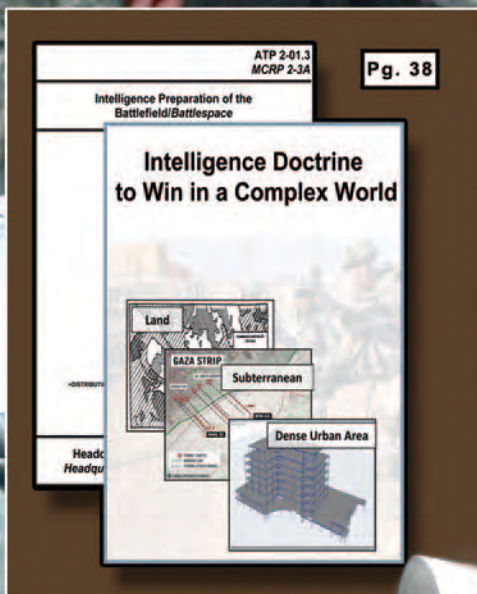




BCT S-2 Operations



Subscriptions: Please see the important notice on the bottom of page 23 regarding changes to MIPB's subscriptions.

Don't forget to email the Editor when your unit moves, deploys, or redeployes to ensure 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 Matthew R. Martin

Command Sergeant Major, MI Corps

CSM Thomas J. Latter

STAFF:

Editor

Tracey A. Remus
usarmy.huachuca.icoe.mbx.doctrine@mail.mil

Design and Layout

Gary V. Morris

Cover Design

Gary V. Morris

Military Staff

CPT Robert D. Wickham

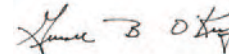
Purpose: The U.S. Army Intelligence Center of Excellence publishes the **Military Intelligence Professional Bulletin (MIPB)** quarterly under the provisions of **AR 25-30**. MIPB presents information designed to keep intelligence professionals informed of current and emerging developments within the 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

By order of the Secretary of the Army:

MARK A. MILLEY

General, United States Army
Chief of Staff

Official:



GERALD B. O'KEEFE

Administrative Assistant to the
to the Secretary of the Army

1703312

From the Editor

The following themes and deadlines are established for:

October – December 2017, Division and Corps Intelligence Operations, deadline for submissions is 7 July 2017.

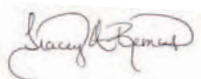
January – March 2018, Military Intelligence Capability Development, the focus for this issue will be on future systems and their fielding. Deadline for submissions is 28 September 2017.

April – June 2018, Leader Development, this issue will focus on developing leaders at all levels within the operational and institutional force. Deadline for submissions is 3 December 2017.

July – September 2018, INSCOM 2020, this issue will focus on how INSCOM supports commanders now and into the future, Deadline for submissions is 4 March 2018.

As always, articles from you, our reader, remain important to the success of MIPB as a professional bulletin. Please continue to submit them, even if the topic of your article may differ from an issue's theme, do not hesitate to submit it. Most issues will contain theme articles as well as articles on other topics. We seriously review and consider all submissions that add to the professional knowledge of the MI Corps and the intelligence community.

Please call or email me with any questions regarding your article or any other aspects of MIPB. We welcome your input and suggestions.



Tracey Remus

Editor



FEATURES

The views expressed in the following articles are those of the authors and do not necessarily reflect the official policy or position of the Departments of the Army or Defense, or the U.S. Government. Article content is not authenticated Army information and does not supersede information in any other Army publication.

BCT S-2 Operations

- 6 Observations from a Year as the Brigade S-2 Observer-Coach-Trainer at the Joint Readiness Training Center**
by Major Nathan Adams
- 15 The Brigade Combat Team Intelligence Staff Officer Course**
by Major Jason Buchanan and Lieutenant Colonel Anthony Covert
- 18 The Keys to Success: Integration between the Brigade Combat Team S-2 and the Military Intelligence Company**
by Chief Warrant Officer Two David Pierce
- 20 Systemic Challenges within a Brigade Combat Team Military Intelligence Company**
by Captain Grace Lu
- 24 Distributed Common Ground System - Army in the Brigade Combat Team: The Path to Success and Mastery**
by Lieutenant Colonel Jim Reed, Chief Warrant Officer Two (P) Rob Buckley, and Mr. Devin Rollis
- 28 Speaking a New Language: MI Gunnery**
by Captain Jamie B. DeSpain, with Chief Warrant Officer Two Trevor J. Kinzel, Warrant Officer One Paul A. Crawford, and Warrant Officer One Jasmin J. Johnson and First Lieutenant Joseph L. Honeycutt
- 31 Intelligence Reachback Genesis**
by Chief Warrant Officer Two Aaron Wolfgang and Chief Warrant Officer Three Keegan Guyer
- 33 Establishing an Intelligence Reachback Cell**
by Chief Warrant Officer Two Orrin Thompson
- 36 Combat Aviation Brigade Intelligence Operations**
by Chief Warrant Officer Two Tia Caywood
- 42 Opposition Forces versus Rotational Training Unit Small Unmanned Aircraft Systems at the Joint Multinational Readiness Center**
by Lieutenant Colonel Matthew T. Archambault, Captain Franklin G. Peachey, Captain Sean D. Hayball, and Staff Sergeant Drew D. Lincoln
- 47 Overcoming One-Handed Punching: Insights on Breaking the Barriers to Integration**
by First Lieutenant Ross Stergios Nikides
- 52 Defensive Cyberspace Operations Intelligence Support**
by Colonel David Kim, Colonel James Adams
- 55 Intelligence Training Management: Noncommissioned Officer Training Strategies**
by Chief Warrant Officer Four John K. Kennedy

DEPARTMENTS

2 Always Out Front

4 CSM Forum

5 Technical Perspective

38 Doctrine Corner

58 MG Oliver W. Dillard Award

59 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



At the core of every U.S. Army intelligence professional, is a competent and proficient analyst. The Army trains us all, even those whose primary task is a collection mission, to be analysts first, and whether we are analyzing new single source data or building a multi-INT product, our information is critical to leader decision-making. In a way, we as intelligence professionals are the master sense makers of extremely complex operating environments. One of the most challenging yet rewarding assignments for any intelligence professional is to serve in a brigade combat team (BCT) S-2 intelligence section. The BCT is the U.S. Army's primary combined arms, close combat force. Within the mission command warfighting function of the BCT resides the command team and key staff sections, like the S-2 section, who serve as principle and trusted advisors. These staff sections provide recommendations and vital information to allow the commander to make informed decisions on the battlefield. The role the S-2 plays in command decisions and BCT operations is incredibly important; as technology and capabilities of threats increase, commanders will rely even more heavily on their S-2 teams to provide timely assessments and predictive analysis.

To emphasize BCT S-2 training efforts across the Army, the military intelligence (MI) senior leadership designated calendar year 2016 as the "Year of the BCT S-2." Since then, the MI Corps made great headway with various projects in support of this initiative. We created new and unique training plans and courses across the operational, institutional and self-development training domains, as well as at our combat training centers. Now with the start of 2017, our new yearlong campaign is "Intelligence Readiness." Though the "Year of the BCT S-2" has ended, the initiatives and impacts of the Corps' focus on the BCT S-2 sections will play a decisive role in increasing readiness for the MI Corps for years to come.

Serving in a BCT S-2 section is one of the most demanding and challenging jobs MI professionals will face during their careers. However, it is not an assignment to avoid. It takes a dedicated team of officers, warrant officers, noncommissioned officers, and Soldiers to perform successful S-2 operations. I have spent the majority of my career serving in a "2" role, from battalion S-2 through combatant command

J-2. During my 159 months as a "2," I have seen what works and what does not. I want to share some key takeaways for all MI professionals currently serving in a BCT S-2 intelligence section or those who will serve in one in the future.

Of the numerous competencies it takes to make a successful S-2 team, I believe developing relationships and building strong partnerships to help create organizations of trust is absolutely essential in everything we do as intelligence professionals. There are three crucial relationships and partnerships I believe are essential for an S-2 team to succeed.

First, a strong and close relationship with the commander is critical. Learning how the commander thinks, makes decisions, and gleaning their intent helps an S-2 intelligence section better answer intelligence requirements and address gaps.

Second, a BCT S-2 section must frequently synchronize the intelligence warfighting function across the brigade by the routine interaction with subordinate battalion S-2s. Creating these effective working relationships between S-2s foster the sharing of best practices, synchronization of collection efforts during training and while deployed, and combining efforts to create collective, multi-echelon training programs across the brigade. Without regular collaboration and synchronization between S-2 sections, brigade intelligence assets will always struggle to maximize their collection and production potential.

Third, robust relationships between the S-2, S-3, and S-6 sections are vital for successful operations across the brigade. When the efforts of these staff elements are working in unison, intelligence can have a very strong, positive influence on operations and vice versa. The commander's intent will be executed, key tasks accomplished, and end state realized.

Leadership expert Stephen M.R. Covey wrote in his book *The Speed of Trust*, "Trust is a function of character and competence."¹ Developing personality and character-based relationships with the commander, subordinate S-2s, and the S-3 are vital for successful S-2 operations, but competence is an equally important piece. The MI observer-coach-trainer teams at the Army's three maneuver combat training centers (CTCs) — National Training Center,

Joint Readiness Training Center, and the Joint Multinational Readiness Center — are constantly assessing the abilities and competencies of BCT and battalion S-2 teams that go through “The Box.” They have identified some overarching challenges and areas for improvement that are causing BCT S-2 teams to struggle. If the CTCs see common issues across various S-2 intelligence sections, it is likely the majority of BCT S-2s are experiencing the same issues. It takes proactive leaders to assess the challenge, develop a plan, and execute before a concern has a chance to become an issue at a combat training center or during combat. Some observed issues the MI observer-coach-trainers identified are:

1) Intelligence preparation of the battlefield (IPB)/military decision-making process (MDMP). Many units have difficulty completing a thorough and proper IPB and MDMP within designated time constraints. S-2 intelligence sections often lack adequate IPB practice prior to the unit CTC rotation, causing issues during the rotation.

2) Establishing an intelligence architecture that can bring all systems online and incorporate the full capability of the intelligence enterprise. The S-2 must collaborate with the S-6 to ensure mutual understanding of the many requirements of an intelligence architecture and the network capabilities. Units should conduct multiple crawl, walk, and

run exercises that stress the set up and tear down, maintenance, and reestablishment of systems architectures.

3) Intelligence synchronization and collection management. Units show up without a deliberate plan, without standard operating procedures (SOPs) designating roles and responsibilities, and without proper collection plans that effectively employ organic assets while leveraging the intelligence enterprise to create a common intelligence picture. During unit exercises, units should test and challenge their SOPs, the synchronization of assets, and the collection management processes.

It takes engaged MI leaders in S-2 teams across the Army to assess their sections’ ability to accomplish the mission while determining the right way forward to make their team proficient and then retain that proficiency. Many of the skill-sets and competencies I discussed are examined in detail in the articles throughout this edition of MIPB. I encourage you to read them and incorporate their lessons into your teams. ✨

Always out Front – Army Strong!

Endnote

1. Stephen M.R. Covey, *The Speed of Trust: The One Thing that Changes Everything* (New York: Free Press, 2006)



CSM FORUM

by Command Sergeant Major Thomas J. Latter
U.S. Army Intelligence Center of Excellence



Brigade S-2: It's a Team, Not a Person

If you have heard MG Berrier speak, you have walked away with his acronym RPMI: Relationships, Partnerships, Mentorship, and Integration. He has condensed his 30 plus years of experience, the majority of which was as a "2" at every echelon from battalion to combatant command, down to RPMI—a recipe for success. None of this however, is about what he accomplished as an individual, but instead as a leader and integrator of a team. Our Army fights with brigade combat teams (BCTs). A BCT S-2 succeeds or fails as a team and that is how you need to train.

Whether you are the junior analyst in the S-2 or the ranking major in the brigade, no one individual can provide situational understanding to the commander 24/7 for a combat training center (CTC) rotation, let alone a nine-month deployment. Therefore, you need to build your team, hone your skills through sets and reps, and know the strengths and weaknesses of everyone around you. For the remainder of this article, when I refer to the S-2 I'm talking about the entire team, not an individual.

It is not enough for you to have a relationship with your brigade S-3 and the commander. Yes, they are important relationships, but beyond that, you need to build the brigade team. The S-2 needs to be a catalyst for integrating the staff to support the commander. The brigade S-2 needs to understand what the fires, engineer, and aviation liaisons need based on the types of operations the S-3 is providing the commander for courses of action. The liaisons as well as the rest of the staff need to understand what and how intelligence is there to support them.

You need to help the S-6 not only plan the best network based on terrain and weather, but help defend that network and tie into cyber electromagnetic activities to support the brigade commander's intent. When was the last time you discussed with the S-6 how the brigade is going to defend the network? During your military decision-making and intelligence preparation of the battlefield (IPB) processes, the S-2 needs to work with the S-6 and S-3 to propose non-kinetic interruption of the enemy's activities using electronic warfare and cyberspace to further the commander's intent.

Brigade S-2s need to develop partnerships with the expeditionary military intelligence brigade and military intel-

ligence brigade – (theater) for projected regionally aligned force (RAF) missions. These partnerships should be exercised when possible to understand all of the dependencies. Partnerships also need to extend to other government agencies depending upon the brigade's mission. Don't wait until you are deployed to reach out and establish working relationships, build partnerships early, and maintain them.

Mentorship needs to include seeking mentors and mentoring others. Brigade S-2s, should mentor military intelligence companies (MICOs) and subordinate battalion S-2s. They are the elements that will continue the battle if you are eliminated. They need to know why you are tasking in specific ways to support your commander. You also need to recognize that there may be expertise in the MICO that can mentor you. For example, learning about the latest Prophet system capabilities or upgrades to an unmanned aircraft system. You should be reaching up to the division or corps G-2 and looking for mentorship to understand how your brigade ties into sister brigades to support a division or corps in decisive action training environments, and finding out what assets may be pushed down to your brigade depending upon the mission.

Integration at the BCT S-2 is focused at the tactical and operational level. However, you need to think joint and multinational. If you have a RAF mission or deployment, are you integrated with special operations forces and coalition/NATO/host nation forces with whom you will be training and fighting? Do you understand their capabilities and limitations? Have you integrated that into your IPB process and built an understanding of dependencies you and they will have to meet commander's needs and support mission requirements? Integration needs to become the norm.

Relationships, Partnerships, Mentorship, and Integration (RPMI) are the elements of success for a "2" at any level, but are critical at the BCT. As the military intelligence professionals advising commanders within our BCTs, you need to be constantly learning more about your profession and passing on what you know. You need to know everything about friendly forces and enemy capabilities. That subject matter expertise needs to be available 24/7; therefore, more than one Soldier in the S-2 needs to be a subject matter expert. Never be a single point of failure, remember you are a team. 🌟

"Always Out Front and Army Strong!"

Technical Perspective

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



The vast majority of my career has been spent within an S-2, G-2, or J-2, with three of my most rewarding assignments being within a maneuver brigade. Just as MG Berrier has covered in this quarter's edition, I feel compelled to offer some observations and lessons learned to provoke further thought and attention.

Our Nation's wars are won at the strategic level but it's at the brigade combat team (BCT) where strategy transitions to decisive action. To match increasing operational complexities and near-peer adversaries within the decisive action environment, the Military Intelligence Corps generated increased capacity and capability within the BCT S-2. It remains incumbent upon the brigade S-2 "team" to successfully leverage the intelligence enterprise through the successful employment of the intelligence warfighting functions core competencies; intelligence synchronization, intelligence operations, and intelligence analysis.

Intelligence synchronization is the art of integrating information collection and intelligence analysis with operations to effectively and efficiently support decision making. Many S-2 sections have operated largely as independent, decentralized intelligence sections. This stovepipe mentality inadvertently creates significant roadblocks towards effective intelligence synchronization. Effective S-2s create live and virtual environments and supporting processes that operate in a multi-functional/multi-echelon domain to alleviate problems created by isolated S-2 sections and to enhance situational understanding. Innovative multi-faceted approaches allow intelligence leaders to build powerful teams capable of rapidly producing and coordinating intelligence across the enterprise. Through a collaborative network of adaptable people, processes, and technology, the BCT S-2 can flatten communications and achieve intelligence synchronization that is directly tied to the commander's decision-making process.

Intelligence operations are defined as tasks undertaken by military intelligence units and Soldiers to obtain information to satisfy validated requirements. The intent is to confirm or deny assumptions, invoke further analysis and discussion, and induce decisions by commanders. It is imperative that

intelligence professionals maintain a firm grasp of operations and intelligence techniques that are applied in both time and space. This requires relationships and integration with the BCT staff, particularly the S-3 and S-6, to ensure the intelligence operations are apportioned and resources maximized to answer commanders requirements. While many BCT S-2s assign a lieutenant to this challenging task, the position requires significant operational experience and the ability to leverage tools, processes, and personnel to transition concepts into reality.

Intelligence analysis is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production. Timely and accurate intelligence analysis serves as a critical foundation to mission planning and staff assumptions leading to mission success. It allows the commander and their staff to accurately visualize the operational environment, appropriately apportion forces, and proactively assess threats, terrain and weather, and civil considerations. Critical thinking, collaboration, and embracing ambiguity are cornerstones of effective intelligence analysis, significantly enhancing staff contributions to the analysis process. Critical thinking allows an analyst to adopt a disciplined, well-reasoned approach to their craft, increasing the possibility of reaching an unbiased assessment. It is important that analysts understand that they will often be required to work in an uncertain environment rife with unknowns. To successfully operate in this environment, it is essential that intelligence analysts develop excellent collaboration skills. Collaboration allows an analyst to develop a common appreciation for the battlefield environment and to ensure the community is working in harmony towards a common goal.

A highly effective BCT S-2 allows the commander and his staff to accurately visualize the current battlefield environment as well as anticipate enemy actions and reactions to friendly force actions. Understanding the roles and responsibilities of the BCT S-2, combined with a willingness to master the core competencies of the intelligence war-fighting function significantly enhances intelligence synchronization, and maximizes intelligence support to mission command. ✪

Always Out Front...Army Strong!

Observations from a Year as the Brigade S-2 Observer-Coach-Trainer at the Joint Readiness Training Center



by Major Nathan Adams

"The measure of success is not whether you have a tough problem to deal with, but whether it is the same problem you had last year."

—John Foster Dulles, U.S. Secretary of State 1953-1959

Introduction

In December 2015, the U.S. Army Forces Command (FORSCOM) G-2 generated an information paper for its leaders to understand brigade combat team (BCT) S-2 progression and development. The opening paragraph cited that in fiscal year 2015, 12 brigade-level S-2s (10 of which were in BCTs) were relieved or removed early from their positions. Further, the paper stated the following as the top three reasons for early removal: underdeveloped skills in synchronizing intelligence techniques and associated capabilities, limited experience as a maneuver battalion S-2, and inability to establish relationships with maneuver commanders and S-3s.¹ This ominous statistic contributed to the Army intelligence community's call to action to remedy failure of BCT S-2s, and resulted in the declaration of 2016 as the "Year of the BCT S-2" for the military intelligence (MI) corps. Actions included creating BCT S-2 courses at the corps G-2 level, charging combat training center (CTC) senior intelligence officers with "finding and fixing" the systemic problems with BCT S-2s, and compiling material by the FORSCOM G-2 for a handbook to guide BCT S-2s through the troubled waters of their new assignments.

The "Year of the BCT S-2" has now passed and we enter 2017 as the "Year of MI Readiness." I served for two years as a BCT S-2 during the period that drove last year's focus on improving BCT S-2 performance. My experience as an S-2 included various unit-level command post and field training exercises, a decisive action training environment (DATE) rotation at the Joint Readiness Training Center (JRTC), a mission readiness exercise at the Joint Multinational Readiness Center (JMRC), and an operational deployment to Kosovo. Following that, I served for more than a year as the BCT S-2 observer-coach-trainer (OCT) at JRTC.

Observations, Challenges, and Recommendations

In a little more than a year, I observed 11 rotations, conducted by 10 active duty brigades and 1 U.S. Army National

Guard brigade, at JRTC. The observations, common challenges, and recommendations in this article resulted from my combined experiences. They include topics that touch on S-2 leadership, intelligence preparation of the battlefield (IPB), information collection, intelligence architecture, intelligence synchronization, command post transitions, relationships, and asset management.

During the training rotations, each S-2 section had areas of strength and areas of weakness. Learning occurred regardless of performance, helping leaders maintain or at least approach their band of excellence as an organization. The 10 points in this article do not comprehensively account for all challenges a BCT S-2 faces. However, they do provide a start point from which a BCT S-2 can prepare for a new job, future training, or future deployments.

Brigade S-2s must be leaders in their staffs and listen to their commanders' needs. Gloomy anecdotes about my future as a BCT S-2 floated around before my first day on the job. While sobering to consider, I found that in the past year, the specter of imminent job loss did not loom quite as large as we in the Army intelligence community believed. Based on pure numbers, not a single S-2 in the 11 rotations I observed lost his or her job at JRTC.

Those BCT S-2s who conflicted the most with their commanders brought conflicts upon themselves by contradicting directly and publicly a directive, or by ignoring a commander's specific guidance. Additionally, BCT S-2s who isolated themselves from the rest of the staff hurt their credibility and that of their team by missing battle rhythm events or coming unprepared to contribute intelligence of value to meetings and planning sessions.

Key to successful performance by BCT S-2s is their ability to form workable relationships with their commanders, senior staff members (deputy commanding officer, executive officers, S-3s), and their peers in adjacent staff sections. Building credibility by providing timely (i.e., meets product deadlines) and relevant (i.e., does not simply regurgitate the news) intelligence and by being team players wins the day amid the rigors of a CTC rotation. It was clear from my observations that not every boss is easy to work for, but S-2s have a responsibility to develop and display social acumen and personal motivation. Technical competence of intelli-

gence systems and processes is an important trait for S-2s as well—it demonstrates credibility. However, sensitivity to organizational dynamics and commanders' needs are even more necessary in order to navigate the relationships BCT S-2s face.

Key, as well, is the S-2s' ability to be leaders within their sections. There was a difference in shift change briefs attended by S-2s compared to those not attended by S-2s. Presence matters and influences the performance of subordinates when they see that a meeting, product, or report has gained the attention of the S-2. The BCT S-2 can set the tone, empower subordinate leaders, and maintain high standards by receiving backbriefs or rehearsing presentations. Leadership matters internally as well—perhaps even more.

Standard operating procedures are essential and must be enforced. BCT S-2 sections require standard operating procedures (SOPs) in writing. I observed four units come to JRTC with nothing in hand, while seven units came with draft SOPs or a start point from which to improve. Easy cut-and-paste errors, such as unit designations (e.g., a sister brigade within the same division), were the first indicators demonstrating, in my opinion, that the S-2 had not taken the time to plan, staff, test, and refine SOPs. Additionally, regular references to counterinsurgency-type operations or garrison security procedures indicated that the SOPs I received were outdated and not ready for employment in a decisive action fight. When SOPs did exist, inadequate knowledge and enforcement caused problems during the stressful, tired days faced by the S-2 staff once a rotation started.

SOPs require proper dissemination. Another primary shortfall was the extent of dissemination across the unit. Dissemination of SOPs without an opportunity to use or rehearse fails to make them truly "standard" for all members of a BCT's intelligence warfighting function. A simple show of hands at the final after action review revealed that BCT S-2 sections arrived with members who had no knowledge of or copies of the SOPs. This incomplete distribution most often affected critical enablers from other installations, such as the aviation task force and sustainment battalion.

BCT SOPs must be available in writing as a reference when the "fog of

war" builds during a CTC rotation. Plans SOPs (PSOPs) focus on how a unit conducts planning. Tactical SOPs (TACSOPs) may describe battle drills, duty positions, and how a unit executes in the field. Mission command SOPs (MCSOPs) provide knowledge management practices; primary, alternate, contingency, and emergency (also called PACE) plans; and decision sequences. Each BCT S-2 section may contribute a portion to each of these SOPs and should ensure continuity of process across all standard documents for the BCT. However, they are each different products from warfighting function-specific SOPs, and therefore, should not replace the need for S-2 SOPs. SOPs provide an organized format for aligning processes and procedures against personnel and equipment. S-2s have to be efficient to distill the volume of information they encounter while assisting the BCT with achieving its mission.

For S-2s trying to develop SOPs, ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*, provides a great start place, as does the 1990s doctrinal classic, FM 34-8-2, *Intelligence Officer's Handbook* [not in the current Army doctrine inventory]. However, S-2 SOPs should inform members of a BCT's intelligence warfighting function how to execute intelligence operations. Key components of S-2 SOPs include duties and responsibilities by position, the intelligence battle rhythm, product contents and deadlines, standard report formats, intelligence discipline-specific processes, PACE plans for dissemination of products, command post transition processes, information collection, and supporting products to staff planning.

Leaders know, communicate, and enforce high but realistic standards. Effective leaders explain the standards that apply to their organizations and empower subordinates to enforce them.² All personnel within the BCT intelligence



A BCT S-2 provides a situation update to recently arrived members of his staff.

Photo by MAJ Nathan Adams

warfighting function must know the SOPs and their contents—or at least have them available to reference. To address the shortcomings observed in SOPs effectively, BCT S-2s must ensure SOPs are well developed, understood, published, and enforced. We must have the SOPs. We must know the SOPs. We must use the SOPs.

Complete the four steps of the IPB process—every time.

While painful to write, one of the most disconcerting trends I observed at JRTC was failure

to complete the four steps of the IPB process. During JRTC DATE rotations, brigade staffs generally have the chance to complete three planning cycles. When the intelligence staff comes to the mission analysis brief with an incomplete IPB process, it affects the entire staff's planning cycle. Two critical faults I observed included failure to conduct a thorough terrain analysis relevant to the mission profile and failure to evaluate all threat groups with their varying capabilities, agendas, and tactics.

Terrain analysis most often fell short when units assumed away the need for thorough terrain analysis either because they were out of practice with performing this analysis for combined arms maneuver operations or because leaders in their unit were "familiar" with JRTC from previous experiences. Terrain assessments did not consider the brigade's mission, and therefore ignored aspects of terrain that could affect the fight. Most often, this lack of consideration manifested itself in the discussion of key terrain. Years of deployed, counterinsurgency-centric operations have appropriately driven the Army to consider the population and population centers as "key" within a unit's area of operations. However, *key terrain* is any locality, or area, the seizure or retention of which affords a marked advantage to either combatant.³ For example, choosing a population center as a piece of "key terrain" in favor of a natural choke point during defensive or offensive maneuvers demonstrates a wholly incorrect understanding of terrain analysis. However, this was a common occurrence among the brigades I observed and was validated by unit leaders.

Evaluation of the threat by identifying threat characteristics (formerly order of battle) and developing doctrinal templates, threat templates, and threat models, consis-



A BCT S-2 conducts a radio update from his BCT's assault command post with subordinate unit S-2s.

tently fell short. The purpose of evaluating the threat is to understand how the threat can affect friendly operations. Although threat forces may conform to some of the fundamental principles of operations, these forces have obvious, as well as subtle, differences in how they approach situations.⁴ I observed threat analysis focusing on a single threat group instead of focusing on all potential threat actors in the environment, their interactions with one another, and their specific capabilities or interests within the unit area of operations. Overlooking one or multiple threat groups, in favor of the most apparent threat group, surprised BCTs when they encountered the multiple problems that more than one threat group could mount at a single time.

Before a CTC rotation, units can study, develop, and brief initial terrain and adversary products. BCT S-2s must fight against staff (and commander) complacency when preparing briefings and revisit terrain analysis upon receipt of their mission to ensure their original products and judgments match the mission profile. Within the BCT 2020 construct, the topographic team has repositioned from the engineer cell to the intelligence cell on the BCT staff. While the physical integration has occurred, BCT S-2s have more work to do to utilize topographic experts within their formation to produce effective terrain analysis. The same can be said of threat characteristics and doctrinal templates/models of threat behavior because they are part of generating intelligence knowledge as support to force generation.⁵ For guidance, a BCT S-2 staff should rely on the TC 7-100 series of publications on threat doctrine. When evaluating the threat, they should account for all threat actors and capabilities that appear in the operation order, not just the ones causing the most problems on a given day.

The event template (EVENTEMP) is a major challenge to overcome. In addition to IPB process shortcomings, I also observed failure to develop a concept of the threat in time and space with enemy decisions, phasing, and named areas of interest (NAIs) in the form of an EVENTEMP. *Event template* is a guide for collection planning that depicts the named areas of interest where activity, or its lack of activity, will indicate which course of action the adversary has adopted.⁶ In 11 rotations, I observed only one EVENTEMP for one operational phase that met the EVENTEMP doctrinal definition.

When S-2s fail to describe the threat in time and space through their IPB products, the operations staff will struggle to plan *when and where* to fight the enemy. This shortcoming compounds problems for the staff during course of action (COA) analysis, where they are unable to test the friendly COA in detail because the maneuver and timing of the enemy are unclear. Targeting working groups and meetings devolve into speculative sessions by the fires and effects cell when they do not have a clear picture of what enemy assets or capabilities are of greatest value to the threat in accomplishing its mission.

NAIs and decision points identified on the EVENTEMP with indicators to aid in determining which COA the enemy commander is implementing.⁷ When the BCT S-2 has an assessment of the enemy in the form of an EVENTEMP, the BCT can proactively anticipate, identify, target, and neutralize the threat to achieve the friendly mission. It also assists the BCT in adjusting decisions or reevaluating the COA because of a change on the battlefield. While ultimately an assessment, the EVENTEMP provides the operations and targeting staffs with a start point for planning the friendly operation. Without an EVENTEMP, the staff reacts instinctively to what the enemy might do. They will ineffectively allocate resources because they are maneuvering blind.

Information collection management is more than just building a collection synchronization matrix. The two key shortcomings I observed regarding information collection are 1) failure to operationalize information collection, and 2) failure to appropriately resource the information collection section. Information collection managers, a position filled by a lieutenant in nine of the rotations I observed, consistently struggle to gather all of the tools, orders, and personnel necessary to accomplish the mission.



Photo by MAJ Nathan Adams

A BCT S-2 and MICO team conduct a synchronization meeting with subordinate unit S-2s.

Completing the IPB process correctly can yield enemy situation templates and threat COA sketches, its units, and key assets arrayed on the specific terrain. I view the EVENTEMP as the culminating product of the IPB process. It comprises time-phase lines, NAIs, and enemy decision points. It provides areas where information collection assets can focus on to determine the enemy's COA. A good EVENTEMP becomes a product the BCT commander carries around and the current operations staff posts in its cell because of its predictive quality. The EVENTEMP is (i.e., should be) always accompanied by an event matrix—a table associating the

Information collection management is a complex process and requires more than just a single junior officer. These officers, though hard working, do not always have the depth of operations knowledge to make their information collection concepts into operational realities. Understanding *when and how* to participate in events, such as the operations synchronization meeting, and incorporating collection tasks into a daily order were often beyond the information collection manager's level of experience. BCT S-2s, who have additional duties that occupy their time, do not allocate the time they need to follow up on the operational aspect of information collection. Too often, they release the operations staff by not getting their input as to what is an operational allocation of BCT assets. Failure to use information collection planning as an integrating process for multiple BCT staff members risks wasting precious resources or missing opportunities.

Tasking information collection in mission orders is a viable way for a BCT headquarters to obtain the information required to answer priority intelligence requirements (PIRs). Planning for how the BCT will process, exploit, and disseminate



A BCT information collection manager updating information collection plan in tactical command post.

nate collected information is critical to close the cycle in the assess activity of operations. However, when the BCT staff overlooks these activities, the information collection plan terminates by being conceptual at best.

The BCT S-2 and BCT staff must also look at how they resource the information collection management team. This team must maintain the running estimates of all potential sensors (scouts, rotary wing aircraft, civil affairs teams, etc.) available across the battlefield to answer PIRs successfully. This requires more than information collection planning; it also requires the information collection manager to thoroughly understand at the brigade level the functionality and capabilities of maneuver as well as component systems of the intelligence architecture. This is potentially more information than a single lieutenant can monitor during the course of 14 days at a CTC rotation. However, there is no designated information collection management team within the BCT modified table of organization and equipment (MTOE).

Units that have collected information successfully have sacrificed personnel from within the MTOE to build a team of at least three to four personnel to maintain 24 hours of operations. The team participates in planning while fielding and submitting requests for information to higher and subordinate units. However, this team cannot be solely a functional team; it must integrate with other members and processes of the BCT staff.

Intelligence synchronization must be a deliberate operation for the BCT intelligence community. Intelligence synchronization is necessary in two forms within the BCT intelligence community. The first form is internal synchronization that occurs among members of the BCT S-2 staff.

The temptation of the various cells within a BCT S-2 section (S-2X, signals intelligence, targeting, collection, current operations, geospatial intelligence, fusion, etc.) is to focus internally on the urgent projects of the moment that every intelligence staff faces during a CTC rotation. However, S-2 sections that take the time to hold shift change briefs with knowledgeable representatives from each subsection increase information sharing and cross talk that benefits the entire staff. When all elements are united to share their updates, members of one subsection often discover other team members who have information vital to their mission. These meetings prove even more valuable

when the actual S-2s attend and share their experiences, perspectives, and priorities gained from interacting with the commander, staff, and subordinate units.

The second form of intelligence synchronization must occur between the S-2 and intelligence staffs of the subordinate units of the task force. The BCT S-2 owes leaders across all echelons a consolidated assessment of the enemy across the area of operations, information collection assets available and planned for the next period of operations, and critical reporting affecting the entire team. Subordinate units owe bottom-up assessments and feedback on their portion of the battlefield, their information collection needs, and battle damage assessments to help the BCT S-2 understand the enemy.

Critical to both of these intelligence synchronization forms is implementation of a standardized meeting agenda delineating each participant's expected contributions, along with a logical sequence on which the meeting will build. Ultimately, the BCT S-2 team will have outputs they can integrate into the BCT's operations process and battle rhythm events. Without a plan, what should be a professional gathering turns into an unstructured, request for information answer session that falls short of achieving a shared understanding of the enemy. When members of the BCT intelligence community participate in such a forum and discover its inefficiency, they stop attending after two to three unsuccessful meetings. During a decisive action rotation there is little time available to waste, and subordinate units especially find that engaging with the BCT S-2 does not help them when there is no clear output of a synchronization meeting. Whether using upper tactical Internet or a radio, a method (agenda) and end state (outputs) help focus intelligence synchronization.

Another requirement for effective synchronization is a clear plan that directs the timing, frequency, and medium for synchronization to occur. All participants from within the BCT's intelligence community must understand when and by what means synchronization will occur. It is possible that the means could change daily; therefore, a method of updating the changes is necessary. An agenda to which the intelligence community rigorously adheres will help all parties overcome inevitable changes in venue—face-to-face, radio, or digitally distributed. Intelligence synchronization is critical for helping BCT S-2s to understand what subordinate units are seeing and to provide top-down context. This process does not happen organically when faced with the adaptive, uncertain CTC environment—it requires a plan.

Dedicate effort to planning mission-command node transitions. Conducting an operation while transitioning mission command nodes is always difficult, and intelligence operations at the BCT level during this transition are no exception. During joint forcible entry operations at JRTC, BCT S-2 sections are limited in the number of personnel and equipment they can initially insert. I have often seen some combination of the S-2, an assistant officer, and radio-telephone operator/analysts as part of initial entry command posts. Depending on the communications equipment available, this team may be capable of battle tracking and have limited information collection management in the first 24 hours of an operation. If they have excellent digital communications with a support element focused on the mission, the team may be able to operate for up to 72 hours. However, at some point, the support element disconnects and moves forward to meet the BCT leadership. The small team is left to run the entirety of the operations for the BCT intelligence community while waiting for the rest of the brigade intelligence support element (BISE) personnel to arrive and establish.

I observed the biggest breakdowns in the following areas: maintaining the intelligence battle rhythm, support to planning, and the ability to answer the commander's PIRs. When the intelligence battle rhythm starts poorly due to limited communications, or the forward S-2 team is overtasked, it is incredibly difficult to recover. Planning efforts and operations will continue, however, the three-to-five person BCT S-2 team that initially deploys will not have the manpower to perform in-depth BCT-level planning. Limited communications architecture may prevent the team from reaching back to support elements in safe-havens to relay the forward team's planning needs. While the information collection plan may be established before initial entry, it changes as the battlefield changes, and the forward S-2

team may not have the ability to analyze collected information coherently to answer the commander's PIRs. In many cases, it reduces S-2 sections to battle tracking and making uneducated guesses based on a combination of old information and new battlefield reports.

S-2 staffs often underestimated the number of tasks their forward elements needed to accomplish, and failed to appreciate the limited communications architecture available to communicate with the BISE. Some of this was due to the lack of MTOE-authorized communications equipment for the S-2 sections. This forced them to share limited resources with other staff sections. Yet, there was also the issue of failing to overcome personnel shortages forward by clearly delegating responsibilities to the supporting elements, specifically the remainder of the BISE.

S-2 sections must plan their transition fully. They must be realistic about how long the transition might take, the equipment needed, and the personnel required to accomplish S-2 section functions in a limited or distributed capacity for several days. If a reachback concept is in the plan, the entire intelligence community throughout the BCT must understand which node is responsible for various operations,



A BCT assistant S-2 briefs his brigade commander.

Photo by MAJ Nathan Adams

including mission planning, warfighting function synchronization, and information collection planning. These actions can and should be part of BCT S-2 SOPs. Identifying a person or team to manage the flow of information, additional personnel, and equipment from the staging base to the forward elements helps shepherd the transition from start to finish.

The Distributed Common Ground System-Army can work—if you use it. One question BCT S-2s commonly ask is, “Does the Distributed Common Ground System-Army (DCGS-A) work at JRTC?” While the short answer is “yes,” much like intelligence synchronization, it takes coordination, standards, and a plan to work. Of the 11 brigades I observed, 10 successfully established their DCGS-A and Intelligence Fusion Server on their tactical networks, and 11 were able to receive data from the Data Distribution Server or Publish and Subscribe Server with the Joint Task Force-21 (JTF-21) Analysis and Control Element.⁸ However, none of these units successfully pushed any of their data to JTF-21.

S-2 sections, despite having a number of tools available on DCGS-A, still reverted to drawing icons in PowerPoint on the screen capture of a map. Those units that developed their threat graphics in DCGS-A were able to share them internally with command post of the future operators in the S-2 current operations section—I believe to both decision and system proficiency. Units and their leaders who use and train on the system provided to support BCT efforts (such as mission planning) will see positive results from DCGS-A. It saves time, is more easily manipulated (once the entities exist in the threat entities database), and is less bandwidth-intensive in a constrained communications environment.

DCGS-A becomes a solution when there is an intentional effort to share data, and intelligence leaders enforce using it as the primary intelligence weapon system of the intelligence warfighting function. The architecture must be discussed, planned, practiced, refined, and ready before JRTC. BCT S-2s must take deliberate interest in understanding DCGS-A’s technical components and its current proficiency,

as well as in training their personnel to use the system for daily operations, unit synchronization, and planning support.

The BCT S2 and military intelligence company relationship is the heart of the intelligence community. The critical relationship in the BCT intelligence community is the one between the BCT S-2 and the MI company (MICO). This relationship sets the tone for how intelligence personnel at all levels will interact with one another and can have exceptional or detrimental effects to

the entire intelligence effort. A MICO commander and BCT S-2 at odds with one another may not manifest their differences in public. Instead, their differences are often manifested through proxies of platoon leaders and NCOs who hold onto their Soldiers and separate intelligence processing efforts. This results in duplicate, ineffective work and creates unclear chains of command, especially when information collection enablers are tasked out across the BCT. A failed relationship is also apparent to battalion S-2s when the BCT S-2 communicates one thing and the MICO executes something completely different.

The biggest source of tension stems from the desire of MICO and BCT personnel to retain their garrison parent-unit identity. They fail to see themselves and their fellow



A BCT assault command post at JRTC.

For data *sharing* to occur, which is what DCGS-A intends for the Army intelligence community, a two-way exchange must occur. Units arrived at JRTC with some team members familiar with mapping, threat entities, and link analysis tools on DCGS-A. However, the understanding of or incorporation into SOPs of product dissemination within DCGS-A was a common shortfall, as indicated by the number of units that successfully shared with JTF-21. Most units did maintain an intelligence shared drive on their Intelligence Fusion Server at the BCT level, but sharing overlays or products via the Publish and Subscribe Server and Data Distribution Server was not the common practice.

Only two units in the course of the last year used DCGS-A applications as the production method for IPB products.

intelligence professionals as members of a single community that will either succeed or fail together. It is a problem when BCT S-2 sections criticize the MICO for “never training with us,” and when MICO personnel focus on their “company business” at the exclusion of the other intelligence team members occupying the same workspace. S-2s who dismiss the MICO as “too attached to their parent battalion” are just as wrong as MICO commanders who concern themselves solely with the administrative and logistical minutiae of running a company. Each fails to see how the entire intelligence community can help the brigade commander achieve the unit’s mission.

The BCT S-2 and MICO command team are responsible for making this relationship work. The best intelligence teams throw the BCT S-2’s and MICO’s identities out the window and allow individual team members to see themselves as part of the brigade’s intelligence community holistically. The MICO must task-organize with the BCT intelligence cell to form the BISE.⁹ It is critical that both the S-2 and MICO commander work on this relationship in the context of a wider network of relationships, including the brigade engineer battalion commander. One positive trend I have observed is engineer commanders being less likely to exercise direct control of the MICO during CTC rotations. Instead—and many would argue appropriately—they allowed the MICO to operate as a brigade-enabling element. MICO commanders are conceivably the most experienced company-grade

intelligence officers in the BCT. As such, a MICO commander who is present and proactive, taking deliberate steps to understand and assist the BCT’s plan, can advise on emplacement of the company’s information collection assets across the battlefield to answer the commander’s PIRs.

Track organic information collection assets and tasks. Battle tracking of information collection assets and follow up to ensure completion of information collection tasks has been a consistent shortfall. The BCT S-2 sections I observed increased their planned employment of organic information collection enablers, such as human intelligence and signals intelligence collection teams from the MICO, to answer PIRs. Some BCT S-2 sections went so far as to incorporate cavalry squadrons and aviation task forces into information collection plans. However, I observed a disconnect between the information collection manager, the BCT S-2, the MICO chain of command, and the information collection elements in understanding what information collection the BCT is actually capable of doing. I did not observe operations staffs displaying a vested interest in the status of the information collection assets beyond the BCT’s unmanned aircraft systems—the most visible manifestation of information collection for the BCT. Failure to track all information collection assets as combat enablers and to understand fully their capabilities, results in mismanagement or exclusion of the limited but effective information collection capabilities that a BCT possesses.



A BCT S-2 works with fellow staff members to complete a synchronization matrix.

The BCT S-2 section, in conjunction with the MICO headquarters, has a vested interest in understanding information collection assets' location on the battlefield and whether their positioning is appropriate to meet information requirements. The S-2 current operations staff can assist the battle captain in tracking information collection assets on the battlefield in real time—it is not enough for the S-2 and MICO simply to know the assets' location on the battlefield. They must know capabilities, shortfalls, and equipment status, especially if they are planning to commit an organic information collection asset to a specific or new mission. Some of this dissonance can be resolved during daily internal synchronization meetings or by validating the plan during an information collection rehearsal before mission execution. As a staff leader, the S-2 can use some friendly force information requirements to keep the running status up to date with existing friendly intelligence capabilities.

Conclusion

The job of the BCT intelligence team is a combination of complexity, challenge, and reward. Staffs that consider these complexities, challenges, and rewards in their SOPs, practice them in their pre-deployment training, and implement them as part of their operation plans are more likely to achieve intelligence synchronization and avoid the pitfalls faced by intelligence teams at previous CTC rotations. The value of deliberate and thorough plans and rehearsed standardized procedures cannot be overstated. They aid in overcoming the confusion and challenges presented by the long days, austere environments, and unanticipated actions of opposing forces—whether simulated or real. Having plans

and standards and practicing them instill confidence and enhance performance through the exercise of a familiar system rather than reinventing or hastily cobbling together a new process in the midst of crisis. As intelligence professionals, we must remember that substandard performance or possible job loss at a training center is infinitely of less concern than the potential loss of human life when our systems and processes fail us in combat. Ultimately, BCT S-2s must consider this in leading their teams to plan, prepare, and execute the intelligence mission when the call to action finally comes. ✨

Endnotes

1. Christine Ngai, "Developing FORSCOM (FC) Brigade Combat Team (BCT) S2." (information Paper, U.S. Forces Command G-2, 1 December 2015).
2. U. S. Army Doctrinal Reference Publication (ADRP) 6-22, *Army Leadership*, (Washington, DC: U.S. Government Printing Office [GPO], 1 August 2012), 6-5.
3. Joint Publication (JP) 2-01.3, *Intelligence Preparation of the Operational Environment*, (Washington, DC: U.S. GPO, 21 May 2014), GL-6.
4. U.S. Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*, (Washington, DC: U.S. GPO, 26 March 2015).
5. Ibid.
6. JP 2-01.3, *Intelligence Preparation of the Operational Environment*, GL-6.
7. ATP 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*, 6-15.
8. JTF-21 is the fictitious division-level headquarters in a JRTC rotation to which BCTs are subordinate.
9. ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*, (Washington, DC: U.S. GPO, 10 February 2015), 2-5.

MAJ Nathan Adams serves at the Joint Readiness Training Center on the Brigade Mission Command Task Force as an observer-coach-trainer. He was previously the S-2 for 4th Brigade Combat Team, 25th Infantry Division (Airborne), Joint Base Elmendorf-Richardson, Alaska, during which he participated in training rotations at Joint Readiness Training Center and Joint Multinational Readiness Center. He deployed with elements of 4-25 to Kosovo as the S-2 for Multinational Battle Group - East. He holds a master of science in strategic intelligence from the National Intelligence University.

I would like to thank my leaders and teammates in the intelligence warfighting function and brigade mission command community of observer-coach-trainers at Joint Readiness Training Center (JRTC). Their editorial review, perspective, and data contributions have made this article possible. I am indebted to them for their mentorship, experience, and advice in ensuring world-class training for the intelligence professionals who come to JRTC.

The Brigade Combat Team Intelligence Staff Officer Course



by Major Jason Buchanan and Lieutenant Colonel Anthony Covert

Introduction

As the “Year of the BCT S-2” ends and the “Year of Intelligence Readiness” begins the Military Intelligence (MI) Corps witnessed several initiatives to improve performance at the tactical level. The MI Corps identified the need to provide additional preparation to all leaders at the tactical level to produce successful brigade combat team (BCT), functional brigade, and battalion S-2s. Trends at combat training center (CTC) rotations indicated that MI S-2s lack the knowledge to establish and maintain brigade intelligence system architecture and to communicate on a complex threat environment.

One initiative I Corps created to help remedy shortfalls in MI training until institutional fixes are in place was to establish a 5-Day BCT S-2 course. I Corps established the BCT S-2 course to provide additional training for current and future MI leaders at brigade and below that deepens their understanding of the intelligence warfighting function (IWFF) core competencies, and emphasizes that only through holistic efforts by the entire intelligence team is success achieved. I Corps’ goals are to provide tailored training to IWFF leaders enabling successful intelligence operations, and providing the tools necessary to be successful intelligence leaders. To achieve these goals, the BCT S-2 course focuses training on five areas of emphasis including —

- ◆ Command Relationships and the Military Decision-making Process (MDMP)
- ◆ BCT Intelligence and Electronic Warfare (IEW) Systems and Mission Command Architecture
- ◆ BCT IWFF Operations
- ◆ Collection, Knowledge, and Training Management
- ◆ MI Certification Requirements

This course is now on its third iteration with the most recent course hosting MI leaders from the following organizations:

- ◆ 7th Infantry Division
- ◆ 25th Infantry Division
- ◆ U.S. Army Alaska
- ◆ 10th Mountain Division

- ◆ 101st Airborne Division (Air Assault)
- ◆ U.S. Army National Guard
- ◆ Several Joint Base Lewis-McChord (JBLM) tenant units

Course Structure

The I Corps BCT S-2 course mentors MI leaders on MDMP from an operations perspective, training on the separate intelligence disciplines and how to merge information into all source intelligence, as well as leverage expeditionary military intelligence brigade (EMIB) capabilities to enable more effective intelligence operations. By the end of the week, students have learned about BCT information management, how to manage intelligence training to ensure effective intelligence readiness within their unit, as well as received an overview on the 180-day training model and intelligence certification requirements for CTC rotations. The weeklong BCT S-2 course includes a series of focused classes, practical exercises, subject matter expert led round table discussions, and key leader engagements (KLE). The intent is to ensure all intelligence leaders understand their roles and responsibilities at the BCT, brigade, and battalion level and then transfer that knowledge to the institutional domain.

Command Relationships and Military Decisionmaking Process. The latest iteration of the I Corps BCT S-2 course started with several KLEs from guest speakers throughout JBLM and across the intelligence enterprise. These guest speakers included —

- ◆ I Corps G-2
- ◆ 201st Expeditionary Military Intelligence Brigade commander
- ◆ 1st Stryker Brigade Combat Team, 2nd Infantry Division commander
- ◆ 1st Stryker Brigade Combat Team, 2nd Infantry Division S-2
- ◆ 1st Stryker Brigade Combat Team, 2nd Infantry Division S-3
- ◆ 7th Infantry Division commander

These speakers discussed a variety of topics such as command relationships, the S-2’s relationship within the staff

and brigade, and various other leadership topics focused around the IWfF and the S-2 role. These KLE's set the stage for the rest of the course highlighting senior leader's expectations from MI professionals.

The opening day also drew on resources from across JBLM including the sitting 2nd Stryker Brigade Combat Team, 2nd Infantry Division S-3 to speak not just on MDMP, but also on his experiences with the IWfF and where he thought S-2s could influence MDMP and the BCT. One key theme that resonated throughout the course was the need for MI professionals to build relationships across all staff sections. The 2nd Stryker Brigade Combat Team S-3 highlighted this throughout his brief, and then the 7th Infantry Division G-6 maintained that theme during his brief on S-2/S-6 integration at the brigade level. One common theme from CTC rotations is that MI system architectures are established too late, or not at all. The G-6 focused on the need for S-2s to become experts in both the craft of intelligence preparation of the battlefield (IPB), but also their systems and their connectivity. This expertise can come from both prior planning between the S-2 and S-6, but also through establishing a good relationship with the S-6. Many briefers throughout the course recognized the need for MI professionals to step outside of their compartmented facilities and interact with other key members of the staff.

BCT IEW Systems and Architecture. The architecture theme discussed on Day 1 by the 7th Infantry Division G-6 carried over into Day 2 with detailed discussion of BCT IEW systems and architecture. The focused discussion was facilitated by senior military occupational specialty (MOS) 353T — intelligence and electronic warfare maintenance technicians and MOS 350F — all source intelligence technicians, from across JBLM. Instruction throughout most of the morning included discussions on the Tactical Ground Station and the Distributed Common Ground System-Army, the Global Broadcast Service, Geospatial Intelligence Workstation, One System Remote Video Terminal, Prophet, and Trojan SPIRIT. Subject matter experts from across JBLM rotated through each class and remained available for additional discussion to facilitate learning. The afternoon portion of this training continued from the morning with MI systems architecture

connection to the BCT Army Battle Command System suite. Discussion included topics on best practices from leader's previous experiences in combat and recent CTC rotations.

Day 1 – 17 Oct	Day 2 – 18 Oct	Day 3 – 19 Oct	Day 4 – 20 Oct	Day 5 – 21 Oct
Command Relationships & MDMP*	BCT IEW Systems and Architecture	BCT IWfF Ops, CM and R&S, INT Support to Targeting	Fighting BCT ISR, EMIB and Higher INT Ops and Support*	Training Management, MI Cert Requirements
<ul style="list-style-type: none"> 0800: Inprocessing 0900-0930: Opening Remarks (Corps G2) 0930-1030: CMD Relationships (1-2 SBCT CDR) 1045-1145: S2 in BDE MDMP Process (2-2 SBCT S3) 1145-1300: Lunch 1330-1430: 7th ID CG 1430-1530: S2/S6 Network Integration (7th ID G6) 1530-1630: Mission Command Systems (7th ID G6 & G2) 1700-1900: No host Ice Breaker, Sam Adams Club 	<ul style="list-style-type: none"> 0900-0930: 35T/353T Support (Senior 353T) 0930-1045: MI Systems: DCGS-A (Senior 353T) 1100-1130: MI Systems: TGS, GBS, OSRVT, GWS, Prophet, TS (Senior 353T) 1130-1300: Lunch 1300-1400: MI Systems: TGS, GBS, OSRVT, GWS, Prophet, TS (cont) (Senior 353T) 1415-1615: BCT INT Architecture (Various G2 ACE leadership) 	<ul style="list-style-type: none"> 0845: Intro, G2 0900-1000: MG Berrier, CG USAICoE VTC 1015-1100: Employing BCT HUMINT/CI (Senior 351M) 1100-1145: Employing BCT GEOINT 1145-1230: Employing BCT SIGINT 1230-1315: Employing BCT All Source Operations 1315: Lunch delivered 1315-1400: MICO & BISE Org, Employment and Integration w/ BCT S2 (Panel, 7th ID G2) 1400-1445: BCT CM 1445-1515: R&S Planning 1515-1545: Intel Support to Targeting 1545-1700: Fighting ISR – How to Sync BCT ISR and Win (panel, 7th ID G2) 	<ul style="list-style-type: none"> 0730-0830: Successful BCT Trends at JRTC (JRTC G2) 0900-1000: Successful BCT Trends at NTC (NTC G2) 1015-1100: EMIB Ops & Enabling Capabilities (201st EMIB CDR) 1100-1130: SWO 1130-1300: Lunch 1300-1400: Corps ACE Ops and Enabling Capabilities 1415-1530: MICO EXPO (1/2 SBCT, MICO CDR) 1530-UTC: BCT IWfF TACSOP & SOP Review and Return 	<ul style="list-style-type: none"> 0900-1000: IWfF Sustainable Readiness, IRCOP, Maint Support 1015-1100: FY 17 CTG 1100-1200: Training Management & IWfF Training Enablers* 1200-1330: Lunch 1330-1430: MI Gunnery and a 365-day IWfF SRM Model 1430-1530: How to Plan and Conduct Your BCT MI Cert Exercise 1530-1600: Closing Remarks (G2)
* BCT IWfF TACSOP & SOP Turn-in (7 th ID G2)			VIP Schedule: 1300-1345: MICO EXPO 1400-1430: IWfF Readiness, CTG, SRM 1430-1500: IC tour	* Foundry, MTC, IEWTPT, and JBLM LCC

UNCLASSIFIED

BCT S-2 Course – Oct 2016.

BCT IWfF Operations, Collection Management and Reconnaissance and Surveillance, and Intelligence Support to Targeting. Day 3 started with a keynote address from the USAICoE commander, discussing both his team's efforts to improve readiness of MI professionals and his experiences and recommendations for future MI leaders in the BCT. Day 3 focused instruction on the BCT collectors including:

- ◆ Employment of counterintelligence, human intelligence, and signals intelligence assets.
- ◆ All-source intelligence operations and best practices.
- ◆ Collection management.
- ◆ Reconnaissance and surveillance planning.
- ◆ Intelligence support to targeting.

The 7th Infantry Division G-2 included two panels into the instruction. One panel comprised previously successful BCT S-2s and MI company (MICO) leadership. The second panel focused on the topic "Fighting Intelligence, Surveillance, and Reconnaissance (ISR)," and how to synchronize information collection within the BCT. This panel included the 2nd Stryker Brigade Combat Team, 2nd Infantry Division cavalry squadron commander and allowed an open forum for discussion on several themes including collection management, task organization of the MICO, and employment of collection assets.

Fighting BCT ISR; EMIB and Higher Intelligence Operations and Support. Day 4 continued with the "Fighting ISR" theme starting with video teleconferences from the senior intel-

ligence officers (SIOs) at the National Training Center and Joint Readiness Training Center. Both discussions covered rotational observations and lessons learned from the BCTs IWfF including MICO integration, intelligence architecture, and ISR management. Discussions from each SIO on their observations and recommendations proved extremely valuable to the students with each presentation going over the time allocated.

The day also included a presentation from the 201st Expeditionary Military Intelligence Brigade commander on EMIB operations and enabling capabilities. Students developed a deeper understanding of the EMIB organizational structure leading to an understanding of how they could collaborate on training opportunities and operational support. Instruction concluded with a tour of the I Corps analysis and control element (ACE) and MICO assets. The tour allowed students to interact with Soldiers of the 1st Stryker Brigade Combat Team, 2nd Infantry Division MICO that establish the BCT's brigade intelligence support element and all of its assets. MICO leaders gave presentations about their equipment describing capabilities, limitations, and each systems role in establishing the tactical intelligence architecture. The I Corps ACE tour facilitated students understanding of each section's current operations and highlighted unit-supporting capabilities.

Training Management, Military Intelligence Certification Requirements. The final day of the BCT S-2 course focused students on training management and MI certification for both system and personnel readiness across the BCT IWfF. Topics included instruction on IWfF sustainable readiness, the use of the intelligence readiness common operating picture, and the multitude of resources for maintenance support. A Foundry presentation helped students understand collective training and the resources available to support intelligence certification and exercises. Lastly, students received the latest briefing on MI Gunnery including presentation on the gates and tables of MI Gunnery.

Command and General Staff College Initiative

This initiative continues with collaboration from both the U.S. Forces Command and the U.S. Army Intelligence Center of Excellence (USAICoE) to establish a BCT S-2 course at Fort Leavenworth, Kansas, for MI students attending the Command and General Staff College (CGSC). The effort at Fort Leavenworth includes a preparatory course prior to the start of CGSC as well as a BCT S-2 course conducted at the conclusion of the school year. The preparatory course reviews MDMP/IPB fundamentals and near-peer decisive action threat tactics. This effort strengthens MI professionals knowledge on staff processes and integration as well as a review of current threat doctrine. The design of the two-week BCT S-2 course is to enhance the skills of BCT intelligence professionals based on the foundation established by the CGSC curriculum. This course examines advanced applications of intelligence support at the BCT and covers intelligence systems, planning, and operations as part of a collaborative and distributed intelligence enterprise supporting tactical level organizations.

Conclusion

The BCT S-2 course is not a new concept and was successful in the past. With the renewed focus on decisive action against near-peer competitors and the continued growth of BCT capabilities, the need to establish the course again was apparent. The full team effort across the MI Corps has increased focus at the tactical level to ensure successful intelligence support at the BCT. I Corps, along with other corps and divisions, anticipates continued execution of the BCT S-2 courses at their home stations. This effort will be complemented with the new BCT S-2 Course at CGSC, which together will build the necessary expertise for MI success at the tactical level in the future. 🌟

MAJ Buchanan currently serves as the I Corps G-2, deputy director of training. His assignments include battalion S-3 and executive officer of 2nd Military Intelligence Battalion, battalion S-2, and military intelligence company commander.

LTC AJ Covert recently commanded the 303rd Military Intelligence Battalion, Fort Hood, Texas and currently serves as the senior intelligence advisor at the Command and General Staff College. Over his career, he has served as the J-2/S-2 in airborne and special operations units, chief, Joint Intelligence Support Element, an observer controller at the Joint Readiness Training Center, and deployed seven times.



by Chief Warrant Officer Two David Pierce

Introduction

Given the complexities of the relationship between the brigade combat team (BCT) S-2 and the military intelligence company (MICO), integration can be tenuous if not carefully planned and executed. Army Techniques Publication (ATP) 2-19.4, *Brigade Combat Team Intelligence Techniques* states, "The MI company provides the majority of intelligence personnel to the BCT to collect, analyze, and disseminate intelligence."¹ Without the collective intelligence capabilities the MICO brings to the BCT, the BCT's intelligence warfighting function (IWfF) would be operationally ineffective at best. Understanding the options for task organizing the MICO and integrating its various elements into the BCT S-2 cannot be overemphasized and should be a top priority as the BCT's mission success depends on it. This article will discuss the two primary ways in which, from my observation, a BCT and MICO can ensure seamless integration – fostering relationships, the more important of the two, and early integration.

Relationships

The collective success or failure of many organizations, not just in the military, is traceable back to relationships – good, bad, or indifferent. The intelligence structure of the BCT is designed with flexibility in order to support a wide range of missions. However, this flexible structure at the same time creates unique challenges for the relationship between the BCT and the MICO. In most military organizations, it is quite clear who is in charge and how orders move down the ranks. However, the MICO, though the primary intelligence provider for the BCT does not report to the BCT S-2, they report through the brigade engineer battalion (BEB) chain of command. In a perfect world, the MICO priorities would align with the BEB, which would in turn align with the BCT — however, many times this does not turn out to be the case. The command's leadership is responsible for ensuring the relationship aspect of integration is therefore a priority—lynchpins are the relationships between the BCT S-2

and MICO commander, the BCT S-2 and BEB commander, and the BCT S-2 and BEB S-3. The overall effectiveness of maintaining productive cohesion within the organization is dependent upon the success of these relationships.

The BCT S-2, as the senior intelligence representative to the BCT commander, sets the stage for ensuring all intelligence elements are integrating effectively to meet the BCT commander's intent. They must ensure processes and procedures are in place which allow the BEB and MICO to have input and feedback into home-station operations and training, while also understanding the outside requirements being leveraged against the BEB which may cause friction. A good BCT S-2 is able to communicate effectively the BCT commander's intent for the IWfF, while incorporating the BEB and MICO's input to manage, assess, and implement the full capabilities of the IWfF in any environment or scenario.

The MICO commander has to understand their responsibilities within the BCT construct as they command the majority of the collective BCT IWfF workforce. The primary mission of the MICO is to support the BCT commander's intent – despite other priorities that will arise within the BEB. A successful MICO commander is able to balance BEB requirements, while also allowing sufficient time and resources to respond to the BCT S-2's guidance and intent for the IWfF as a whole. Overall success hinges on the ability for the MICO to not only function as a company within the BEB, but ultimately to understand and meet the BCT commander's objectives and intent for the IWfF through the relationship they establish and maintain with the BCT S-2.


The BEB commander and BEB S-3 both play important roles in successful integration of the MICO and BCT S-2. The BEB commander must fully understand the BCT commander's intent for the IWfF and be able to facilitate and direct the MICO in accordance with those objectives. The BEB S-3, similarly, must understand the mission and purpose of the MICO and be willing to dialogue often with the BCT S-2 on proper training, integration, and support the MICO will provide the BCT. When the BEB commander and

S-3 have a stake in the success of the IWfF, as per the BCT commander's directives and intent, success becomes more achievable.

Early Integration

The IWfF cannot expect to be successful during operations or training without making an effort at early holistic integration. If the BCT S-2 and MICO are not training, talking, and operating together on a daily basis the concept of integration is inherently flawed from its inception. The responsibility for this integration starts with the BCT S-2 – ensuring that training incorporates all enablers of the IWfF and organic battalion S-2s. Fundamental to integration is ensuring the “team” concept is instilled within all aspects of the IWfF and that positive ideology flows down throughout the respective organizations. Though the BCT S-2 accepts initial responsibility for this tenet of success, it inherently has secondary responsibilities that fall on the BEB and MICO leadership. The MICO must want and strive to integrate with the BCT and not operate separately until an operation or exercise begins. Again, without integration from the start, true unity of effort will not occur, leaving the BCT without its full IWfF capability during operations and exercises.

Conclusion

The BCT IWfF is only as good as its weakest link – it cannot operate in a decisive action environment, or any environment for that matter, lacking true unity of effort between its organizations. The BCT S-2, MICO, and BEB must all understand and work together to achieve the BCT commander's intent – understanding the inherent organizational roles and responsibilities of each. Integrating daily training and dialogue, though at times tedious and time consuming have to remain a priority. Without fully embracing the two tenets of success – fostering relationships and early integration – the IWfF will fail on every occasion. Every leader going into a BCT S-2 or MICO has to proactively embrace these concepts and diligently work to integrate holistically the IWfF into one team – the BCT will not succeed without a fully functional, cohesive, and integrated IWfF. 

Endnotes

1. U.S. Army Techniques Publication (ATP) 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington, DC: U.S. Government Printing Office [GPO], 10 February 2015), 2-5

CW2 David Pierce has been in the Army 14 years and is currently serving as the senior all source intelligence technician for 2nd Stryker Brigade Combat Team, 2nd Infantry Division at Joint Base Lewis-McChord, Washington. His previous assignment was to the 10th Army Air and Missile Defense Command in Kaiserslautern, Germany where he spent four years specializing in combating ballistic missile threats inside the U.S. European Command and U.S. Central Command areas of responsibility.

Excerpt from Draft Publication ATP 2-19.4, Brigade Combat Team Intelligence Techniques

Brigade Combat Team Intelligence Structure

By table of organization and equipment (TO&E), the brigade combat team (BCT) intelligence structure is comprised of the BCT intelligence staff section, military intelligence (MI) company, and battalion intelligence staff sections. However, during operations the BCT commander and staff, and subordinate battalion commanders and staffs work together to task organize those elements into intelligence cells and units to meet the many intelligence requirements within the BCT. There is no single doctrinal solution to the task organization of these cells and units.

Normally, the intelligence structure is comprised of a BCT intelligence cell supporting the BCT command post structure, MI company (minus) that is general support (GS) to the BCT, and battalion intelligence cells for each subordinate battalion. When appropriate, the intelligence structure includes providing signals intelligence (SIGINT), human intelligence (HUMINT), or multifunction team (MFT) augmentation to battalions or companies and analytical augmentation to the battalion intelligence cells or as many as ten maneuver companies. Additionally, the tactical unmanned aerial systems platoon is often under an administrative control relationship to the combat aviation brigade for aviation safety, standardization, and sustainment reasons while still providing GS as part of the MI company (minus) to the BCT.

The MI company provides the majority of intelligence personnel to the BCT to collect, analyze, and disseminate intelligence. At home station, the MI company is assigned to the brigade engineer battalion (BEB). However, during operations the BCT commander and staff task organize the MI company based on the mission variables (METT-TC). The BCT intelligence staff section is not adequately manned to support BCT operations. Therefore, the information collection platoon, intelligence and electronic warfare system integration platoon, and staff weather officer section of the MI company are task organized under an operational control relationship to the BCT S-2 in order to combine with the BCT intelligence staff section to form the BCT intelligence cell. These elements of the MI company provide the BCT intelligence cell with automated intelligence processing, exploitation and dissemination (PED), analysis, and dissemination capabilities, as well as access to the intelligence products of higher and lower echelons.

After the MI company provides those three elements to the BCT S-2 to form the BCT intelligence cell, the unit operates as an MI company (minus). The MI company (minus) conducts GS intelligence collection in support of the BCT except in exceptional circumstances. There is an assumption, but no guarantee, that the expeditionary military intelligence brigades will provide HUMINT, SIGINT, and/or counterintelligence augmentation to the MI company (minus) as needed. As a result of the complexity of this intelligence structure and how the cells and units are task organized during operations, the BCT commander and staff, BEB commander and staff, and MI company commander must continuously work together as a team in garrison to ensure the MI company is trained and ready for deployment and operations.



Systemic Challenges within a Brigade Combat Team Military Intelligence Company

by Captain Grace Lu

Introduction

The military intelligence company (MICO) within a brigade combat team (BCT) has two primary challenges that drive friction points, which continually impact MICO leaders at all levels. First, the BCT organizational structure is not responsive to the management of a MICO. This results in significant training difficulties, as well as minimal support for specialized MICO needs. Second, the MICO has a significant property management challenge—extremely complex and nuanced equipment—that other companies in a BCT do not share. This results in a continual administrative burden to the MICO.

The intent of this article is to help frame and articulate these two key challenges facing today's BCT MICO leaders. This article also attempts to act as an introduction to leaders currently overseeing or newly assigned to a MICO, with information drawn primarily from the author's experiences and observations. However, it is important to acknowledge that the challenges described in this article are not comprehensive. Differences in BCT mission requirements, personalities, and command emphasis are a reality, and will likely compensate for or create additional challenges outside the scope of this article. Likewise, each MICO platoon has its own unique set of challenges. Some of these are mentioned, but these challenges remain outside the scope of this article.

Military Intelligence Company Overview

The MICO adds significant value to the BCT structure, providing organic intelligence collection and analytical support at the brigade level. The MICO is also a highly capable organization, able to employ multiple intelligence disciplines simultaneously at dispersed locations on the battlefield. Generally, MICO capabilities are organized within three distinct platoons: information collection, multifunction, and unmanned aircraft system (UAS).

The information collection platoon primarily provides intelligence analysis to the brigade intelligence support ele-

ment and includes all-source intelligence analysts (Military Occupational Specialty [MOS] 35F) and geospatial intelligence (GEOINT) imagery analysts (MOS 35G) with their associated equipment, a cryptologic support team, operations management team, and intelligence and electronic warfare systems integration section.

The multifunction platoon provides an intelligence collection capability by way of human intelligence (HUMINT) and signals intelligence (SIGINT). Specifically, the platoon has HUMINT collectors (MOS 35M) and cryptologic linguists (MOS 35P). Historically, this platoon has deployed HUMINT collection teams and low-level voice intercept (LLVI) teams to support BCTs. With a modified table of organization and equipment (MTOE) change in fiscal year 2015, the multifunction platoon is now organized to provide a multifunction team capability when a need to combine HUMINT and SIGINT capabilities arises.

The UAS platoon provides the RQ-7 Shadow platform to the brigade and generally includes UAS operators (MOS 15W) and UAS repairers (MOS 15E). This platoon is the only aviation asset in the BCT and the sole organic full motion video asset for the brigade commander.

Based on these capabilities, it is evident that the BCT MICO's structure is unique and intricate. While a standard 654 Soldier light infantry battalion has 25 different Army MOSs, a standard 96 Soldier MICO has 17. The MICO has roughly two-thirds as many specialties as an infantry battalion that includes five separate battalion staff sections, multiple specialty sections (to include the chaplain, fires, and physician's assistant), as well as a medical and mortar platoon. In other words, the MICO is a company-sized element with battalion-sized complexities and responsibilities. Platoon leaders and platoon sergeants are expected to manage platoons that have as many working pieces as most headquarters and headquarters companies. Similarly, the UAS platoon is expected to maintain the same aviation requirements as any squadron within a combat aviation brigade (CAB). This reality indicates that MICO leaders are often oversaturated with both training and administra-



An RQ-7B Shadow UAS launching in support of Brigade Combat Team operations.

tive requirements generally reserved for and performed by staffs at higher echelons.

Brigade Combat Team Organizational Structure

The Challenge. The BCT organizational structure is one of the MICO's main challenges. Specifically, the BCT organizational structure focuses on supporting and facilitating the mission of its infantry and/or armored battalions, with the MICO structured as a brigade enabler. As a result, the MICO is often conceptualized as a brigade-level asset and needs to coordinate closely with the S-2, S-3, and aviation element within the brigade staff. However, the MICO must also be capable of deploying intelligence collection teams to each maneuver battalion and the reconnaissance squadron within the brigade. The MICO is under the brigade engineer battalion (BEB) for administrative purposes and day-to-day operations. This results in multiple customers, but more pragmatically, multiple bosses for MICO leadership to navigate. For instance, given competing requirements from the BEB commander and brigade S-2, who ultimately takes precedence? Given three LLVI teams and four battalions to support, which battalion field training exercises do they enable?

The friction point conceptualized above displays the difficulty of training management within the MICO. The MICO mission essential task list encompasses providing intelligence support to the brigade through its three separate and distinct platoons. Although simple in concept, MICO training management is much more difficult to employ in practice because of the number of elements the unit supports. Ultimately, MICO leaders need to understand the training calendars of both the brigade and five subordinate battalions. MICO leaders must then take this information and translate, balance, and ultimately execute training that is consistent with a specific MOS or platoon training glide path. These are not simple tasks, especially for company- and platoon-level leaders.

While the BCT organizational structure creates significant training management friction points for the MICO, the lack of tailored MICO support also challenges its lead-

ers. For instance, the first echelon above the MICO that provides dedicated SIGINT support is the division level or higher—it depends on the BCT's parent organization—while a GEOINT warrant officer is not organic until the corps level. Furthermore, a BCT does not have an allocated flight surgeon. In the MICO of the 3rd Brigade Combat Team, 25th Infantry Division, this meant that UAS platoons were dependent on the CAB for flight surgeon support.

These small administrative details, when combined, accumulate into an extremely complex, and often time-consuming, challenge for a company-sized element to manage and overcome. The center of gravity within a BCT lies within its maneuver elements. As a result, an infantry platoon will have increasing support at each echelon within a BCT. However, the MICO does not have that luxury. Likewise, the BEB is structured as the administrative headquarters for the MICO, but is limited in its ability to provide the specialized services needed for its intelligence and aviation assets. This commonly results in elements from the MICO having to coordinate and interact with echelons above battalion, as well as other brigades, to fully utilize resources and assets needed to sustain and improve the company. For a 96 Soldier company with no allocated staff sections, this is extremely challenging to overcome.

Mitigating the Challenge. To overcome the organizational challenges within a BCT, MICO leaders must be able to build rapport outside the direct chain of command. With both a customer base and support zone that expands well beyond the BEB footprint, the MICO must be able to build and maintain relationships that other companies might otherwise ignore. First and foremost, the MICO must have a healthy relationship with the brigade S-2. This relationship has been continually highlighted and elaborated on during combat training center evaluations, and should be a priority for all MICO leaders to maintain. A MICO that is able to nest its training within the broader intelligence warfighting function will be more successful than one that operates independently. Similarly, the top cover and resources available by position and rank to the brigade S-2 can help mitigate some of the support deficiencies within the BEB.

However, the brigade S-2 is only the starting point. Building rapport within the CAB will mitigate some of the UAS friction points, while talking to the equipment program managers will pay dividends in the maintenance and property realms. Maintaining a relationship with the BCT reconnaissance and maneuver battalions, often through capability briefs and exercise support, is also a necessity. These working relationships are crucial in alleviating the cultural and procedural differences between the MICO and its custom-

ers, and often open doors for additional training and support opportunities.

It is important to note that rapport building is extremely time and energy intensive. There never seems to be enough time in a day to get work done, tempting leaders to replace relationship building with more immediate and pressing concerns. However, to mitigate the organizational difficulties, MICO leaders must develop and foster a network that transcends the formal chain of command. The BCT is not capable of supporting the MICO in its basic set-up, nor should it. MICO leaders need to build their own supports.

Property Management

The Challenge. Conducted through the Army Command Supply Discipline Program (CSDP), property management cannot be overlooked by any MICO leader. Although most companies would say that CSDP is challenging, the challenge is amplified in the MICO due to the complexity of its property book. The MICO property book has large amounts of radios, tool kits, and specific intelligence and aviation equipment that are extremely difficult and time intensive to inventory. Coupled with commercial off-the-shelf (COTS) and project manager- (PM-) facilitated equipment, the MICO property book can easily overwhelm its leaders.

Neither COTS nor PM-facilitated equipment follows the CSDP system well. COTS equipment includes property procured outside of the formalized Army acquisitions and supply processes. COTS equipment generally fills a capability gap within standard Army equipment or complements the Army supply system in times of significant operational need (such as during deployments). In the MICO, COTS equipment can range from specialized antennas and receivers, to HUMINT peripherals and kits, to dedicated aviation equipment. PM-facilitated equipment is also inescapable within the MICO. For instance, Program Managers provide sustainment support to both the RQ-7 Shadow and the Prophet system programs of record.

The majority of Army property fits nicely under CSDP. Supply specialists and hand receipt holders are accustomed to using the Property Book Unit Supply Enhanced (PBUSE) system for updating component hand receipts and filling shortages, while technical manuals are the final authorities on the components of end items and basic issue items for most equipment. COTS and PM equipment are an exception to the rule. Most of this equipment has neither technical manuals nor consistent national stock or serial numbers to maintain standard accountability. Oftentimes,



Photo by CPT Grace Lu

Loading of Delta Company (MICO), 29th Engineer Battalion equipment onto a logistic support vessel for deployment within the Pacific region.

hand receipt holders have to maintain their own inventory and picture binders, as well as hand receipts with components of end items and basic issue items. Fielding new equipment and upgrading and transferring PM equipment add yet an additional variable that can create CSDP friction points, since these operations generally have minimal administrative oversight or support from higher echelons.

An example that highlights this exception to the rule is the UAS generator. When I was a MICO executive officer, an outgoing lateral transfer order (equipment to be removed from the unit) from the brigade property book office was for an obsolete generator variant in the Army inventory. This transfer order seemed legitimate because the obsolete generator was being phased out and replaced by an upgraded generator, which was already on the property book. However, I discovered that the obsolete generator was still a vital part of the UAS platoon. It was the only trailer-mounted generator, and thus field expedient power source, in the inventory. The upgraded generator was still undergoing aviation testing, and therefore, not authorized for use with the RQ-7 system. Consequently, the equipment program manager had kept the obsolete generator as part of the UAS package—unbeknownst to the Department of the Army.

To resolve this confusion, the MICO had to surge significant organizational effort to cancel the lateral transfer. The UAS platoon contacted the equipment program manager to explain the situation and create a legitimate top cover for cancelling the lateral transfer. The MICO supply team translated the explanation into a memorandum for record, which codified the UAS need. MICO leadership communicated this friction point to higher echelons and the brigade property book office. In the end, this one lateral transfer sapped significant MICO organizational energy. This is just

one of many property management challenges facing MICO leaders.

Mitigating the Challenge. Given the complexities of intelligence and aviation equipment, property management will usually challenge MICO leaders. However, mitigating the risk involved with CSDP boils down to one concept: command emphasis. Those units that actively prioritize CSDP will be more successful than those that do not. For instance, leader development is one way to codify CSDP command emphasis. MICO leaders that continually mentor their subordinates on property management through counseling sessions and leader professional development programs will likely have more success than those who ignore the topic. Similarly, units that meticulously include inventories and hand receipt reconciliation in their training schedules will likely succeed. Oftentimes, I have witnessed CSDP performed poorly due to training events that directly conflict with monthly sensitive items or cyclic inventories, or exercise recovery operations that fail to account for field loss.

Ultimately, MICO leaders must emphasize property management. Realistically, competing requirements will make this concept difficult to maintain in execution. However, given the complexity of the MICO's equipment and the inclusion of PM and COTS equipment, MICO leaders cannot hand wave CSDP.

Conclusion

To overcome BCT organizational structure and property management challenges, MICO leaders must develop and



Photo by CPT Grace Lu

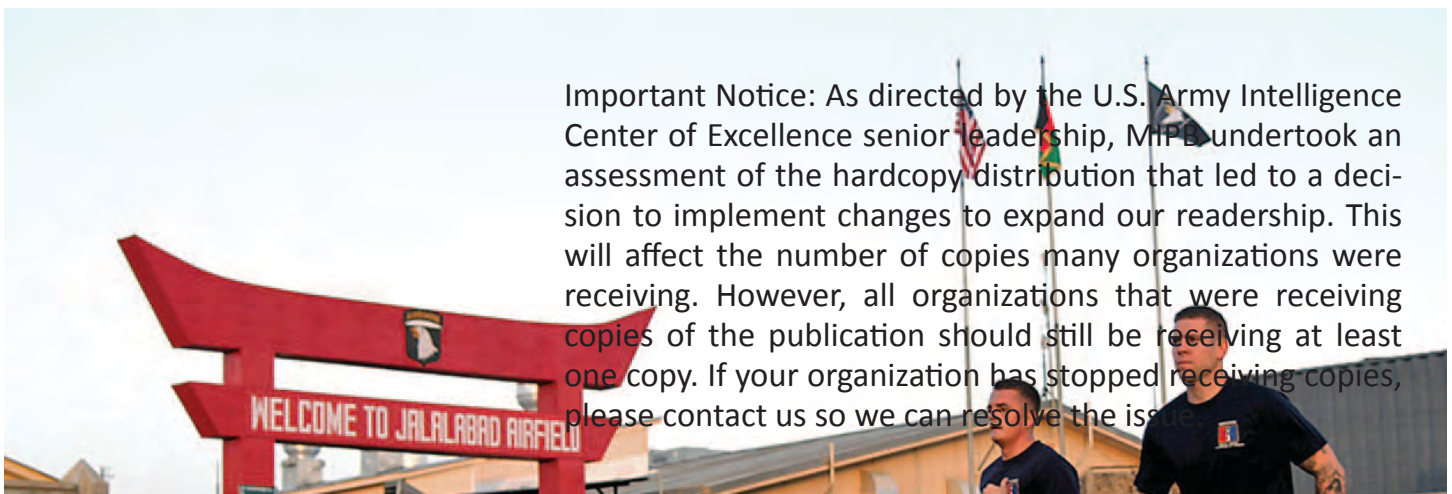
Preparation of Delta Company (MICO), 29th Engineer Battalion equipment for change of command inventories.

foster a network that transcends the formal chain of command. MICO leaders must be comfortable branching out of the BEB. Moreover, MICO leaders must actively emphasize CSDP. Given the complexities of intelligence and aviation equipment, MICO leaders must embrace CSDP in an already task-saturated environment. 🌟

References

- U.S. Army Force Management Support Agency, "Brigade Engineer BN (BEB), IBCT (Recap) – MTOE.", accessed July 25, 2016, <https://fmsweb.army.mil>.
- U.S. Army Force Management Support Agency, "Infantry Battalion (IBCT) – MTOE.", accessed July 25, 2016, <https://fmsweb.army.mil>.

CPT Lu served as the executive officer for the military intelligence company of the 3rd Brigade Combat Team, 25th Infantry Division from October 2014 to February 2016. She is currently an intelligence officer serving at Fort Campbell, Kentucky. Her military education includes the Military Intelligence Captains Career Course and Military Intelligence Basic Officer Leadership Course. CPT Lu holds a bachelor of science in electrical engineering from the U.S. Military Academy.



Important Notice: As directed by the U.S. Army Intelligence Center of Excellence senior leadership, MIPB undertook an assessment of the hardcopy distribution that led to a decision to implement changes to expand our readership. This will affect the number of copies many organizations were receiving. However, all organizations that were receiving copies of the publication should still be receiving at least one copy. If your organization has stopped receiving copies, please contact us so we can resolve the issue.

Distributed Common Ground System - Army in the Brigade Combat Team: The Path to Success and Mastery



by Lieutenant Colonel Jim Reed, Chief Warrant Officer Two (P) Rob Buckley, and Mr. Devin Rollis

The Distributed Common Ground System-Army (DCGS-A) is the primary automated information processing system employed by the Army's intelligence warfighting function (IWFF). It allows the IWFF to operate successfully within the larger digital environment of the Army Mission Command System (AMCS). This article provides information that all DCGS-A users should know in order to successfully integrate DCGS-A into the AMCS architecture. In this article, we will discuss recent unit level observations with a focus on DCGS-A employment in the S-2 intelligence cells. Important keys to success are also offered, outlining how units can most efficiently work towards DCGS-A mastery. Lastly, several training resources are listed in order to assist units with their DCGS-A training efforts.

Recent Observations

Unit exercises and combat training center (CTC) rotations result in some of the most noteworthy observations involving the use of DCGS-A at the brigade and battalion levels. Some recent observations involving personnel, systems hardware, and systems software are discussed in the following paragraphs.

Collective Training. There is an overall lack of collective level training of the IWFF, including intelligence processes using DCGS-A tools. Many unit S-2s make good use of the Army's Foundry Intelligence Training Program to conduct individual skills training. However, they often do not follow-up with team/section level collective training prior to command post exercises, leaving their units untrained and unprepared for follow-on CTC rotations or real-world deployments.

Standard Operating Procedures. Few brigade S-2 intelligence cells develop useful, comprehensive standard operating procedures (SOPs) to codify intelligence processes, responsibilities, and production schedules. This results in S-2 intelligence cells not understanding what their own production timelines are and what they need their DCGS-A products to look like. Written SOPs are essential, as they help to standardize processes, establish uniformity in products, reduce miscommunications, and improve overall efficiency.

Shapefiles. Instead of disseminating Shapefiles (a geospatial vector data format for geographic information system software, think ArcGIS), brigade S-2 intelligence cells often provide products in PowerPoint to subordinate battalion S-2 intelligence cells. These PowerPoint products cannot be easily refined or adjusted and do not have embedded geospatial vector data, grid coordinates, or other metadata, making it difficult to determine the precise or reported locations of enemy units or activity.

Data Dissemination Service. Data Dissemination Service (DDS) software allows for dissemination of data across mission command systems. However, S-6 section DDS managers often lack the knowledge required to configure the DDS, which involves the loading of software onto the DDS laptop. For instance, DDS managers must know to use the latest Tactical Services Security System (TS3) certificate—the digital code that allows DDS to communicate with other mission command systems. Additionally, DDS managers must know how to assign user permissions to individual mission command systems, which allows DCGS-A users to create advertisements, publish to advertisements, or subscribe to advertisements. Advertisements are services that provide data between mission command systems, and which allow data to transfer between the various types of mission command systems (e.g., DCGS-A, AFATDS, GCCS-A, etc.).

Communications-Electronics Command Software Updates. Software updates from the Communication Electronics Command (CECOM) come out monthly and quarterly. The quarterly update includes the three prior monthly updates. These updates include generic software fixes. Units must ensure their DCGS-A servers and computers are able to receive these important software updates to remain current and operational.

DCGS-A System Configuration. Field service engineers/representatives (FSEs/FSRs) and military occupational specialty (MOS) 35Ts (military intelligence (MI) systems maintainer/integrator) often skip steps listed in the FSE setup guides, resulting in software anomalies later. Depending on the

software version, typically 10 to 14 books comprise an entire FSE setup guide. Failure to follow ALL steps when configuring the DCGS-A systems may result in units experiencing unique anomalies (software bugs).

Software Problem Reports. FSEs/FSRs and MOS 35Ts are not submitting software problem reports (SPRs) to document DCGS-A issues encountered during exercises or operations. The DCGS-A program relies on SPRs to discover software glitches and develop remedies. SPRs provide details of the malfunction so engineers can develop software patches (inserted via monthly and quarterly CECOM software updates). SPRs for both DCGS-A v3.1.7 software and v3.2 software are submitted to CECOM through a Project Forge web portal.

Sustainment Training. Many units lack DCGS-A sustainment training programs and lose expertise when trained personnel depart the unit, resulting in steep learning curves for new Soldiers. Units train hard in preparation for a CTC rotation, but then often relax their DCGS-A training objectives/goals immediately afterwards. Sustainment training is necessary to maintain unit proficiency, to carry-on DCGS-A training efforts throughout units busy training schedule, and to preserve the IWFF in a high state of readiness.

DCGS-A Mastery

Units should strive for mastery in their use of DCGS-A. In order to do so, S-2 intelligence cells and MI companies must be willing to dedicate the training time required to master this system. DCGS-A is the primary tool S-2 intelligence cells utilize within the unit's larger digital environment. Just as a trumpet is part of a larger symphony orchestra, so too is DCGS-A part of the larger digital environment of AMCS.

Mastery is a relatively straightforward process, and typically takes place in three stages. Stage 1 involves *learning about the environment* in which the unit must operate. Stage 2 involves *understanding the environment* in which the unit must operate. Stage 3 is the level of mastery; achieved when a unit is truly proficient in a series of skills to the extent they can *master their own environment*.

While seemingly a simple concept, understand that musicians often require a minimum of 10 years or 10,000 hours of practice with their chosen instrument to achieve a level of mastery. Time is the most critical factor with regard to mastery. In order to achieve a level of mastery with DCGS-A, S-2 intelligence cells must set aside time to train on collective level skills. Achieving mastery with DCGS-A does not re-



Digital intelligence system master gunner, CW2 (P) Robert Buckley, training on the portable multi-function workstation at Fort Huachuca, Arizona.

Photo by LTC Jim Reed

quire thousands of hours, but S-2s should plan to spend 200 to 300 hours using DCGS-A in collective level training events in order to begin to achieve DCGS-A mastery within the digital environment. Ideally, S-2 intelligence cells should shoot for achieving at least a modest level of DCGS-A mastery prior to participating in a brigade or battalion level command post exercise or CTC rotation. Stage 1 can be achieved through professional development sessions, whereby unit personnel are familiarized with the various components and capabilities that make up the DCGS-A family of systems (e.g., P-MFWS, IFS, IPC-2, TGS, GWS, CHARCS, etc.). Stage 2 is achieved during the unit's initial 200 to 300 hours of employing DCGS-A in various collective level training events.

Keys to Success

On the path to DCGS-A mastery, there are several important factors involving the same crucial elements previously discussed — personnel, systems hardware, and systems software — the S-2 should consider.

Understand the DCGS-A Components. All intelligence leaders must understand the various components of DCGS-A, to include:

- ◆ Portable multi-function workstation (P-MFWS)
- ◆ Intelligence fusion server (IFS)
- ◆ Intelligence processing center-2 (IPC-2)
- ◆ Tactical ground station (TGS)
- ◆ Geospatial intelligence workstation (GWS)
- ◆ Counterintelligence human intelligence automated reporting and collection system (CHARCS)
- ◆ Joint tactical terminal (JTT)
- ◆ Trojan SPIRIT Version 3

- ◆ Prophet
- ◆ Trojan-LITE

This may require numerous leader professional development sessions to train leaders on the capabilities of these components.

Involve the brigade executive officer, S-2, S-3, S-6, military intelligence company leadership, and MOS 353Ts in planning. Inform and educate MI and non-MI leaders when planning DCGS-A related training. Be sure to also include them when establishing (i.e., setting up) the various components of the intelligence architecture.

Develop a relationship with your digital intelligence system master gunner. Who is your unit digital intelligence system master gunner (aka, DCGS-A master gunner)? Whom from your unit can you send to this course? Master gunners can help units plan for how to best setup their intelligence architecture. They receive training on how to conduct initial troubleshooting of intermediate DCGS-A system issues, filling the gap between the operator and the MOS 35T/353T. They are also capable of supervising unit training, and reviewing SOPs and training plans.

Integrate mission command systems during all collective training events. How will DCGS-A be integrated with mission command systems? Always attempt to train DCGS-A interoperability with other mission command systems. For instance, DCGS-A can send data through the S-6's DDS to the S-3's command post of the future and the fires section's advanced field artillery tactical data system, so whenever possible include these systems in IWFF training events. This may require additional coordination with the S-6 section, S-3 section, fires section, or others in order to have them provide systems and operators.

Standard Operating Procedures. Develop SOPs, keep them updated, and ensure they are used and followed during every training event. Document all digital intelligence processes and the successful tactics, techniques, and procedures, as well as any backup analog processes. SOPs are needed at brigade, battalion, and even company level.

Crew Drills. Ensure crew drills for assembling the intelligence architecture are documented and rehearsed. Soldiers should understand their individual roles, to include responsibilities for maintaining their systems,

cabling their systems to the network, and powering systems on and off.

PACE Plan (communications plan). PACE is a memory aid for primary, alternate, contingency, and emergency means of communication. What is the PACE plan for communication across the brigade and to higher echelons (e.g., Division)? Ensure there is a PACE plan in the SOP that works and which you intend to use. For instance, units will need to implement their PACE plan when they conduct jump tactical operations center (TOC) operations.

Intelligence Fusion Server. Consider keeping IFSs mounted inside both the IPC-2 vehicle and the TGS vehicle, in order to minimize challenges with reloading them back into the vehicles when the main command post jumps forward.

Knowledge Management. While a brigade staff will have a knowledge management officer (KMO) who is responsible for knowledge management processes throughout the TOC, this individual may have very little understanding of the complexity of intelligence processes or DCGS-A. Brigade S-2s should designate an S-2 intelligence cell knowledge management representative (KMR) to ensure knowledge management efforts are properly coordinated with the brigade KMO. The KMR should be able to improve DCGS-A interoperability with other mission command systems, as well as assist with the documenting of knowledge management procedures and activities. The KMR can also assist with designing the intelligence architecture plan, which must be developed in concert with the brigade S-6's communications architecture plan.

Tactical Entity Database. Consider whether the brigade S-2 intelligence cell will maintain the tactical entity database (TED) and provide it to battalions, or whether the battalions



A BCT S-2 provides guidance to his staff following an internal synchronization meeting.

Photo by MAJ Nathan Adams

will maintain their own TED and provide it to brigade. How will TED replication occur, will it be listed on S-2 intelligence cell battle rhythms, and how will it be shared (i.e., shared via Datamover, Excel or Vcab over Psi Jabber, Transverse, email, or JCR/BFT2)?

Analysis. Determine where analysis will occur. Will it be federated? Will it be conducted via intelligence reach (reach-back) or at the forward location? Will it be done from a fixed site or on the move?

Threat input to the common operational picture. Plan and rehearse how the threat data input to the common operational picture will be shared and visualized up, down, and laterally?

Computer Logins. Ensure user names and passwords conform to standards that avoid cyber intrusion attacks.

Training

Well-trained units can do these four tasks, which put them well on the way to success and ultimately mastery of DCGS-A skills.


- ◆ Combine and operate DCGS-A components.
- ◆ Conduct DCGS-A database synchronization between echelons.
- ◆ Pass DCGS-A graphics to other mission command systems.

- ◆ Establish and exercise a PACE Plan.

The Training and Doctrine Command Capability Manager – Foundation at the U.S. Army Intelligence Center of Excellence is the centralized manager and coordinator for capability development and user activities associated with the Army’s sensor processing, exploitation, and dissemination capabilities and programs. They maintain a NIPRNET DCGS-A Mil Suite website located at: <https://www.milsuite.mil/book/groups/dcgs-atcm-sensor-processing/> (login required)

Another NIPRNET Mil Suite website maintained by the DCSG-A Support Activity Detachment is dedicated to the tactical ground station and is located at: <https://www.milsuite.mil/book/groups/dcgs-a-support-activity-dsa> (login required)

The SIPRNET DCGS-A user forum is located at: <https://dcgsaconusbrain.mi.army.smil.mil/phpbb3> (login required)

For additional information about the Digital Intelligence Systems Master Gunner Course, please refer to the Military Intelligence Professional Bulletin article in the October – December 2016 issue titled, “Digital Intelligence Systems Master Gunner Course.” Further information can also be obtained by contacting the course officer in charge at (910) 643-0400. 

LTC Jim Reed served as brigade S-2 for 4th Brigade Combat Team (Airborne), 25th Infantry Division during 2008-2010. He is currently the assistant Training and Doctrine Command (TRADOC) Capability Manager (TCM) for Training at TCM-Foundation, Fort Huachuca, Arizona. Previous assignments include J-2 for Task Force 2010, G-2 operations chief at U.S. Army South, brigade S-2 for the 18th Military Police Brigade, 11th Armored Cavalry Regiment assistant regiment S-2, and 96th Civil Affairs Battalion S-2 and Headquarter and Headquarters Company commander.

CW2 (P) Rob Buckley served as senior all source analyst for 4th Brigade Combat Team (Airborne), 25th Infantry Division during 2008-2010. He is currently the senior all source technician at TCM-Foundation, Fort Huachuca, Arizona. Previous assignments include Central Asia intelligence analyst for the 513th Military Intelligence Brigade, knowledge manager for Intelligence and Security Command’s Ground Intelligence Support Activity, and chief of all source training for the U.S. Army Foundry Intelligence Training Program.

CW5 (Ret.) Devin Rollis currently works as all source advisor at TCM-Foundation, Fort Huachuca, Arizona. Previous assignments include all source analyst at 3rd Armored Division and V Corps, and all source technician at 3rd Brigade, 24th Infantry Division, I Corps, VII Corps, the 66th Military Intelligence Brigade, and the Defense Intelligence Agency.

Speaking a New Language: MI Gunnery



by Captain Jamie B. DeSpain, with Chief Warrant Officer Two Trevor J. Kinzel,
Warrant Officer One Paul A. Crawford, Warrant Officer One Jasmin J. Johnson,
and First Lieutenant Joseph L. Honeycutt

Editor's Note: In the last issue of MIPB, we published an article titled "MI Gunnery: Why and How?" In the article the U.S. Army Intelligence Center of Excellence, Training Development and Support Directorate presented the development strategy for MI Gunnery that is in revision with a planned update to TC 2-19.400, MI Gunnery for the Military Intelligence Company of the Brigade Engineer Battalion. The updated manual will address the valid problems identified in this new article based off the training guidance provided in the currently available training manual.

Introduction

The concept of Military Intelligence (MI) Gunnery is the MI Branch's effort to identify a way to rebrand the method for qualification and certification of intelligence professionals and units into a construct that is more familiar to the units they support. Saying MI Gunnery within an armored brigade combat team will initially cause more than a few double takes, followed by a smattering of confused looks, and finally a flurry of questions will bring up the rear of the crowd's confusion. Did you say MI Gunnery? As in shooting? What are you shooting? Frankly, the confusion is understandable, and despite the growing pains, the concept developers did a good job creating better conditions for shared understanding across multiple echelons. I first found out about MI Gunnery about two weeks before taking command of 2nd Armored Brigade Combat Team/1st Infantry Division's MI Company (MICO) and I was initially apprehensive about tagging a combat arms-type qualification process to my information collection, multifunction, and unmanned aircraft system (UAS) platoons. Additionally, each unit who developed an initial MI Gunnery plan had their own way of approaching the problem. Therefore, immediately my company leadership and I began to evaluate what appeared to be a large amount of latitude to accomplish this new directive. This latitude was more than we were used to or expecting, but I will never complain about being given too much freedom when developing a concept of operations to accomplish a mission. Training Circular (TC) 2-19.400, *MI Gunnery for the Military Intelligence Company of the*

Brigade Engineer Battalion, provided a general way ahead and with that TC as a guide, we got to work. The primary goals for MI Gunnery are to fully mesh the MICO with the brigade S-2, deliver the intelligence collection capability to the brigade, and therefore enable the brigade S-2 and brigade mission success in any threat scenario.

The Unit Training Plan

The first step in laying out our plan for MI Gunnery entailed breaking down what each individual certification table really required. At first glance, the tables were slightly misleading, especially with regard to Table II. We eventually determined that Table II was an assessment of Table I tasks and not a separate set of tasks. Next, we began to backwards plan based on the training events already planned that lined up with the tables. For example, we knew Table VI is, by definition, a combat training center rotation and we had that on the calendar with our brigade combat team's (BCT's) upcoming National Training Center rotation. Table IV contains unit collective tasks and Table V is the assessment of Table IV. Therefore, we planned to conduct both tasks simultaneously at Danger Focus - our BCT's training exercise held in January and February by using a "rolling assessment" format. Observer-controller-trainers will evaluate the platoons on a continual basis as they practice their Table IV tasks until a Table V trained "T" status is reached. Table fluidity is further highlighted in training events like the All-Source Production Course II where at times the information collection platoon could be conducting Table I and Table II due to the course make-up and end-of-course evaluation.

Tables I, II, and III (Set-up and Tear-down of MI Equipment) were the difficult tables to determine where to train, but the latitude in the plan allowed us to take Foundry Courses, participate in brigade command post exercises (CPX), and schedule mobile training teams in order to apply MI Gunnery tables to them. In addition, the latitude allowed us the freedom to create and tailor training events to en-

sure we achieved the remaining tables. Table II is the most notable of this group as we determined that each platoon needed their own Table II assessment exercise of Table I tasks. As an example, we accomplished this for our multi-function platoon by aligning the Table II assessment with the fielding of the Prophet Enhanced System. The platoon exercised both signals intelligence and human intelligence Table II during the final culminating field training exercise (FTX) portion of the Prophet new equipment training effectively achieving two training objectives with a single event.

Observations

Although not all of the MICO's platoons are yet complete with this first iteration of MI Gunnery, I am confident that we are far enough into this process to offer several constructive observations to the MI community on this concept. Beginning with the positive aspects, MI Gunnery is an outstanding additional tool for the MICO and brigade engineer battalion leadership to ensure training of required tasks. Second, it allows a focused look at smaller subsections of the company like the intelligence and electronic warfare and geospatial intelligence sections. Third, it provides a new, fresh way to explain to maneuver commanders the training already conducted by MICOs annually.

One key to success with MI Gunnery is early integration with the brigade S-2 and staff. The primary reason is to add emphasis and mutual benefit to ensuring the MICO participates in brigade situational training exercises (STX), CPXs and FTXs as they accomplish Tables II, III, IV and V. By participating in these brigade level training events, the MICO enables the collective team to be successful during larger training events, such as our BCT exercise Danger Focus II, and then the subsequent rotation at the National Training Center. Previous rotations have proven that intelligence is only successful when integrated with mission command. If the MICO's focus is only to conduct company level exercises, it will lack the scope needed to support mission command without the brigade staff sections present and that staff will lack experience in properly leveraging the capability. It is preferable for the MICO to execute company exercises prior to a brigade level training event to ensure the intelligence architecture, standard operating procedures and troop leading

procedures are effective. However, there is no success until integration is accomplished with mission command. The take away is the MICO can be proficient with all individual, collective and company mission essential task list (METL) tasks with operational equipment, but if there is no integration with the brigade S-2 and staff, expectations and ad hoc requirements render the support degraded or ineffective to fully support mission command. Therefore, precedence should be given to utilizing a brigade STX, CPX, and FTX as a certification exercise for Table IV instead of a company level exercise.

There are some negatives with MI Gunnery that the MICO must be aware of and address. The first lies with the concept's application for the UAS platoon. My UAS standardization officer could not find any direction from the aviation community regarding MI Gunnery. This led us to inquire further into the outcome of coordination between the U.S. Army Intelligence Center of Excellence (USAICoE) and the U.S. Army Aviation Center of Excellence (USAACoE) during the development of the concept. At the MICO level, there exists significant confusion when explaining MI Gunnery tables versus the required UAS Aviation Gunnery tables. The bottom-up refinement recommendation is for USAICoE to coordinate closely with USAACoE when updating the MI Gunnery TC to account for requirements of the UAS platoon, specifically the certification of set-up and displacement of UAS equipment. In accordance with current guidance, the UAS platoon accomplishes the majority of the listed MI Gunnery tasks through their daily flight operations; however, if the UAS platoon is going to be fully certified, then the MI Gunnery and Aviation Gunnery tables need to mesh, or at least work in concert with each other.



A BCT S-2 briefs during the BCT's combined arms rehearsal during a decisive action training environment rotation at the Joint Readiness Training Center.

Photo by MAJ Nathan Adams

The second negative is the absence of DCGS-A for Table III certification. This presents an issue since DCGS-A is the anchor point for knowledge management, intelligence architecture, and analysis for the MICO. Since it is not present in Table III, this could indicate to some that the system is becoming irrelevant; likely, because of how complicated it is to set up and because it lacks a standard. This must change to renew confidence of both commanders relying on and intelligence professionals using DCGS-A.

The third negative is the absence of tactical sensitive compartmented information facility set-up and teardown in the certification requirements. As a part of the shift from focus on a counterinsurgency environment to decisive action training environment/hybrid threat, the need to resource and practice maintenance of this key facility is significantly greater because of the added value the capabilities each intelligence discipline brings to the fight with access to higher levels of classification.

The final negative, albeit not as important as the previous three, still requires consideration. As discussed at the beginning of the article, discussions of MI Gunnery with non-MI personnel often causes some level of confusion and misunderstanding. A recommendation is to change the name to MI Certification Tables (MICTs). It is a better descriptor of what the program really is (and is not), and it will allow others to understand MI Gunnery is different from actual gunnery tables without requiring explanations.

Conclusion

MI Gunnery still has a good distance to go before it matches the organization and familiarity of armor gunnery tables or engineer qualification tables, but it is a step in the right direction. The table format allows a level of comfort by verifying the training of our Soldiers with the necessary tasks. The success so far with MI Gunnery was in large part due to our brigade and battalion focus on requiring a detailed and synchronized METL crosswalk. The MICO METL crosswalk allowed us to prioritize tasks in MI Gunnery and further helped us to identify table application to training events. Like all change, MI Gunnery was met with apprehension, as the language and method of quantifying the “manned crew” concept, so widely used in combined arms, did not mesh with anything else in the MI community. However, at the end of the day, the MI Gunnery concept will benefit the MICOs and the MI branch overall by bringing us closer to other branches in terminology, construct of training plans, and shared understanding as we seek to better integrate in the BCT. This initial assessment of MI Gunnery indicates that the MI branch would greatly benefit from extending the construct and guidance to intelligence sections at all echelons in order to develop more professional, highly trained, and easily integrated members of the Army intelligence community. ✪

CPT Jamie DeSpain joined the Army in 2010 and is currently assigned as a MICO commander (D Co, 82nd EN, 2ABCT) at Fort Riley, Kansas. His previous assignments include brigade assistant S-2 and battalion S-2. He has deployed twice to Afghanistan and once to Kuwait.

Fort Huachuca Museum



Check out the Fort Huachuca Museum website at:
<https://www.ikn.army.mil>
Click on the Fort Huachuca Museums link



Intelligence Reachback Genesis



by Chief Warrant Officer Two Aaron Wolfgang and Chief Warrant Officer Three Keegan Guyer

The U.S. Army's understanding and practice of support to the warfighter has changed throughout the last 15 years of modern warfare. Intelligence support to the warfighter has also undergone drastic changes in the past four years. One of those changes beginning to see prevalence at the brigade combat team (BCT), division, and corps levels is the intelligence reachback cell (IRC). IRCs are a product of necessity, spawned from the boots on ground (BOG) restrictions imposed on International Security Assistance Forces in Afghanistan. The mission of an IRC is to enable warfighters with time-sensitive intelligence support from locations outside of the theater of operations, thus not counting against BOG numbers. With Operation Enduring Freedom well into its 14th year in 2015, initial plans were to reduce U.S. troop strength in Afghanistan to 5,000. Circumstances changed, and this did not happen as planned. The current assessed troop strength in Afghanistan is well over 10,000 requiring more cuts to meet the requirements.

This baseline requirement entails keeping a majority of intelligence support personnel at their home stations. With increasing threats and decreasing deployed workforce requirements, IRCs have been supporting emergent and continued requirements for almost a decade but the U.S. Army has published little regarding their makeup or utility.

First, what is the purpose of an IRC and why are they becoming a norm? Field Manual 3-96, *Brigade Combat Team*, states, "The military intelligence company supports the BCT and its subordinate units through collection, analysis, and dissemination of intelligence information. The company provides analysis and intelligence synchronization support to the BCT S-2."¹ How this translates into an adequately staffed and applicably focused team that provides utility to the BCT S-2 and subordinate commands from the other side of the world is the challenge for a BCT IRC.

The 3rd Brigade Combat Team, 101st Airborne Division "Rakkasans" IRC, at Fort Campbell, Kentucky, is staffed

with 23 Soldiers from both the military intelligence company (MICO) and the BCT's Headquarters and Headquarters Company S-2 staff section. The Rakkasans runs a seven day a week, 20 hour a day operation, to be in-line with real time Afghanistan battle rhythm events and mirrors the 0530 Afghanistan Time (AFT) to 0030 AFT workday in Afghanistan. To facilitate these hours the Rakkasans IRC team works two shifts daily from 2000 Central Standard Time (CST) to 0600 CST (1st shift) and another from 0500 CST to 1500 CST (2nd shift) with a one-hour handover period from 0500 CST to 0600 CST.

The design and staffing of the Rakkasans IRC is as follows:

- ◆ Fusion Team — comprised of all-source intelligence technicians, intelligence analysts, and human intelligence (HUMINT) collectors
- ◆ HUMINT Team — comprised of a HUMINT collection technician and HUMINT collectors
- ◆ Signals Intelligence (SIGINT) Team — comprised of a SIGINT analysis technician, cryptologic linguists, and SIGINT analysts
- ◆ Geospatial Engineer Team - comprised of a geospatial engineering technician and geospatial engineers

The MICO commander and staff execute mission command over the Rakkasan's IRC. The MICO commander also acts as the IRC assistant S-2. The day-to-day intelligence operations and production management is orchestrated by the brigade's senior all-source intelligence technician from the fusion team.

The fusion team primarily focuses on two products — one weekly and one bi-weekly. The first is an Afghanistan military releasable significant activity summary and the second is a non-Afghanistan military releasable enemy targeting product. These two deliverables fill an intelligence gap due to limited staffing at other organizations. The fusion team has also developed a handful of requests for informa-

tion (RFI) directly from the 3rd Brigade Combat Team S-2. The Rakkasans IRC's HUMINT team compliments the 36th Infantry Division (U.S. Army Reserve) "Arrowhead" IRC with daily source validation inputs. The Rakkasans IRC's SIGINT team works directly for the 3rd Brigade Combat Team SIGINT technician (who is forward deployed) as a traditional SIGINT analysis cell. The geospatial engineer team supports a limited geospatial engineer team at the Kandahar intelligence fusion cell and works closely with subordinate 3rd Brigade Combat Team battalions when they require geospatial engineering products through an efficient digital RFI process.

The Rakkasans IRC may not embody the traditional role of a brigade intelligence support element but it "supports the BCT and its subordinate units "through...analysis, and dissemination of intelligence information." from home station to the operational units deployed in theater. ✨

Endnotes

1. U.S. Army Field Manual (FM) 3-96, Brigade Combat Team (Washington, DC: U.S. Government Printing Office, 8 October 2015), 6-8.
2. Ibid.

CW2 Wolfgang is currently serving as operations OIC for 3rd Brigade Combat Team, 101st Airborne Division's intelligence reachback cell and brigade combat team senior all-source intelligence technician. His previous assignments include: 2nd Brigade Combat Team, 1st Cavalry Division senior all source intelligence technician; regional command north deck chief, Information Dominance Center, Afghanistan Interim Joint Command and training developer and critical task list manager career management field military occupational specialty (MOS) 35F – intelligence analyst, U.S. Army Intelligence Center of Excellence.

MI Professional Bulletin

Has a new website!

The current issue of MIPB is available on the front page of our website at <https://www.ikn.army.mil/apps/MIPBW>.

To access all of our issues back to 1974, click the archive tab and login with your CAC.

Establishing an Intelligence Reachback Cell

by Chief Warrant Officer Two Orrin Thompson



The downsizing of U.S. Forces in operational environments has significantly reduced the number of uniformed intelligence professionals operating within a theater and created a greater need for the establishment of an intelligence reachback cell (IRC). More often than not, a maneuver commander is willing to assume risk by leaving an intelligence Soldier in garrison to bring another trigger puller for security or mission requirements. Although this is not always the best solution, the reality is that the continued downsizing of troop strength leaves a commander with few alternatives. With this reality of the operational environment, commanders identified the need for their own IRCs as critical. This article will focus on firsthand experiences of the 3rd Brigade Combat Team, 101st Airborne Division (Air Assault) establishing an organic IRC. It will discuss some best practices identified for the establishment of IRCs, personnel considerations, as well as some basic planning factors.

Establishment of an Intelligence Reachback Cell

This is a lengthy process that requires adequate preparation time and begins immediately after identifying the need for an IRC. This stage of development is the hardest to get started. There are many moving parts across the intelligence enterprise making communications with commanders and their staff critical to mission accomplishment. The first task is not to identify the personnel who will form the reachback cell but to establish a feasible workspace and identify the required operating systems.

Coordination for Sensitive Compartmented Information Facility Workspace. Fortunately, for the 101st Airborne Division a tactical sensitive compartmented information facility (T-SCIF) is available where every brigade has its own room for day-to-day operations. A downfall to this facility is when not conducting preparation for deployment or a rotation at one of the Army's combat training centers these

rooms largely go unoccupied. This created the immediate issue of needing to establish the intelligence architecture with operating systems and placement of systems for workspaces. A significant benefit of these pre-identified brigade work areas is that the division had already recognized they were not large enough to support forward deployed unit operations. Therefore, the division identified two additional rooms specifically for IRCs. This enabled the division to support multiple deployed brigades with additional workspace.

In essence, the IRC is a fully functional brigade intelligence support element with slightly reduced staffing. Size became a determining factor in the need for space to support the different

sections operations. Having the fusion cell in a separate room from the other sections best enabled our production without outside interference. We paired the smaller-sized human intelligence (HUMINT) and geospatial intelligence (GEOINT) cells together and in the same building with the fusion cell. The basis of this decision was completely upon space allocation due to room size and computer ports available, not because of any mission requirement.

Establishing the Intelligence Architecture. When first establishing computer space our unit identified the desire to be on multiple networks (e.g. Trojan and Department of Defense information network [DODIN] continental United States [CONUS]) in the event one of the networks failed. This would provide the IRC with redundancy for our numerous laptop computer systems, such as the Distributed Common Ground System—Army components. The larger systems, such as GEOINT Workstation and the Intelligence Fusion Workstation remained on the Trojan network due to system accreditation. Integration of the military occupational specialty (MOS) 35T's, military intelligence systems maintainer/integrator, into the process of establishing our networks and computer system architecture was critical during this planning phase. Some of the sub-tasks required

Establish the IRC Sub Tasks

- ◆ Coordinate workspace through building owners
- ◆ Coordinate SCIF certifications
- ◆ Identify communications and network mediums
- ◆ Prepare system network architecture
- ◆ Coordinate with property owners for equipment use and allocation
- ◆ Coordinate through S-6/G-6 for T-SCIF equipment list
- ◆ Coordinate through S-6/G-6 for allocation of IP addresses
- ◆ Create a production repository

update of the brigade's equipment list within the T-SCIF through the division G-6 and allocation of required internet protocols for DODIN CONUS systems.

Communication capabilities are a critical point that requires detailed attention. Establishing contact with the current forward deployed elements and previously established IRCs will help identify how they conducted meetings and over what mediums. These forums will likely be the same ones your unit will use during the relief in place with the other unit. Discussing these mediums with your commander will give you a head start on getting these capabilities established to ensure open and easy communication when your unit deploys.

Units conducting operations in Afghanistan often have different capabilities and requirements than units have at CONUS locations. For example, most meetings in Afghanistan occur over a video teleconferencing (VTC) capability. The most commonly used VTC capability is a TANDBERG. Within CONUS, the Army no longer uses the TANDBERG 1000 or below on its networks. This results in the loss of this easy to use VTC capability until the unit:

- ◆ Purchases updated equipment (not a likely scenario, as higher priorities receive funds first).
- ◆ Finds direct access to a different VTC capability.
- ◆ Dismisses VTC capability from the IRC and utilizes a different communication option (e.g. secure voice over internet protocol).

Identification and Coordination of Equipment. Predominately within a brigade combat team (BCT), the military intelligence company (MICO) holds a majority of the supporting equipment needed by the IRC (e.g. DCGS-A components, VTC equipment, etc.) in comparison to the BCT S-2. This means communication between the MICO commander, who owns the equipment, and the supported commands staff in order to maintain property books. An open and candid conversation between the respective property owners greatly reduces the stress of identifying where systems are coming from and where they will be utilized.

Create a Production Repository. Creation of product repositories is required during this stage to collaborate efforts between forward deployed elements and pre-established IRCs. This takes some time to generate dependent upon the server used. For example, we utilized Intelink (Intel Share) to create these repositories, as this site is accessible from anywhere in the world. This alleviates issues of inaccessibility to sites due to firewall restrictions and email size limitations. This is a good best practice regardless of deployment status, as it will remain accessible for the unit and personnel throughout the years.


Personnel

Identifying the right Soldier for the right job is essential. There are multiple elements the personnel selected will effect—primarily capabilities! Do you have enough personnel to accomplish the mission? Are they the right people? In some cases, more is not always better. There needs to be a good mixture of leaders (officers, warrant officers, and noncommissioned officers [NCOs]) and junior Soldiers. This section will focus primarily on the Fusion cell of the IRC, but the considerations and best practices are applicable to all sections. See the next page for a comprehensive list of personnel considerations.

The first IRC the 3rd Brigade Combat Team established was composed of junior leaders and junior Soldiers. They lacked the practical knowledge skillset and leadership to train and mentor, which directly affected their ability to provide supporting intelligence. The leaders were too new to be highly effective as senior leaders. The junior Soldiers were mostly comprised of people who were not available to deploy. This immediately set the IRC up to fail as all the experienced leaders and Soldiers deployed.

The second IRC, which I am a part of, is composed of three MOS 350Fs, all-source intelligence technicians; four MOS 35F, intelligence analyst; and five MOS 35M, HUMINT collectors. I will admit initially it was thought the Fusion Cell would have a severe handicap from being staffed with a significant number of HUMINT personnel, but utilizing the MOS 35M's to fill analyst positions has been highly successful. The decision to use HUMINT collectors in this manner was due to a lack of intelligence analysts within the brigade who did not or could not deploy.

The most significant issue observed regarding personnel and the IRC is finding the optimum balance of skills between those deployed and those left to staff the IRC. Instead of deploying a mix of experienced/inexperienced analysts and leaders, a unit will most often take the experienced and leave the inexperienced. This does not provide the inexperienced Soldiers opportunity to improve, nor does it provide the experienced Soldiers the opportunity to lead. There is a middle ground, which, if met better serves our units, Soldiers, and overall capabilities.

Make sure you have a cohesive team. Your team will make or break your IRC. You do not all have to be friends and get along, but the cohesive group will make your next several months not only bearable but also enjoyable. These have been some of the 3rd BCT, 101st Airborne Division's lessons learned, best practices, and planning considerations for establishing an IRC. Each unit will of course discover their own techniques, but I hope I have provided some helpful insights. 

Personnel Considerations for IRC Operations

1. Do Soldiers possess the proper clearances with appropriate read-ons?

- ◆ If read-ons are required, submit request paperwork immediately.
- ◆ If Soldiers do not have the proper clearance levels, it is too late to begin the process. You cannot assume the risk of having uncleared personnel working in an environment they are not supposed to enter. This is kind of a given, but it is not unheard of for it to be attempted anyway.

2. Do Soldiers have the user accounts and permissions required to perform duties?

- ◆ The basics would consist of NIPRNET, CENTRIXS, SIPRNET, JWICS (if applicable).
- ◆ Other user accounts will depend upon what will support the forward-deployed forces. A good rule to follow is plan for using the same communications capabilities, databases, and tools as the forward element. This will enable you and the forward element to not only pass information to each other, but also enable you to find the same information to discuss what you are working on.

3. Do personnel have adequate training to work the intelligence mission?

- ◆ The 3rd BCT all-source intelligence technicians developed a certification program for the fusion cell of the IRC. We identified what skills were needed to operate at a minimum baseline of understanding. We utilized some of the products we created during previous briefings to the brigade commander to set this baseline. In addition to basic demonstrations of "buttonology," this also consisted of pulling data from repositories and ingesting that data into product development. After completing these basic tasks, analysis and briefing the group completes the basic certification.
- ◆ Sending Soldiers to a Foundry or home station-training course will be highly successful.

4. Do the leaders have Special Security Office/Special Security Representative certification so you can open and close your SCIF properly?

- ◆ This may seem like a small detail if you have one or two, but you need to ensure you are within compliance of your brigade, division, and higher headquarters policy.

5. Do you have command emphasis? Has the BCT commander acknowledged your mission and identified it as one of their priorities?

- ◆ Knowing tasking and missions will come down from rear-detachment units you MUST sit down with your command early to identify the IRC as a priority.
- ◆ A best practice, which our commander implemented, is to publish an operations order to highlight the mission and responsibilities of IRC personnel. It also indicated IRC personnel were not subject to additional duties or details to include staff duty. This provided us the ability to operate shifts without issues and accomplish the mission.
- ◆ The 3rd BCT took this a step further and attached all IRC personnel to the brigade's Headquarters and Headquarters Company. This brought all IRC personnel into one organization and prevented the parent units in the rear detachment from interfering with operations.
- ◆ The order authorized IRC personnel separate rations, as shift work often does not coincide with dining facility hours.
- ◆ After receiving support from the brigade command team, make sure to have the same support from the company command team, as it makes life much easier.

6. Do you have a clearly identified rating scheme with responsibilities?

- ◆ Make sure your officers and NCOs are clear about rating schemes and the requirements of performance counseling.
- ◆ Make sure the team knows who is in charge and the chain of command. Personnel, leadership included, will still have regular appointments, meetings, and other events that will take them away from the work place.

7. Do you have a plan for time off?

- ◆ Daily IRC operations are similar in many aspects to those of deployed operations. However, down time for personnel is still going to be required.
- ◆ IRC Soldiers will go home every day, unlike deployed Soldiers. Therefore, you will still have the everyday problems of the normal garrison environment. There will still be doctor appointments, family issues, illnesses, and other unseen factors that will remove Soldiers from duty.
- ◆ Planning with this mindset will make it easier to adjust when things happen and allow for some much needed down time.

Editor's Note: Photo on the previous page depicts 3rd Brigade Combat Team, 101st Airborne Division Soldiers running past the Operational Base Fenty entrance in eastern Afghanistan during the Train, Advise, Assist, Command-East Soldier and Noncommissioned Officer of the Year competition, Aug. 5, 2015. (CPT Charles Emmons, 3rd BCT -101ABN Public Affairs).

CW2 Orrin Thompson joined the Army in 2003, some of his previous assignments include: S-2 NCOIC for 1st Battalion, 77th Armored Regiment from 2008-2010, Operations/Intelligence NCO for 2nd Battalion, 2nd Field Artillery Regiment from 2010-2012, TAAC-E collection manager from 2014-2015, and currently serving as the IRC dayshift fusion chief for 3rd BCT, 101st Airborne Division.



Combat Aviation Brigade Intelligence Operations

by Chief Warrant Officer Two Tia Caywood

Field Manual 2-0, *Intelligence Operations*, states, “the brigade combat team (BCT) S-2 is the principal advisor to the BCT commander and staff for all matters concerning the intelligence warfighting function.”¹ The role of a combat aviation brigade (CAB) S-2 is further described in Army Techniques Publication 3-04.1, *Aviation Tactical Employment*, as “focusing on collecting and analyzing information about threats to friendly aircraft, air and ground threat trends, indicators and warnings, and pattern analysis, but also works closely with the operations section for mission analysis and the targeting process.”² When compared to a BCT S-2 section’s duties and responsibilities, the CAB S-2 is not very different but must develop aviation-centric intelligence, such as helicopter landing zone threats and weather impacts on aircraft. However, the organizational structure of a CAB S-2 is different from BCT S-2 in that the CAB S-2 only consists of all-source intelligence analysts and geospatial intelligence imagery analysts while the BCT S-2 intelligence cell receives augmentation from the brigade engineer battalion’s military intelligence company making it more robust. These differences force the leaders within the CAB S-2 to become well versed in the myriad intelligence disciplines in order to provide pertinent and fused intelligence to the CAB commander. As a CAB S-2 all-source intelligence technician, this is a position I have found myself experiencing.

The CAB can support multiple brigade, division, or corps operations in task-organized aviation teams, which leads to the questions: what is the CAB’s operational environment (OE), and how does the S-2 present the ground and air threats to the commander, allowing him to visualize the OE to maneuver his aircraft in support of ground operations? Before identifying the threat, it is first necessary to understand the capabilities and limitations of the CAB’s rotary wing assets.

A Note on Training

Soldiers occasionally arrive to certain atypical assignments feeling they did not receive adequate preparation from their institutional training. This is unfortunate, but the institution should not be preemptorily blamed for this shortcoming. U.S. Army Training and Doctrine Command (TRADOC) institutions, like the U.S. Army Intelligence Center of Excellence (USAICoE), have a challenging process to determine what is trained and how it is trained. TRADOC governs the process and oversees all the available resources (training time, people, equipment, etc.).

The January – March 2016 issue of MIPB contained an article titled, “No USAICoE Course at Rest,” by Ms. Beth A. Leeder, Director, Teaching, Learning, and Technology Division, USAICoE. This article explains in some detail, yet in easy to understand language, the very important process that TRADOC uses for training development. It also discusses how you can be a part of the process. Input from the operational force is necessary and encouraged.

Having spent most of my Army career in BCTs, I had no previous experience with focusing primarily on air assets and threats, nor had I received any previous training on those subjects from military schools. Prior to assignment to the CAB, an introduction to Army Aviation (through resident institutional training or distance learning) would have been useful. It could have explained what a pilot needs to know about the ground (e.g. opposing force air defense tactics, threat weapon systems, electronic warfare) and how ground commanders can improve their use of rotary wing assets (e.g. targeting for attack aviation, Army airframes and capabilities, aviation tactics).

When assessing the threat to rotary wing aircraft, the CAB S-2 section places an emphasis on what the airframe can and cannot do. The aviation mission survivability officer (AMSO) is a valuable asset for support in connecting airframe capabilities to threats. I have worked with the AMSO

to develop training and helped other intelligence sections understand various aspects of aviation operations.

With the CAB's ability to support multiple units at the same time, it is important to synchronize operations with the supported unit's intelligence section as early as possible. In my experience, this facilitates transparency across echelons, provides understanding of and delineates tasks, and ensures all air and ground factors are included. Establishing these relationships allows the CAB S-2 to identify intelligence gaps, risks to the force, and mitigation. Additionally, synchronizing with supported units early allows us to establish an intelligence architecture that both intelligence sections can access. The preferred systems are the Distributed Common Ground System- Army and Geospatial Intelligence Workstation because of the ability to share intelligence via an Intelligence Fusion Server or through the Ozone Widgit Framework. Synchronizing with the supported units early and often has proven beneficial for CAB intelligence operations because it allows the S-2 to provide the CAB commander a detailed depiction of the battlefield throughout the planning and operational phases.

Finally, establishing positive relationships with the CAB S-3 and specialized brigade staff such as the safety officer, standardization officer, and the AMSO (all of which are senior pilots) aids in establishing a clear but detailed intelligence picture. These relationships are vital during the military decision-making process and operations planning. I have relied heavily on the AMSO when refining the air threat in relation to enemy ground operations. Additionally, getting the safety and standardization officers' input allows

the S-2 section to understand aircraft capability and limitations in a given environment. We all have the mission of preserving our fleet and protecting our pilots—that common goal is where our relationship starts. I believe good communication and rapport with the CAB S-3 and AMSO, at a minimum, compensates for intelligence training focused solely on land operations.

Serving as a CAB all-source intelligence technician has allowed me to develop a broader knowledge base and expertise in air threats while providing analysis up to the corps level. As the only all-source intelligence technician in the CAB, my success is dependent upon the relationships developed with the brigade staff, the synchronization with the supported unit's intelligence sections, and working closely with the pilots. If I had been asked what a combat aviation brigade does prior to my assignment to 1st Combat Aviation Brigade, 1st Infantry Division, I would probably have said something similar to air assaults, reconnaissance, and personnel movement. Today, I can explain exactly how the CAB supports and is a valuable combat multiplier for brigade, division, or corps operations. ✨

Endnotes

1. U.S. Army Field Manual (FM) 2-0, Intelligence Operations (Washington, DC: U.S. Government Printing Office [GPO], 15 April 2014), 2-3
2. U.S. Army Techniques Publication (ATP) 3-04.1, Aviation Tactical Employment (Washington, DC: U.S. GPO, 13 April 2016), 1-11

CW2 Tia Caywood serves as the 1st Combat Aviation Brigade, 1st Infantry Division all-source intelligence technician. Her previous duty assignments include Fort Drum, New York; Yongsan, South Korea; Fort Bliss, Texas; and Fort Riley, Kansas.



Photo by SSG Warren W. Wright Jr., 1st ABCT

A pair of M2 Bradley Fighting Vehicles from Company C, 1st Battalion, 16th Infantry Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division, participate in a live-fire exercise May 6 at a Fort Riley Training Area as an AH-64 Apache from the 1st Combat Aviation Brigade, 1st Inf. Div., flies overhead. The event was a part of operation Danger Focus, a month-long exercise designed to prepare the "Devil" brigade for its upcoming rotation to the National Training Center at Fort Irwin, California.

Doctrine Corner

Intelligence Doctrine to Win in a Complex World

Note: This article is an excerpt from a draft white paper prepared by Doctrine Division, Capabilities Development Integration Directorate, U.S. Army Intelligence Center of Excellence. This paper discusses the need to update key intelligence doctrine in an effort to stay abreast of the challenges the intelligence war fighting function faces from the future operating environment.

As articulated in the Army Operating Concept, the future is unknown, unknowable, and extremely complex. This paper describes the ongoing effort to account for significant changes in How the Army Fights and combined arms doctrine. As a result of those changes, we will need to update our key intelligence doctrinal publications including Army Techniques Publication (ATP) 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*. The intent of this paper is to start a constructive dialogue with key doctrinal proponents and various intelligence units/organizations on how we plan to account for changing doctrine within ATP 2-01.3.

Following the successful implementation of Army Doctrine 2015, we are faced with the dilemma of quickly updating our publications to remain relevant while protecting our doctrinal foundations, which remain solid. In updating our publications, we have to account for both the major trends the Army is facing and the stark intelligence challenges that are now a reality.

Converging Trends

The four major trends that challenge the intelligence warfighting function are—

- ◆ A sophisticated and capable hybrid threat.
- ◆ The inherent complexity of the operational environment.
- ◆ Technological advances on the battlefield.
- ◆ The corresponding demands on the intelligence warfighting function.

The Combined Arms Doctrine Directorate (CADD) white paper titled, “Field Manual 3-0: Operations, Doctrine to Win in a Complex World” does a good job describing the first three of the major trends. Assessing the intelligence implications of each trend and then looking at the combination of those implications reveals significant current and future demand on the intelligence warfighting function.

Sophisticated and Capable Hybrid Threats. In the future, the United States will most likely face adversaries who combine all available means (traditional, irregular, disruptive, and catastrophic) to achieve a desired effect or effects. The Army must consider that all operations will routinely encounter hybrid threats that combine traditional, irregular, and disruptive means; and the Army must also be prepared to address catastrophic means when encountered. The sophisticated combination of different threat capabilities adds to the challenge of defeating an adversary. Further, the ability to quickly adapt a particular combination of threat capabilities to the situation enable enemies to capitalize on perceived vulnerabilities, combining sophisticated weapons, command and control, propaganda, cyber activities, and combined arms tactics to engage U.S. forces when conditions are favorable. Finally, hybrid threats may use global networks to influence international perceptions of the conflict and shape global opinion.¹

Complexity of the Operational Environment. In the immediate future, nation states and non-state groups will continue to compete for a place in the world order and for access to resources. This competition when combined with the dynamics of a growing global population, regional instability, and continued migration to and friction within dense urban areas is a challenge for the United States. The rate of human interaction continues to increase, and as world connectivity increases, regional populations around the globe have exposure to more information, which creates an increased risk for instability. Information is often a catalyst for action that may result in conflict with traditional hierarchies. In some cases, there is even an increased interest among international competitors to increase their control of the global commons. Friendly forces must be prepared to fight and win in demanding environments like jungles, mountains, deserts, littoral expanses, and mega-cities.²

Technological Advances on the Battlefield. Global connectivity has accelerated the spread of many technologies with military applications. Highly developed nation states continue to develop and proliferate advanced weapon systems. The rapid development of, and ease in procuring, commercial off-the-shelf technologies allow our adversaries to significantly increase their capabilities. The proliferation of

weapons of mass destruction, sophisticated anti-access area denial systems, long-range precision strike capabilities, cyberspace capabilities, and counter-space capabilities will present challenges and may provide our adversaries some capability overmatch. Some examples include—³

- ◆ Cheap but effective anti-tank missiles that can defeat our armor.
- ◆ Air defense missiles that could negate our air operations.
- ◆ Supersonic anti-ship missiles that could degrade naval operations.
- ◆ Electromagnetic spectrum systems that degrade friendly position, navigation, timing, and satellite communications capabilities, and friendly force tracking.

Demands on the Intelligence Warfighting Function. The intelligence warfighting function challenge starts with the requirement to continually understand sophisticated and capable hybrid threats and complex operational environments previously discussed. We must orchestrate adequate collection against those threats in complex environments, not only in all domains but also across dozens of significant aspects within each domain. Significant aspects include—

- ◆ Subterranean networks.
- ◆ Difficult-to-navigate littoral slums.
- ◆ Dense urban areas.
- ◆ Illegal sub-economies.
- ◆ Cybercrimes.
- ◆ Use of small drones.
- ◆ Space considerations.
- ◆ Culturally diverse populations.
- ◆ Violent border regions.

Orchestrating collection against all of these significant aspects of the environment is further complicated by the fact that intelligence operations are inherently joint and increasingly rely on other unified action partners to meet the ever-increasing number of requirements. This reliance on unified action partners presents great opportunities but also requires skill.

After information is collected, we must quickly process (from a giant pool of disparate data types), analyze, and produce intelligence that meets the commander's requirements addressing the threat and other relevant aspects of the operational environment. In many cases, our intelligence products must predict the actions of a sophisticated threat and/or proxy threat while simultaneously addressing the following interrelated factors:

- ◆ A dynamic political realm.
- ◆ Socio-cultural considerations.
- ◆ Conditions that are causing instability.
- ◆ Very detailed civil considerations within an urban or dense urban area.
- ◆ The media and social media.

Reframing the Challenge

The task of updating our doctrine spans from accounting for changing combined arms doctrine to better describing our intelligence challenge to spinning out the right sequence of changes across most if not all of our doctrinal inventory. No single set of changes to the Intelligence Preparation of the Battlefield (IPB) publication, Intelligence Support to Cyber Operations, or any two or three publications will be adequate. We must maintain a body of synchronized intelligence doctrinal publications that are current and relevant.

Keeping the Fundamentals

As the Army transitioned and surged to conduct operations in Iraq and Afghanistan, we learned a number of doctrinal lessons. Our first step was to assess our fundamental doctrine and to relook our older doctrine covering low-intensity conflict. The results of that effort validated our most fundamental doctrinal constructs and confirmed the value of updating older doctrine to address counterinsurgency and stability tasks in a complex environment. Then from that base, we introduced new doctrinal topics like—

- ◆ Counter-improvised explosive device analytical techniques.
- ◆ Increased emphasis of civil considerations.
- ◆ High-value individual targeting techniques.
- ◆ Multi-function teams.
- ◆ Company intelligence support teams.
- ◆ Processing, exploitation, and dissemination (PED).

Following the doctrinal surge, we executed our portion of the larger Army Doctrine 2015 effort. As a result, we are confident that we have an inventory of intelligence publications that provide a solid doctrinal foundation for all decisive action tasks: offensive, defensive, stability, and defense support to civil authorities. Our foundational doctrinal constructs like the intelligence process, IPB, planning requirements and assessing collection, and our analytical frameworks and techniques are optimal to deal with current and future operations. However, the task at hand is to update our techniques to better account for complexity. We must account for many specific considerations across

all domains within our publications without merely creating “catchy” new terminology devoid of substance.

The Right Sequence of Updates

CADD is using the right approach to update all the Army Doctrine Publications (ADPs) and Army Doctrine Reference Publications (ADRP) and create a new FM 3-0. The Intelligence Center of Excellence will use an approach similar to CADD’s; we will follow a top-down deliberate and meticulous approach to updating our doctrine. In fact, the campaign already started with our participation in the CADD-led efforts to create a new FM 3-0 and synchronize the updates of the other ADPs and ADRPs based on ADRP 3-0, Operations. In line with those CADD efforts, we will update ADP and ADRP 2-0, Intelligence. We will also execute focused doctrinal updates covering—

- ◆ IPB for multi-domain battle.
- ◆ Specifics on analysis for cyberspace operations.
- ◆ Developing the intelligence architecture.
- ◆ Analyzing social media.
- ◆ Company intelligence team and multifunction platoon operations.

During each successive FY, we will update focused areas to make sure our doctrine supports the complexity of emerging demands on the intelligence warfighting function. That way we can maintain our foundational doctrine while improving and building out new considerations with better descriptions, graphics, tools, vignettes, and example products.

Updating our Intelligence Preparation of the Battlefield Publication

Taking a closer look at how we plan to update ATP 2-01.3, IPB, provides some insight into the approach we will use to eventually update all our publications to account for emerging trends and evolving combined arms doctrine. As we update our publications, we will assess those publications based on how well the techniques address—

- ◆ Meeting the challenge caused by a sophisticated and technologically enhanced hybrid threat.
- ◆ Meeting the challenges caused by a complex operational environment across all relevant environmental aspects within each domain and across domains.
- ◆ Leveraging the intelligence enterprise to solve more complex situations and meet the ever-growing demand on Army intelligence.

We have to address only the first two perspectives with ATP 2-01.3, since it is a process-oriented publication and does not address the entire scope of analysis and tech-

niques to leverage the intelligence enterprise. We will address those specific techniques in our echelon and other publications. Changes to the IPB ATP will necessitate a number of corresponding changes in the Intelligence Analysis and other ATPs, especially with respect to emphasizing the importance of generating intelligence knowledge as a precursor to IPB.

Based on our initial assessment of ATP 2-01.3—

- ◆ The current IPB framework of steps and sub-steps is already optimized to account for any new threat and range of complex environments.
- ◆ While our IPB framework is sound, there is an immediate need to provide descriptions, graphics, tools, vignettes, and example products across all the steps of the IPB process to account for emerging trends.
- ◆ We must provide adequate details covering all domains (specific to the operational environment), significant aspects of each domain, specific hybrid threat capabilities and vulnerabilities for each domain, and how the threat can use cross-domain capabilities to attain an operational advantage.
- ◆ We need to add vignettes of IPB in a dense urban area and against a more sophisticated hybrid threat in chapter 9, IPB Considerations for Unique Environments.

Some of the specifics of the assessment include the following:

Step 1, Define the Operational Environment. The most important aspect of step 1 is *identify significant characteristics within the operational environment*. This sub-step ensures the staff accounts for various operational and mission variables, which are inherently multi-domain and sometimes cross-domain. The staff starts with those intelligence products that are developed during the generate intelligence knowledge task and the operational frames developed during the Army Design Methodology. Through this sub-step, the staff ensures the IPB process addresses all relevant aspects of the threat and environment. We need to improve the discussion to better articulate the multi-domain nature of the operational environment, the breadth of those aspects, and domain interdependencies (for example, a friendly country’s debarkation capabilities, threat drone capabilities, and threat cyber capabilities).

Step 2, Describe Environmental Effects on Operations. An important aspect of step 2 is *describe how civil considerations can affect friendly and threat operations*. This sub-step was added during operations in Iraq and Afghanistan to better account for the complexity of the operational

environment. We need to improve this discussion to provide better staff tools and example products (for example, satellite communications coverage charts, radio-frequency effects, subterranean networks, dense urban area infrastructure, and press and social media influences).

Step 3, Evaluate the Threat. The two sub-steps of step 3 are *identify threat characteristics and create or refine threat models*. These two sub-steps provide a flexible way the staff can account for every capability of a hybrid threat in each domain and significant threat aspects of each domain (for example, subterranean, maritime, air, space, cyber, and criminal or proxy capabilities). In some cases, the staff should identify methods the threat uses to achieve effects across domains for an operational advantage. We need to expand the types of threat models and expand the list of capabilities (for example, threat drone and counter-UAS capabilities) that the staff should consider when developing a threat model. Threat models can extend across multiple domains. These changes will require developing some new descriptions, graphics, tools, and examples.

Step 4, Determine Threat Courses of Action. The two sub-steps of step 4 are *develop threat courses of action and develop the event template and matrix*. These two sub-steps are a natural continuation of the work performed in steps 2 and 3. They provide a flexible method to account for the threat and other significant characteristics of the environment (i.e., all relevant domains and significant aspects of each domain). This enables the staff to account for the entire operational environment within the subsequent steps of the military decision making process. We need to

expand the discussion of how situation templates are used. Additionally, we must develop a number of different example templates to cover the potential breadth of capabilities a hybrid threat may possess. There needs to be emphasis on the discussion of how the threat will use capabilities and effects across various domains to achieve an operational advantage. An example of a cross-domain capability is a threat ground force's use of small drones controlled with a software program that sends commands over the electromagnetic spectrum allowing the threat to monitor friendly naval forces.

Conclusion

As we account for significant changes in How the Army Fights and combined arms doctrine, we must maintain a body of synchronized intelligence doctrinal publications that are current and relevant. Our intelligence foundational doctrinal constructs are already optimal to deal with current and future operations. However, the task at hand is to update our techniques to better account for complexity. We must account for many specific considerations across all domains within our publications. ✨

Endnotes

1. Combined Arms Doctrine Directorate, Mission Command Center of Excellence, Combined Arms Center, "Field Manual (FM) 3-0: Operations, Doctrine to Win in a Complex World", (white paper, version 1, 30 September 2016), 2-3. The majority of this paragraph is taken directly or paraphrased from the source document.
2. Ibid., 4.
3. Ibid., 4-5.

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.





by Lieutenant Colonel Matthew T. Archambault, Captain Franklin G. Peachey,
Captain Sean D. Hayball, and Staff Sergeant Drew D. Lincoln

Introduction

The rapid expansion of the commercially available small unmanned aircraft systems (sUASs) enables many countries to easily collect information to support offensive and defensive operations. Employment of the sUAS is significant to modern operations because it provides collection for reconnaissance, target acquisition, and battle damage assessments. At the Joint Multinational Readiness Center, the 1st Battalion, 4th Infantry Regiment (1-4 IN) (known as the “Warriors”)—the U.S. Army European Command’s Opposition Force Battalion—replicates real-world threat tactics, techniques, and procedures (TTP) to engage and challenge rotational training units (RTUs). The Warriors’ use of the sUAS as a collection and target acquisition asset is crucial to their success and provides lessons for the entire U.S. Army in terms of practical considerations as well as tactical employment.

This article is a broad assessment that—

- ◆ Focuses on the sUAS threat posed to RTUs.
- ◆ Briefly compares the relative combat power of the Warrior Battalion to RTU’s.
- ◆ Discusses the factors limiting sUAS employment by RTUs.
- ◆ Describes best practices and preferred employment techniques from the 1-4 IN’s perspective.
- ◆ Offers recommendations for future RTUs to effectively employ sUASs as part of the combined arms effort.

The sUAS Threat to RTUs

In the last three decades, technological advancements have revolutionized the modern battlefield. Today, commanders have more information about the battlefield than at any other point in history. One of the most important links in this transformation is the proliferation of sUASs in increasing quantities and capabilities. Today, these assets can provide a real-time stream of information that feeds commanders’ decision making and their accurate targeting of enemy assets. Despite this significant impact, RTUs lack an appreciation for the lethality tied to information collected from sUASs.

This lack of appreciation has been repeatedly observed in the training environment, where Soldiers often ignore the sUAS completely or assume a 1-4 IN Raven system is friendly.¹ Incoming units receive briefings on the presence of enemy sUASs; however, activity is routinely not reported or countered. Units allow their battle positions, seams, attack positions, and schemes of maneuver to be reconnoitered. This unimpeded collection assists the 1-4 IN in answering priority intelligence requirements to exploit the RTU’s vulnerabilities.

The 1-4 IN collection assets effectively acquire and pass-on time-sensitive targeting information, which queues the targeting cell, generally resulting in continual RTU losses. These largely unanswered reconnaissance and fires on RTU positions enable the 1-4 IN to effectively neutralize RTU courses of action both offensively and defensively. When all aspects of these collection opportunities are combined, a smaller unit is capable of rapidly neutralizing or defeating a much larger force. A timely real-world example occurred in Eastern Ukraine, where this reconnaissance and target acquisition ability combined with mass fires resulted in the destruction of two Ukrainian mechanized battalions in a matter of minutes by rebel forces.²

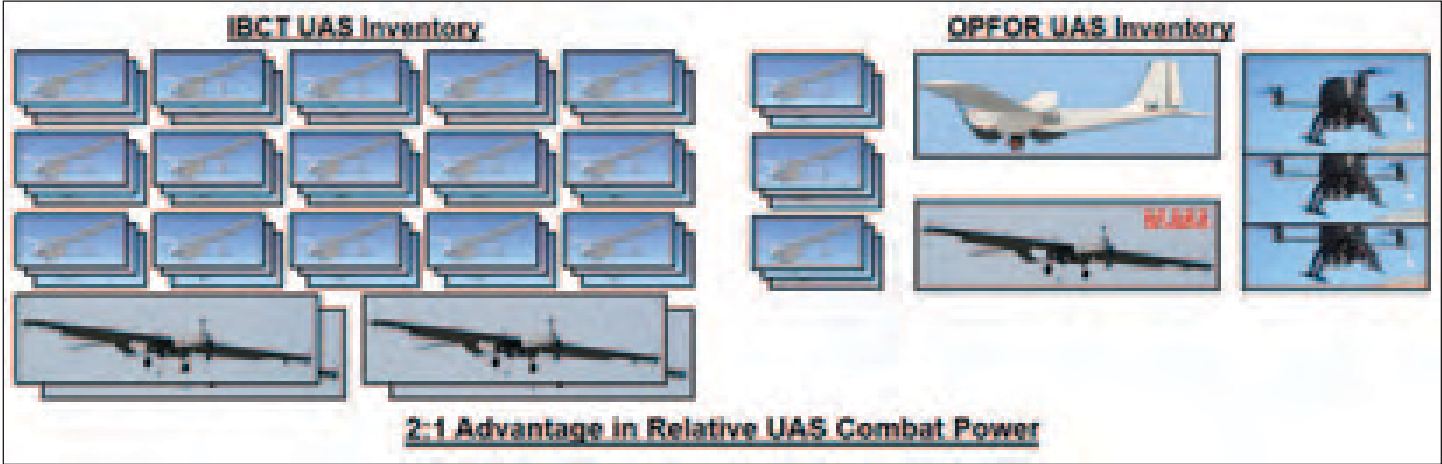
Another observed vulnerability in RTUs is poor password protection or operations security (OPSEC) procedures when employing sUASs. This enables open viewing of their sUAS feed and allows the 1-4 IN to better assess the current RTU common operational picture of its elements. The Joint Multinational Readiness Center has observed this OPSEC vulnerability across much of the RTU digital infrastructure. Despite the various threats outlined, RTUs can disproportionately exploit these capabilities based on their superior relative combat power to the 1-4 IN.

Comparison of Relative Combat Power and Results

RTUs have at least a two-to-one advantage in collection capability compared to the 1-4 IN’s. In an infantry brigade combat team (IBCT), this collection capability usually comprises 15 RQ-11B Digital Data Link systems, each composed

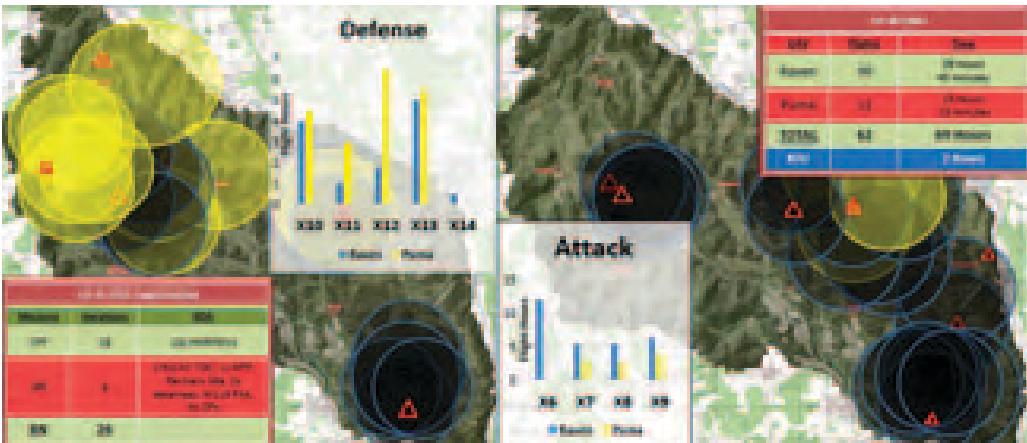
of three Raven systems. A typical allocation includes three systems per reconnaissance squadron, four per maneuver battalion, two per artillery battalion, one per support battalion, and one system in the special troops battalion. An IBCT also has four Shadow RQ-7BV2 unmanned aerial vehicles in a tactical unmanned aerial vehicle platoon.³ This provides an IBCT 49 airframes for employment across its area of operations.

In comparison, the 1-4 IN has only three Raven systems, three rapidly deployable aerial surveillance systems (RDASSs), and one Puma system, giving the unit 13 airframes to employ. To replicate a near-peer capability accurately, the 1-4 IN also employs a virtual unmanned aircraft system (UAS) capable of two flights per day. Despite this advantage in sUAS capability, the 1-4 IN routinely outmatch RTUs in the employment of these systems.



Based on the reporting of sUAS use in ongoing conflicts, the 1-4 IN has made a deliberate effort to accurately replicate an active sUAS environment. During the 14 days of Exercise 16-04, the 1-4 IN flew 69 hours of sUAS coverage compared to the RTU’s 2 hours (See Saber Junction 2016 graphical UAS rollup). During the 13 days of Exercise 16-06, the 1-4 IN had aerial collection assets on station in the battle and disruption zones even longer, at more than 100 hours compared to the RTU’s 4 hours (See Swift Response 2016 graphical UAS rollup on the next page).

The 1-4 IN’s combat power is enhanced significantly due to its disproportionate advantage in information collection. The 69 hours or more of uncontested sUAS coverage enabled unfettered target acquisition, the accurate identification of emplaced RTU obstacles, and the exploitation of the RTU’s coordination seams. By maintaining sustained and accurate fires, bypassing emplaced obstacles, and massing forces at the decisive point, the 1-4 IN successfully used sUASs to maximize its combat power. As the capability to employ sUASs expands within the 1-4 IN, the presence of sUASs on the battlefield and the battalion’s combat power will grow.

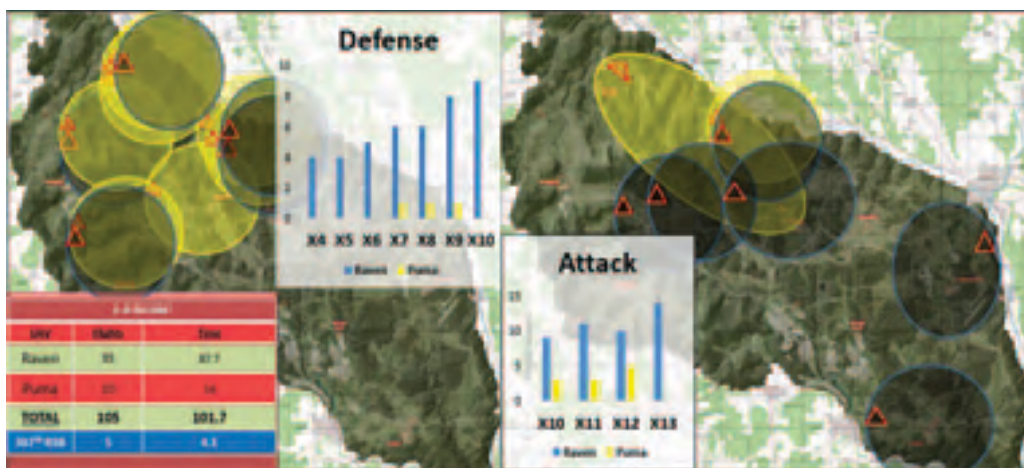


Employment Limitations of the sUAS

A critical limiting factor to sUAS employment is the RTU’s mindset toward sUASs. Most sUAS employment experiences stem from a largely permissive counterinsurgency battlefield. Many RTUs ineffectively transition their planning and training for operations in a competitive sUAS environment. Effective development and execution of vital tactical integra-

tion techniques and well-trained counter-sUAS procedures are lacking, resulting in ineffective or nonexistent communications within the RTU about friendly or enemy sUAS operations.⁴

A lack of prioritization of sUAS employment during a RTUs training cycle at the home station is another limitation resulting in untrained operators and undeveloped operating procedures. The effective employment of a RTU’s sUAS capa-



1-4 IN UAS Rollup. Swift Response 2016.

bilities must begin, and be maintained at the home station. Only command-level emphasis ensures certification and training currency of sUAS operators, otherwise the sUAS will not reach its true capability as a force-multiplier for a unit's operations. Command-level emphasis should result in standard operating procedures that establish the roles and responsibilities of master trainers, pilots, and the chain of command through battalion and brigade levels.

An additional limitation to sUAS employment occurs during the airspace deconfliction process, and when synchronizing restricted operating zones (ROZs). Again, these processes and procedures must be coordinated and practiced to gain proficiency. Consistent employment of battalion-level graphic control measures on intelligence, surveillance, and reconnaissance overlays significantly aided in synchronizing tower operations. Ultimately, pre-coordination, while not always possible, is the best method of facilitating ROZ deconfliction and enabling simultaneous flights.

Another limiting factor is risk aversion. Many RTUs maintain their sUAS capabilities securely in their battle zone, limiting their range and collection potential. In comparison, the 1-4 IN accepts tactical risk by placing some of its sUAS operators forward with scout elements in the disruption zone or deeper to employ their capabilities fully. For the 1-4 IN, the risk associated with losing contact with a friendly company or the payoff of reconnoitering and targeting enemy positions significantly outweighs the risk faced by forward sUAS teams. To stay competitive, RTUs must adapt tactics that support the targeting and survivability of the brigade as a whole.

Best Practices and Preferred Employment Techniques of the Warrior Battalion

The 1-4 IN uses its three primary sUAS platforms differently, based on their respective capabilities. The rapid launch and return of the Raven system provides a company

commander with quick target identification and the flexibility to maneuver Raven control station sites. The Puma system has a longer range and flight time, allowing for deeper operational views and support to fires as enemy elements enter 1-4 IN kill zones. Both systems have an infrared camera and laser target designation that support the 10-digit grid identification of a target. Depending on environmental factors (such as wind), 1-4

IN sUAS operators prefer using the Raven system in the offense and the Puma system in the defense, although pairing the systems to queue their capabilities has provided significant advantages if a Raven system is engaged. The newly implemented RDASS, which replicates a nonconventional UAS capability, has a high definition camera, but limited range and target support capabilities. UAS operators prefer using this system in a reconnaissance capacity, while in towns or along tree lines, to fully employ the system's abilities and minimize risks associated with detection.

In order to use these platforms, it is vital for the Warrior Battalion to maintain a master trainer. Currently, the 1-4 IN has one master trainer, a staff sergeant, who conducts all standards, currency, and proficiency tasks, and coordinates class IX support for 32 sUAS operators and 13 airframes. The master trainer plays a crucial role in planning and employing the battalion's sUAS capabilities. Alongside the reconnaissance company commander and intelligence section, the master trainer develops a sUAS scheme of maneuver and named area of interest overlay/observation plan. Simultaneously, the trainer coordinates with the installation tower chief to operate multiple sUASs while deconflicting for



Photo by SFC Michael Guillory

SGT Dane Phelps, from 2nd Battalion, 27th Infantry Regiment, 25th Infantry Division prepares to launch the Raven unmanned aerial vehicle during a joint U.S. and Iraqi cordon and search operation.



U.S. Army CW2 Dylan Ferguson, a brigade aviation element officer with the 82nd Airborne Division's 1st Brigade Combat Team, launches a Puma unmanned aerial vehicle June 25, 2012, Ghazni Province, Afghanistan.

live aircraft and fires throughout the training area. Although all of these tasks are important, the master trainer's most important role is instructing and certifying operators.

The master trainer is the only Soldier authorized to instruct and certify new operators. In addition to ensuring all Puma, Raven, and RDASS operators are current with their airframe, the trainer must also track Soldiers scheduled for a permanent change of station or expiration of term of service. Each company must maintain a total of six Puma/Raven operators and five RDASS operators. Therefore, the master trainer must find time between rotations to conduct the 10-day initial qualification course to replenish each company. Upon completion of this course, Soldiers go through an up to 60-day program to progress from mission preparation to mission qualified. After these formal training gates, the experienced operators practice more technical or new TTP gained from recent rotations. The unit trainer and master trainer mold their newest operators to fly unassisted. Outside of a rotation, the master trainer designates evaluation days to test operators on basic knowledge, skills, and emergency procedures required of experienced operators.

Prior to a rotation, the master trainer consolidates certified personnel into a sUAS squad-sized element covering the Puma and Raven systems and RDASS. The squad is divided into two-man sUAS assault teams responsible for specific airframes. Team members either are in military uniform or dressed as innocent civilians to penetrate deep into enemy territory. Most importantly, the teams are either accompanied by a forward observer or personally capable of effectively coordinating fire support, dramatically shortening the sensor-to-shooter timeline.

The night before each rotation, the master trainer and team conduct rehearsals, layouts, and final reconnaissance planning for their initial collection areas. Once the rotation begins, the master trainer takes the new operators into the fight so they can receive on-the-job training. Overseen by the master trainer, new operators construct a ROZ plan, route, flight path, and rules of engagement. After developing the plan successfully, the new operators execute their plan alongside the master trainer. The master trainer briefs experienced operators before operations and mentors them throughout the rotation. Throughout the rotation, the master trainer also links up with the teams

to conduct a rolling after action review and to ensure they maximize their sUAS capabilities.

Once teams are in position, senior team members take charge and shift teams, as required, to provide the best security and overwatch for their positions. Each sUAS operator can fly in different types of environments and terrain. They operate by means of launching, driving, and recovering while mobile, working from rooftops in cities, camouflaging themselves to blend in with terrain, or operating in the tops of trees while working beyond the forward line of protection. At every position, sUAS teams conduct a short reconnaissance and fortify their positions for time to evade if discovered.


At the end of every rotation, the master trainer conducts a 100-percent inventory for each company to annotate all shortages and damages. The master trainer contacts Redstone Arsenal and branch movement control teams to coordinate shipping of replacement parts. When ordered, each replacement part is assigned to a specific company for proper tracking. At this time, the master trainer builds an in-depth after action report sUAS tracker detailing every flight, location, and battle damage assessment from the rotation. This report is submitted to the battalion commander and used for battalion rotational after action reviews. One week later, the master trainer resumes coordination of flights to qualify and progress operators.

Recommendations for Future RTUs

RTUs must embrace and prepare for the sUAS fight through aggressive training, planning, and employment of UAS assets. The following lists concise recommendations for RTUs to implement:

- ◆ Change the mindset—the RTU is fighting in a competitive UAS environment.
- ◆ Implement and train counter-UAS drills, including the consistent employment of cover, concealment, camouflage, and deception.
- ◆ Ensure adherence to OPSEC, and secure and protect all information technology systems.
- ◆ Ensure commanders emphasize and prioritize the certification and training currency of sUAS operators.
- ◆ Train at least two master trainers per brigade and two per battalion (master trainers are not limited by the modified table of organization and equipment); empower them to lead and coordinate their element.
- ◆ Ensure commanders enforce the development and implementation of sUAS standard operating procedures.
- ◆ Incorporate and practice the synchronization of UAS, fires, and maneuver elements at home-station training events.
- ◆ Ensure leaders aggressively employ sUASs and exploit the collected information.

Conclusion

The Warrior Battalion provides the toughest, most realistic threat to train United States and multinational partners. During mission execution, the Warriors constantly learn and refine their skills in the critical areas of the maneuver battlefield, collecting valuable lessons for Army units and our partners. 

Endnotes

1. Former Joint Multinational Readiness Center (JMRC) senior intelligence officer LTC Eric Remoy noted this observation: “AWG training experiments...have been consistent with the findings at JMRC in similar training environments, the training units often ignore proximate UAS and assume it is operating in a friendly capacity.” Eric Remoy, “Summary of Current Counter-Unmanned Aerial Systems Efforts.” (information paper, JMRC, 18 February 2016).
2. “...a combination of artillery and MLRS, with the latter employing top-attack munitions and thermobaric warheads, caught two Ukrainian mechanized battalions in the open. This intensely concentrated fire strike created high casualties and destroyed most of the armored vehicles in a shelling that lasted only a few minutes...without having the means of real-time target acquisition, Ukrainian forces were at a severe disadvantage.” Dr. Phillip A. Karber, “Lessons Learned from the Russo-Ukrainian War, Personal Observations,” (information paper, Georgetown University, July 2015).
3. Scott R. Masson, “Unmanned Aerial Vehicle use in Army Brigade Combat Teams: Increasing Effectiveness across the Spectrum of Conflict,” (master’s thesis, Naval Postgraduate School, December 2006), <http://www.dtic.mil/dtic/tr/fulltext/u2/a462656.pdf>
4. “JMRC assessed that the Combined Resolve V training unit in November of 2015 lacked procedures to inform the tactical formation of friendly overflights as a first step in characterizing the airspace, lacked procedures to feed information from tactical units to higher headquarters about the presence of UAS, and lacked material solutions beyond engaging UAS with small arms and crew-served weapons.”, Remoy, “Summary of Current Counter-Unmanned Aerial Systems Efforts.”

LTC Archambault is the commander, 1st Battalion, 4th Infantry Regiment. He previously deployed to Iraq and Afghanistan where he served as a rifle company commander, maneuver planner, battalion S-3, and brigade S-3. He holds a bachelor of arts from the United States Military Academy in political science and a master of arts in theater operations from the School of Advanced Military Studies.

CPT Peachey is the battalion intelligence officer for 1st Battalion, 4th Infantry Regiment, Hohenfels, Germany. He served as a scout platoon leader during a deployment to Afghanistan and a military intelligence company commander at the National Security Agency. He holds a master of arts in diplomacy from Norwich University.

CPT Hayball is the Grizzly Team intelligence observer-coach-trainer, Joint Multinational Readiness Center, Hohenfels, Germany. His deployments include two to Afghanistan, where he served first as a signals intelligence platoon leader, and second as a Security Force Advisory and Assistance Team advisor. He holds a bachelor of arts in international studies from the University of St. Thomas, Houston.

Ssg Lincoln is the 1st Battalion, 4th Infantry Regiment master sUAS trainer. His deployments include two tours to Afghanistan where he served as a scout team leader, personal security detachment team 1, fire team leader, and squad leader. He holds an associate of arts in criminal justice, and is finishing his bachelor of arts in unmanned systems applications from Embry-Riddle Aeronautical University.

Overcoming One-Handed Punching: Insights on Breaking the Barriers to Integration

by First Lieutenant Ross Stergios Nikides

There is still a tendency in each separate unit ... to be a one-handed puncher. By that I mean the rifleman wants to shoot, the tanker to charge, the artilleryman to fire. ... That is not the way to win battles. If the band played a piece first with the piccolo, then with the brass horn, then with the clarinet and then with the trumpet, there would be a hell of a lot of noise but no music. To get harmony in music, each instrument must support the others. To get harmony in battle, each weapon must support the other. Team play wins. You musicians of Mars ... must come in the concert at the proper place and at the proper time.

—MG George S. Patton Jr.¹

Introduction

On Joint Base Lewis-McChord, northwest Leschi valley, the low rumbling sound of a convoy crescendos into a screech as they round an intersection at a quickening pace toward a small square in the enemy controlled town of Leschi. Two Strykers carrying a platoon of riflemen cordon off the intersections surrounding the square, allowing for two mine resistant all-terrain vehicles carrying a multifunction team (MFT) of intelligence collectors to halt just before their objective. A slight drizzle of rain starts to splatter the team members that just exited their vehicles as they stack alongside the squad of infantrymen on the backside of an internet café. Within seconds, both teams are inside the building securing a high value target and exploiting the café for sensitive information pertinent to stabilizing the town and defeating the growing enemy threat in the valley.

A signal intelligence (SIGINT) collector intercepts radio communications between an observer of the raid and another unknown individual, “Notify the others, we should attack the Americans.” The SIGINT collector immediately analyzes the signal and identifies possible enemy positions, and submits reports instantaneously to the rifle platoon informing them of the potential attack. The platoon leader of Ghost Platoon, 2nd Battalion, 1st Infantry Regiment dispatches a quick reaction force to raid the secondary objectives. The squad, cued by the collector, captures the observer and questions him utilizing the human intelligence (HUMINT) team embedded within their platoon to thwart a possible counter attack.

This series of events executed during the 109th Expeditionary Military Intelligence Battalion’s Table VI certification exercise² presents a perfect example of synchronization described in General Patton’s 1941 speech. When the intelligence assets and the maneuver unit work in full concert, the whole team was able to successfully raid, exploit, and secure multiple targets and objectives crucial to the overall effort within that area of operations. Each member of the collection team completely integrated with the maneuver force and each entity was able to support the others, leading to overall mission success.

This example is one of the few integration successes with intelligence assets and teams working in concert with a supported unit. More often than not, attempts at synchronizing intelligence collection with maneuver operations fall short of desired end states. Examples of this problem range from failures at the strategic level with organizational compartmentalization of information, causing a lack of integration of intelligence, down to the tactical level, where ground based forces do not fully understand capabilities and improperly employ assets or exclude them from mission planning processes altogether.

The failure to integrate the growing number of enablers and support assets in concert with maneuver elements can



A HUMINT collector tactically questions a detainee alongside a squad leader from the rifle platoon during Operation Disrupter's Edge at Joint Base Lewis-McChord, Wash., June, 2016.

Photo by 1LT Michael Norohna

result in lost capabilities, poor resource management, and even worse, mission failure. In today's complex operating environments, state and non-state actors work to unify their actions to "challenge the U.S. ... directly and indirectly," through "an ever-changing variety of conventional and unconventional" strategies. As such, lack of synchronized efforts can have catastrophic, global effects to both strategic and tactical victories on the battlefield.³ Why then does this process fail so often and how can leaders better orchestrate efforts?

This problem set has challenged intelligence leaders over the last half decade and continues to be a point of contention for those seeking to better support maneuver and adapt the Military Intelligence (MI) Corps to meet the requirements of future operating environments. As the Army transitions into a globally responsive force, the focus of the MI Corps training and employment strategies must also transition – a task that continues to be increasingly difficult to execute given resource constraints and the classified nature of intelligence operations.

This article seeks to address how the leaders in the Collection and Exploitation Company, 109th Expeditionary Military Intelligence Battalion have framed this problem set and adapted their resources, personnel, and equipment requirements to tailor a package in support of 1st Stryker Brigade Combat Team, 25th Infantry Division for a future National Training Center (NTC) rotation.

Framing the Problem: Historical Perspectives

To understand how this problem was framed, we must explore the inputs to integration, focusing on how previous leaders built shared understanding, collective experience, and synthesized organizational differences to maximize a full range of capability. By studying historical and anecdotal examples of the integration process, leaders can better understand the importance in overcoming barriers to integration in order to synchronize and orchestrate lines of effort in today's complex operating environments.

The concepts of integration, synchronization, and orchestration are not new. For centuries military theorists have examined these concepts considering them vital components to military principle. Theorists have defined integration as "the full employment of all forces and resources available, maximizing each capability to achieve the objective at the lowest cost."⁴ Similarly, synchronization refers to "timing... not only for the separate operations or tactical actions, but also in the application of forces within a specific action."⁵ In other words, integration efforts bring all the resources to bear, in turn, driving synchronization of all forces and resources, linking them together in space and time for the application of a specific action. When actions are synchronized and coordination efforts allow for maximum employment of force, units take "maximum advantage of an enemy's vulnerability" denying them the opportunity to "regroup and concentrate" their forces.⁶ Integration and synchronization are key principles to planning effective operations against an enemy, allowing leaders to assimilate all assets and coordinate their efforts toward a specific purpose and end state.

BG Russell Honoroe, in an excerpt from *66 Stories of Battle Command*, takes the concepts of synchronization and integration a step further, focusing on the eventual orchestration of efforts as a key piece to effective battle command. For General Honoroe, leaders spend too much time focusing on the syn-

chronization of assets on the battlefield and not enough time focusing on the operational art to orchestrate resources and forces at the right time.⁷ He states that "the problem with focusing synchronization is it suggests working sequentially vice simultaneously" because it only looks at battlefield functions "in terms of time and space."⁸ Sequential planning only goes so far, especially when events on the battlefield occur simultaneously – linear planning and synchronization of resources counteract the ability and "opportunity to throw [the enemy] off balance and wrestle the initiative from him." However, orchestration is the "concept of simultaneous operations, simultaneous execution," starting from synchronization as the building block necessary in order to fully maximize and optimize operations.⁹

In many ways, General Honoroe was correct in his thought process of orchestration as the key principle to mission command. Current Army doctrine on unified land operations accounts for the simultaneous execution of offensive, defensive, and stability tasks, through flexible and empowered mission command.¹⁰ Military leaders have made significant progress to recognizing the intricate nature of future conflict against hybrid threats, but it is often in the *process* and *linkage* of integrating forces, synchronizing their actions, and then orchestrating their efforts to fight *simultaneously* in any operating environment. This so-called integration roadblock challenges leaders and can present significant problems on the battlefield for leaders seeking to fully optimize their force's potential.

Historically, as more enablers are introduced onto the battlefield, the integration roadblock becomes apparent. In World War I, for example, the Russian Army faced significant issues with maximizing force potential while fighting on the Eastern Front in 1916. LCDR Gordon Evans Van Hook writes:

"By 1916 the futile stalemate of the Western Front had been matched by the bloody and often pointless surges of ineffective offensives and counteroffensives on the



General Aleskey Brusilov.

Eastern Front....by sheer weight of numbers they [Russia] had been able to reverse some of the disasters of 1914, but most of the army suffered from gross systemic inadequacies that hindered operational effectiveness...artillery was massed and directed in aimless bombardments that did little damage... Reconnaissance was deplorable, and there was a constant bickering between the artillery, infantry and cavalry...Logistics was a hopeless tangle of bureaucracy and confusion..."¹¹

The Russians possessed the force structure and enabler support to achieve small victories at the operational level. However, their inability to properly integrate them, understand the employment and capabilities of their forces, and in turn orchestrate their efforts, led to complete ineffectiveness as a fighting force. Such ineffectiveness eventually led the Russian Army to its lowest levels of morale and obedience, and ultimate collapse after years of unnecessary carnage and failed operations.

Nevertheless, one Russian military leader, General Aleskey Brusilov, used lessons learned from the Western Front through "exhaustive study" with his staff to develop new tactics based on security and force array.¹² In the past, artillery would conduct a large opening bombardment to signal an attack, often with no tactical objective. Brusilov and his staff decided to better integrate the artillery, opening with small bombings to deceive enemy forces. These allowed ground forces staged in underground bunkers located near the forward line of troops to shock and overwhelm the enemy.¹³ This tactic proved increasingly effective, allowing Russian forces to cause the near collapse of the Austrian Army on several occasions throughout the war. Of course, failure by the northern armies to "integrate the artillery" like Brusilov had, and their "lethargy in coordinating with the South," virtually "guaranteed failure" for the Russian Army. Brusilov's ability to utilize the lessons learned and the time to integrate the Russian force array proved to be largely successful for the army he commanded.¹⁴ He used his staff to develop new tactics and techniques from lessons learned, generating shared understanding of proper employment of Russian enablers to seize the initiative and overwhelm the Austrian Army.

Taking *lessons learned* to build experience and *shared understanding* as inputs to the integration process is key to overcoming the integration roadblock and paving the way for proper synchronization and orchestration of mission command. At the advent of World War II, Nazi Germany's *Blitzkrieg* offensive also drew from lessons learned. From the failed Schlieffen Plan where logistical support did not keep up with troop movement, they developed a plan where offensive maneuver elements were synchronized with rapid logistical support. German blitzkrieg tactics coordinated "tremendous striking power with the capability to support short, stabbing thrusts within 600 miles or so of the German border" while also incorporating "mobile supply and repair teams into the fast columns" to continue sustained operations with lightning speed.¹⁵ Apart from using advances in aerial assets and armored vehicles to overwhelm Belgian, French, and Polish lines, the ability to draw lessons learned from prior operational blunders, proved significant in the overall success of the German strategy.

Overcoming the Integration Roadblock

The historical perspectives illustrate that the larger problem with integration roadblocks lies not necessarily in applying lessons learned or having the right past experiences to orchestrate mission command, but in fundamentally understanding the forces' capabilities and properly linking those capabilities at the right time and place to win. This lack of understanding creates a dilemma for military leaders as they weigh risks, make assumptions, and plan for operations in complex and time-constrained environments. It is close to impossible to be a subject matter expert on every piece of equipment or capability possessed by the Army. However, not having the understanding of those capabilities leads to operational failures, de-synchronization, and causes the one-armed boxing described by General Patton.



A signals intelligence collector maneuvers with a sniper team to a hide site in the town of Leschi during Operation Disrupter's Edge at Joint Base Lewis-McChord, Wash., June 2016.

This dilemma directly affects the process of integration. In making assumptions about unfamiliar capabilities, assets, or general objects in an environment, leaders are taking risks that can lead to inefficiency or improper employment of force. More often than not, a leader will use a force they understand rather than a force or asset they do not. The opening scenario of this article paints a picture of flawless integration, but before any orchestration were to happen, days of cooperation between the MFT and Ghost Platoon were required to learn capabilities, share experiences, and gain a common understanding of the operating environment. Several missions before the Leschi raid resulted in the ineffective use of the MFT, causing lapses in collection and missed opportunities. At the same time, the MFT team leader struggled to accurately portray planning considerations necessary for the team to be operational alongside the rifle platoon.

As a result, the platoon leader was not comfortable taking another seven individuals onto an objective when he first had to manage the risks of safety to his personnel while clearing several buildings. The platoon leader did not believe the MFT enabled his team because of misunderstanding and lack of translation between the teams' members regarding the capabilities of the MFT and the tactics of the platoon. Many missed opportunities passed during operations—opportunities that are key in today's decisive actions.

Framed under these conditions, discussions of how to best integrate a MFT and an Expeditionary Processing,

Dissemination, and Exploitation Platoon (E-PED) from the 109th Expeditionary Military Intelligence Battalion into 1st Stryker Brigade Combat Team's future operation focused first on overcoming the obstacles to communication and helping to train the brigade's leaders on the capabilities of the deploying package. Table VI Gunnery proved that the integration process needed to occur as soon as possible while the historical examples showed that an understanding of the capabilities of each team was necessary to enable leaders at all echelons. The integration roadblock became apparent early in the initial phases of planning as leaders of 1st Stryker Brigade Combat Team stated that they were unfamiliar with the employment of both MI teams in a decisive action environment. Moreover,

the location disparity between the two units allowed for little to no opportunities for combined training, further hindering integration. Understanding that proper integration meant mission success or failure, arrangements were made to eliminate barriers to communication, explain capabilities, and start the integration process by embedding leaders from the 109th Expeditionary Military Intelligence Battalion into 1st Stryker Brigade Combat Team's decision-making process.

In late September 2016, 1st Stryker Brigade Combat Team held a combined planning exercise focused on taking lessons learned from a previous exercise to build capacity at the brigade and battalion staff level for mission planning and command. The platoon leaders from each team, both MI and maneuver, traveled to Fort Wainwright, Alaska and spent the next seven days immersing themselves into the planning process by explaining capabilities and showing proper employment of the teams. Different courses of action for support were discussed over the short exercise. The platoon leaders saw the value added to spending as much time as possible helping staff leaders across all warfighting functions understand how each organizations team enabled them, while also learning 1st Stryker Brigade Combat Team's capabilities and operational vision. A month later, team leadership attended the Leader Training Program at the NTC, Fort Irwin, California to continue initial steps made towards fully integrating the two units. Leaders laid the groundwork for the next level of integration by ensur-

ing both sides understood each other's capabilities. This allowed the 109th Expeditionary Military Intelligence Battalion to build a flexible and adaptive deploying package based off the needs of both units, and gave 1st Stryker Brigade Combat Team leadership a fundamental understanding of the capabilities and support the intelligence enablers could provide.

Conclusion

In order for military leaders to synchronize and orchestrate forces on the battlefield, maneuver forces and enablers must integrate properly through shared experience, understanding of capabilities, and eliminating barriers to communication. Historically, the process of integration hinders the commanders' ability to achieve full force potential as they link together the various tenants of battle command and enablers at their disposal. The same holds true today as the Army transitions its strategic focuses. Recognizing this challenge, leaders from the 109th Expeditionary Military Intelligence Battalion framed options to overcome the integration roadblock. By building shared understanding of capabilities and experience to maximize 1st Stryker Brigade Combat Team, 25th Infantry Division commander's potential on the battlefield, the MFT and E-PED collection teams hope to overcome one-handed punching and facilitate orchestration during the upcoming NTC rotation. ✱

Endnotes

1. Center for Army Lessons Learned (CALL) Handbook 16-12, "Musicians of Mars II" (Fort Leavenworth, KS: CALL, April 2016), iii, <http://usacac.army.mil/organizations/mccoe/call/publications>.
2. Table VI - ICATS training event focused on certifying intelligence collection teams on mission essential tasks and information collection operations.



Photo by 1LT Michael Norohna

Multifunction team members wait for a post-mission brief and to reconsolidate with their maneuver counterparts after conducting a night raid during Operation Disrupter's Edge at Joint Base Lewis-McChord, Wash., June, 2016.

3. U.S. Army Training Circular (TC) 7-100, *Hybrid Threats* (Washington, DC: U.S. Government Printing Office [GPO], 26 November 2010), 1-1-1-2.
4. Gordon E. Van Hook, *Tactical Victory Leading to Strategic Defeat: Historic Examples of Hidden Failures in Operational Art* (Newport, RI: U.S. Naval War College, 22 February 1993), 4, <http://www.dtic.mil/dtic/tr/fulltext/u2/a264169.pdf>.
5. Ibid., 5.
6. Ibid.
7. Adela Frame and James w. Lussier, eds., *66 Stories of Battle Command* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2000), 15, <http://usacac.army.mil/cac2/cgsc/carl/download/csipubs/66stories.pdf>.
8. Ibid.
9. Ibid., 16.
10. U.S. Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations* (Washington, DC: U.S. GPO, 11 November 2016).
11. Van Hook, *Tactical Victory Leading to Strategic Defeat*, 23
12. Ibid., 24.
13. Ibid.
14. Ibid., 26.
15. David C. Rutenberg, "Synchronized Support: An Irrepressible Principle of War", *Air University Review*, January- February 1986, <http://www.au.af.mil/au/afri/aspj/airchronicles/aureview/1986/jan-feb/rutenberg.html>.

1LT Ross S. Nikides graduated and commissioned out of Hofstra University in 2014 with majors in political science, global studies, and history. Lieutenant Nikides previously served as the assistant S-2 for 1-229 Attack Reconnaissance Battalion, 16th Combat Aviation Brigade. He currently serves as a multifunction platoon leader in Bravo Company, 109th Expeditionary Military Intelligence Battalion, 201st Expeditionary Military Intelligence Brigade.



Defensive Cyberspace Operations Intelligence Support

by Colonel David Kim and Colonel James Adams

Introduction

Commanders require properly operated and defended information networks to execute mission command; precision fires; intelligence, surveillance, and reconnaissance; joint logistics; and other necessary warfighting capabilities. Defending those networks requires timely and accurate intelligence support. U.S. Army Training and Doctrine Command Pamphlet 525-2-1, *The U.S. Army Functional Concept for Intelligence*, highlights the need to leverage predictive and operational intelligence to support defensive cyberspace operations (DCO) and Department of Defense information networks (DODIN) so that commanders may focus attention on actions that reduce vulnerabilities. The concept states, "Intelligence staffs and units will support cyber operations by identifying and assessing foreign intelligence threats directed towards command assets and functions. They will consider the threats to the command's information systems and transport layers as part of their overall intelligence support."¹

As highlighted in the recent U.S. Army War College paper, "Tailoring Intelligence Support to U.S. Army DCO and DODIN Operations,"² by Colonel Laura Knapp, intelligence is a critical enabler of successful DCO and DODIN operations. Intelligence support directly contributes to the security of Army networks and freedom of action in cyberspace.

With this backdrop in mind, the U.S. Army Intelligence and Security Command (INSCOM), in close coordination with U.S. Army Cyber Command (ARCYBER), U.S. Army Network Enterprise Technology Command (NETCOM) and the U.S. Army Intelligence Center of Excellence (USAI CoE), is in the process of improving defensive cyberspace operations intelligence support (DCOIS) at four of the Army's Regional Cyber Centers (RCCs). An RCC is the combination of the former Theater Network Operations and Security Center and 1st Information Operations Command's Computer Emergency Response Team elements. The RCC provides non-classified

internet protocol router and secret internet protocol router services to theater Army forces, and depending on location, to theater joint and combined force commanders as well.

U.S. Army Europe Pilot—Building Momentum

The INSCOM commanding general, in concert with Army strategic guidance, prioritized building cyber operational capability as a strategic objective for the command. Given this goal, and a simultaneous request from U.S. Army Europe (USAREUR) for assistance securing their networks, INSCOM initiated a pilot program in USAREUR in October 2015. The purposes of the pilot was to improve all-source intelligence support to defend the USAREUR DODIN from cyber threats; assure USAREUR mission command; and inform Army doctrine, organization, training, material, leadership, personnel, and facilities (DOTMLPF) development as it relates to all-source intelligence support in the cyberspace domain.

The pilot officially began on 1 October 2015, but preparation started months earlier and focused on initial training for participating analysts and development of the initial operating concept. Concept development was a collective effort between the 66th Military Intelligence Brigade—(Theater) (MIB-(T)), INSCOM G-7 (the INSCOM headquarters lead for coordinating and synchronizing the activities of all pilot participants), ARCYBER G-2, NETCOM G-2, USAREUR's 5th Signal Command, and NETCOM's RCC-Europe (RCC-E).

The 66th MIB-(T) was the INSCOM operational lead for the pilot. The brigade established an intelligence fusion cell comprised of seven participating 66th MIB-(T) analysts within workspace provided by RCC-E's facility located on Clay Kaserne, Wiesbaden, Germany. Their mission focus was to provide intelligence in direct support of the RCC-E's Defensive Cyber Operations Division (DCOD).

On a daily basis, the pilot analysts' job was to facilitate an improved understanding of the operational environment and the associated threat actors for the DCOD cyber de-

fenders. The objective was to get the DCOD to “know the adversary” and assist in making informed decisions about how best to protect the networks.

The analysts chosen to participate in this groundbreaking mission were Soldiers from across the brigade who volunteered and went through an interview process to establish their interests, aptitude, and motivation. Led by a Chief Warrant Officer Two, they possessed a mix of skills—signals intelligence, all-source intelligence, and counterintelligence. They all required additional operational cyber training specifically tailored to their new duties. The ARCYBER G-2 developed a course syllabus for a two-week mobile training team (MTT) to support this requirement. In August 2015, the MTT went to Germany to teach the analysts the basics of intelligence collection and analysis in cyberspace. A live environment training (LET) opportunity quickly followed at Fort Belvoir, Virginia, again conducted by ARCYBER G-2. The LET exposed the analysts to ARCYBER and INSCOM organizations that would support them and allowed them to observe their counterparts firsthand in the Army Cyber Operations Intelligence Center, ARCYBER Analysis and Control Element, and ARCYBER G-2X.

Teaming with the DCOD began almost immediately and focused on the basics, such as answering the questions “what is the operational environment?” and “what are the commander’s priority intelligence requirements that will drive analysis and production efforts?”

Though fundamental questions, answering them required thoughtful consideration. From the beginning, it was evident that this new merger of intelligence analysts with DCOD network defenders required a change in culture. Operations and intelligence integration within maneuver units is nothing new. The performance of any infantry, armor, special operations, or other unit depends on a close working relationship between the S-2 and S-3. However, the pilot immediately highlighted the fact that operations and intelligence integration in cyberspace within the RCC was a new approach requiring a different outlook by those involved. RCC directors are not just service providers; they are the maneuver commanders of the cyberspace domain. Like other maneuver commanders throughout the Army, they will depend on a military decision-making process supported by their intelligence team. In recognition of the importance of the RCC director position, it was recently added as a lieutenant colonel centralized selection list position.

Adding to the challenge of integrating an intelligence team into the RCC has been the integration of the team into the broader, and rapidly emerging, Army cyber intelligence en-

terprise. The start of the pilot coincided with the ARCYBER G-2 development of a concept of operation (CONOP) describing cyber intelligence support at echelon. Originally published in April 2016, the CONOP defined broad missions, functions, roles, and responsibilities. Revised in June 2016 (V.2, dated 31 May 2016), the pilot has significantly helped inform and refine intelligence support operations at the tactical level (RCC/DCOD).


Documenting Lessons Learned

Another objective of the pilot was to document lessons learned to inform Army DOTMLPF capabilities development and long term resourcing decisions. USAICoE, with the U.S. Army Cyber Center of Excellence and INSCOM support, is leading the effort to capture these insights and emerging lessons learned over the course of the pilot. The DOTMLPF assessment will provide a means to determine enduring solutions for the challenges posed by the evolving cyberspace domain. It will also help inform and support Force 2025 and Beyond, the Army’s strategy to ensure the future joint force can win in a complex world, across the full spectrum of military operations. USAICoE is currently coordinating a draft assessment with the stakeholder community.

Advancing Support to Other Theaters

The pilot officially ended on 30 September 2016. However, the mission continues, and based on positive feedback from the European pilot, the commanding general of INSCOM provided guidance to expand support to U.S. Army Pacific (USARPAC), U.S. Forces Korea (USFK), and U.S. Army Central (ARCENT). INSCOM leveraged the existing military workforce from MIB-Ts in response to the demand and provided an interim capability until the Army prepares a long-term solution. DCOIS efforts supporting USFK began on 1 May 2016, and efforts supporting USARPAC and ARCENT began on 1 August 2016. At RCC-E, the end of the pilot marked the transition of participants to an enduring DCOIS operational mode.

Conclusion

This initiative is paying early dividends in providing better defense of the DODIN and assuring mission command today. It is essential to adapt intelligence support to enhance the security of Army networks and maintain the Army’s freedom of action in cyberspace. The Army intelligence corps must be bold and innovative in its approach, or we risk the failure to provide effective intelligence to support and drive cyber operations in the environment as it now exists. It might take some time to include fully the pilot’s findings across all Army doctrine and resource planning, but -- in this drive -- intelligence must be out front. 

Endnotes

1. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-2-1, *The U.S. Army Functional Concept for Intelligence* (Fort Eustis, VA: TRADOC, 13 October 2010), 46.
2. Laura Knapp, "Tailoring Intelligence Support to U.S. Army DCO and DODIN Operations" (Carlisle, PA: U.S. Army War College, 1 March 2015).

COL David Kim is the assistant chief of staff, G-7, U.S. Army Intelligence and Security Command. His command assignments include Headquarters and Headquarters Company, 34th Support Group, Yongsan, Republic of Korea and Minneapolis U.S. Army Recruiting Battalion. Colonel Kim held key staff assignments as S-3 and executive officer 527th Military Intelligence Battalion, (Field Station, Korea) 501st Military Intelligence Brigade; intelligence program analyst, Program Analysis and Evaluation, Army G-8, Pentagon; planner, J-5, U.S. Cyber Command; director, Force Modernization, J-2, United States Forces Korea; joint staff officer, Defense Intelligence Operations Coordination Center, Washington DC; and operations officer, Joint Intelligence Operations Center - Afghanistan, Operation ENDURING FREEDOM Kabul, Afghanistan.

COL James Adams is the deputy G-2, U.S. Army Training and Doctrine Command. His previous assignment was as G-2, U.S. Army Cyber Command. His command and staff positions include battalion S-2, brigade S-2, division G-2 staff, brigade commander, analysis and control element chief, military intelligence battalion S-3 and executive officer, executive officer to the PAED-Army G-8, and ACoS, G-2, 1st Infantry Division. Colonel Adam's assignments include three tours with the 1st Infantry Division to include Operations DESERT SHIELD/STORM, Implementation Force and Stabilization Force - Bosnia, and Operations IRAQI FREEDOM/NEW DAWN. He also served in the 513th Military Intelligence Brigade during Operation IRAQI FREEDOM and on Army Staff.

Contributors:

COL (Ret.) Steve Stewart currently serves as the senior program analyst for the Office of the Assistant Secretary of the Army Acquisition, Logistics, and Technology Special Programs Directorate. Before retiring from the Army in 2011, Colonel Stewart served as the division chief, Battle Command Division, LandWarNet Battle Command, Army G/3/5/7 (Pentagon). His other key staff assignments include strategist, Office of the Chief of Staff of the Army (Pentagon); director, Intelligence Evaluation Directorate, Army Evaluation Center, Army Test and Evaluation Command; and chief, Intelligence Transition Team, Multinational Forces Iraq. He also served as commander of the 742nd Military Intelligence Battalion, 704th Military Intelligence Brigade.

COL (Ret.) Paul Seitz currently serves as a senior associate for intelligence support to cyber operations within the U.S. Army Intelligence and Security Command Capability Development Directorate. Before retiring from the Army in 2014, Colonel Seitz served as chief, Operations Division, Office of Collection Management and Targeting, Defense Intelligence Agency; chief, Current Operations and Plans Division, Defense Intelligence Operations Coordination Center, Defense Intelligence Agency; deputy director and chief of staff, Iraq Training and Advisory Mission - Intelligence, Baghdad, Iraq.

LTC (Ret.) Jan Army currently serves as a senior associate for intelligence support to cyber operations within the U.S. Army Intelligence and Security Command (INSCOM) Capability Development Directorate (G-7). He previously worked on other technology and quick reaction capability initiatives within INSCOM's G-7 and Futures Directorate. Before retiring from the Army in 1997, Colonel Army served in leadership positions in the Army's first advanced capability technology demonstration, joint precision strike demonstration, and the precursor to the information warfare acquisition program.

Intelligence Training Management: Noncommissioned Officer Training Strategies

by Chief Warrant Officer Four John K. Kennedy

Introduction – The Scenario

Somewhere in the Army, SGT Schmedlap a military occupational specialty (MOS) 35F, intelligence analyst, is assigned to a military intelligence company (MICO). He is the senior noncommissioned officer (NCO) within the collection management section of the information collection platoon. The collection management section is at a little over 60 percent strength with recent losses of personnel, and SGT Schmedlap, has just received a warning order to prepare his section for a unit training exercise.

There are several challenges ahead for SGT Schmedlap. He must prepare a section training plan, and he has questions regarding how and on what tasks to train his Soldiers to support the mission.

Developing the Training Plan

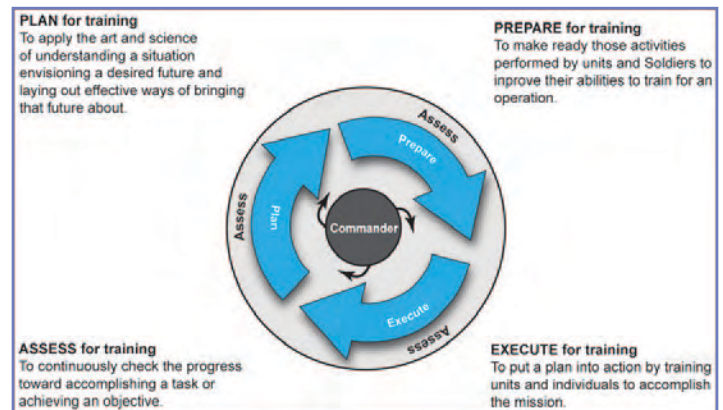
There are several publications available for SGT Schmedlap to consult for training guidance. Some of them are:

- ◆ Army Doctrine Reference Publication (ADRP) 7-0, *Training Units and Developing Leaders*. Introduces the concepts of training and leader development.
- ◆ Field Manual 7-0, *Train to Win in a Complex World*. Expands on the concepts introduced in ADRP 7-0.
- ◆ Training Circular 2-19.400, *MI Gunnery for the Military Intelligence Company of the Brigade Engineer Battalion*. Provides guidance for the MICO to conduct unit training management and planning.
- ◆ Soldier Training Publication (STP) 21-1-SMCT, *Soldier's Manual of Common Tasks: Warrior Skills Level 1*. Provides a training plan and task summaries for warrior skill level 1 common tasks that support unit wartime missions.
- ◆ STP 21-24-SMCT, *Soldier's Manual of Common Tasks: Warrior Leader Skill Level 2, 3, and 4*. Provides a training plan and task summaries for warrior leader skill levels 2 through 4 common tasks that support unit wartime missions.

- ◆ STP 34-35F14-SM-TG, *Soldier's Manual and Trainer's Guide for the Intelligence Analyst MOS 35F Skill Level 1/2/3/4*. Provides training objectives in the form of task summaries to train and evaluate Soldiers on critical tasks that support unit missions during wartime.

The Army Training Network (<https://atn.army.mil/>) and the Combined Arms Training Strategy, accessible through the Army Training Network, are Army websites that can be consulted as sources of knowledge for training aids, and tasks, conditions, and standards for Army individual and collective tasks.

Planning for training begins with the initial training guidance from the commander. This guidance helps determine the battle focus for the unit with the commander's training priorities. The staff will develop a unit training plan (UTP) to conduct the training in the time given. The UTP will list the training events that will develop the unit's proficiency. Each event follows a Plan, Prepare, Execute, and Assess cycle.¹

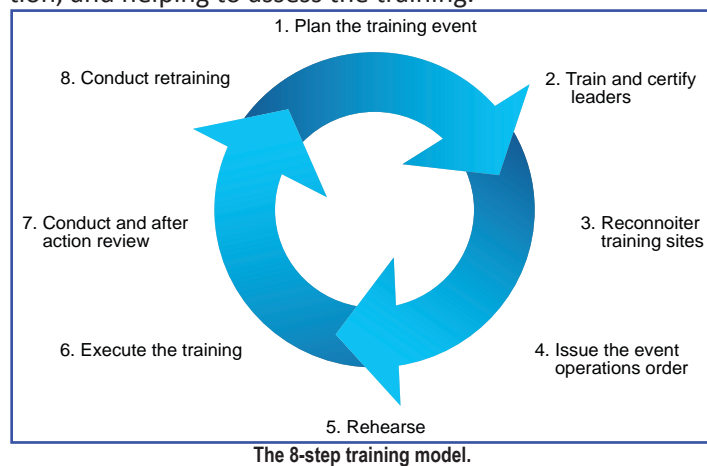


Operations Process.

From the UTP, SGT Schmedlap can identify what his requirements are to have the training completed in the time allocated.

SGT Schmedlap needs to know what the unit collective training tasks are. The UTP, and the commander's guidance, will tell him about the commander's training priorities. In the scenario, a field training exercise or warfighter exercise

is a top priority for the commander. Tasks of the collection management section supporting the MICO's operations will be part of that training. SGT Schmedlap is aware that his section has new Soldiers with different skill levels. They will need training too, in order to become proficient. SGT Schmedlap knows that SPC Smith is the section expert on the Distributed Common Ground System-Army (DCGS-A). SGT Schmedlap will need to ensure that all section personnel receive training on DCGS-A operations, not rely exclusively on SPC Smith. SGT Schmedlap's role will be helping the MICO staff identify the training for his section, and preparing the Soldiers for the training, ensuring execution, and helping to assess the training.



Planning the Training Event

At a company or platoon level, a training model that helps plan training is the 8-step training model.²

It can be an effective planning and execution tool to ensure the major activities and steps are accomplished. The 8-step training model is not specific to any MOS. It is applicable to all Army tasks and skill levels.

When units receive a training mission, they receive a warning order (WARNORD). The first step of the 8-step training model is to plan the training event. The warning order is the start of the planning process. The order helps to understand the 5W's of the training. In the scenario, knowing the commander's guidance, and having the WARNORD, SGT Schmedlap can understand how Step 1-Plan the training event, feeds Step 2-Train and certify leaders, and the subsequent steps. SGT Schmedlap will gather the references that help identify the tasks, conditions, and standards of the training.

Section tasks are nested within tasks from the unit mission essential task list, or can be those tasks necessary for an assigned mission. This influences the long-range training plan. The leadership will conduct backward planning to identify other significant training events that are on the horizon. The leadership will identify unit training priorities based upon

the commander's guidance, and focus training into those areas. The NCO's will put that plan into action based upon the training priorities, and the timelines.

SGT Schmedlap will conduct his own backward planning in order to prepare the section for training, and ensure that the equipment for his section can be ready and available if the training is to occur at a different location. He will ensure coordination for automation, equipment, administrative supplies, and other requirements for his section to conduct training.

An example critical skill for the MICO collection management section found in STP 34-35F14-SM-TG, *Soldier's Manual and Trainer's Guide for the Intelligence Analyst MOS 35F Skill Level 1/2/3/4*, would be Information Collection and ISR Tasks. This has several individual skill level tasks that are inclusive to this critical skill. One example task would be to lead the development of information collection products. The task summary contains information Soldiers must know and skills they must perform to standard.

SGT Schmedlap would read the tasks, conditions, and standards, and would plan resourcing for the performance steps, and arrange for the conditions to be present to train the Soldiers.

Preparing for the Training

The second step of the 8-step training model is to train and certify leaders. The commander's guidance can help SGT Schmedlap determine how to deliver the section training. He can coordinate with the MICO staff to identify who can lead the training. Training execution can be through a train-the-trainer approach, or other methods (i.e., using instructors from higher commands to teach the training).

The train-the-trainer method utilizes a qualified trainer that can provide instruction to other Soldiers to conduct a task to standard. However, if utilizing instructors from a higher command headquarters, then SGT Schmedlap will want to have the training references on hand for himself, the trainers, and the evaluators. The references should also identify PASS and FAIL criteria. He will want to ask about any certifications as part of the training for the Soldiers. The certification will feed into future training iterations and decisions, such as if any certifications will expire during a major exercise, combat training center rotation, or deployment.

The third step of the 8-step training model is to conduct a reconnaissance of the training site. A question answered during the planning process is where to conduct the training. Will it be a field environment, classroom environment, or in a simulated virtual, interactive environment? A virtual, interactive environment may have specific vignettes, and

scenarios to support training objectives. SGT Schmedlap will want to be familiar with the area, and he will want the Soldiers to be familiar with the area too.

The fourth step of the training model is for the commander to issue an operations order (OPORD). The OPORD contains information on tasks to be trained, the training objectives, and mission statement. SGT Schmedlap should use the OPORD as a reference to inform his section of the training event now that he knows the commanders end state objective. He will also be on the alert for fragmentary orders that could affect the training guidance, timetable, or training tasks.

The fifth step is to rehearse. Rehearsals are to ensure that Soldiers understand planned training and their responsibilities. Rehearsals also address how trainers intend to evaluate Soldiers performance. SGT Schmedlap would use this time to practice training tasks with his section. Each Soldier would be reviewing the tasks and ensuring they understand the performance steps and standards. During rehearsal, all requested materials and equipment to support the training should be in place. This is the time to resolve any remaining deficiencies.

Executing the Training

The sixth step of the 8-step training model is training execution. Training, regardless of the task, requires adequate preparation, presentation, and practice for Soldiers, and it is finished with a thorough evaluation. Executing the training is ensuring that the tasks, conditions, and standards identified for training are met. Other equally important factors are that the training event occurred as planned and that a majority of Soldiers participated.

Assess the Training

The seventh step of the 8-step training model is to conduct an after action review. Training is assessed both during and after it is conducted. The AAR is a guided discussion of the unit's performance from the start to the end of the training event. Its objective is to improve future perfor-

mance. The AAR has a facilitator who directs questions and records responses from the participants. Identification of unit strengths for sustainment and weaknesses that need to improve is the end state objective. The commander's judgment of how the unit performed, and the ability to accomplish the mission determines how the commander assess success of training.

SGT Schmedlap would get feedback from his Soldiers during execution of the training. He should also identify those insights that would make the next iteration of training better. SGT Schmedlap's overall AAR comments should address if the Soldiers within his section understood the training objectives, and if the training helped them to achieve proficiencies on their tasks.

The final step of the 8-step training model is to conduct retraining. Retraining occurs when Soldiers have failed to perform tasks to standard and training objectives are not met. This step is most important and should not be neglected. Units need to retrain tasks before the conclusion of the training event not wait for another training opportunity.

Conclusion

As the Army continues to draw down its forces, more Soldiers will be leaving the Army and taking with them the institutional knowledge that has been acquired over the years. The effect will be greater responsibility placed on lower ranks of both officers and NCOs. Junior NCOs carry the responsibility of training Soldiers, and will be expected to be more effective in their positions. How they train future MI Soldiers for tomorrow's missions begins with having the right focus for training success today. ✨

Endnotes

1. U.S. Army Field Manual (FM) 7-0, "Conducting Training Events." in *Train to Win in a Complex World* (Washington, DC: Government Printing Office [GPO], 5 October 2016), 3-1 – 3-7
2. FM 7-0, *Train to Win in a Complex World*, 3-3

CW4 John Kennedy is a senior analyst for the Concepts Evaluation Branch, Capabilities Development Integration Directorate, U.S. Army Intelligence Center of Excellence, Fort Huachuca, Arizona. Previous assignments include collection management senior analyst G-2, 2nd Infantry Division; Non-Lethal Effects, Special Operations Task Force 82, Herat Province, Afghanistan; and Afghan Reachback Team, 1st Information Operations Command. CW4 Kennedy holds a bachelor of arts from the American University, Washington DC, and a master of science from Adelphi University, Garden City, New York.



TEAM Nighthawk: BEST MILITARY INTELLIGENCE COMPANY IN U.S. ARMY FORCES COMMAND FOR FY 16

by Captain Young K .Kim



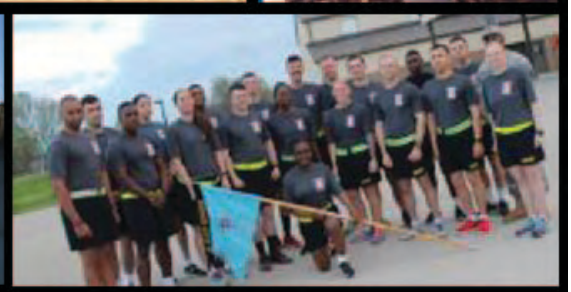
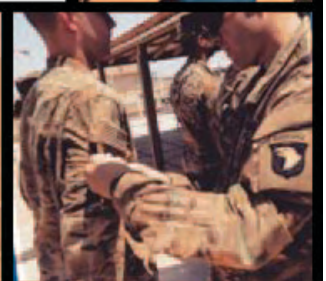
The MG Oliver W. Dillard Award honors the most outstanding company-size military intelligence (MI) unit assigned to a brigade combat team. Although MG Dillard was an infantry officer during the Korean and Vietnam Wars, he was a decorated battalion S-2 in Korea and became U.S. Forces Command's (FORSCOM's) first deputy chief of staff for intelligence (G-2) in 1973. Continuing his service as an infantry officer within a MI functional area, he promoted the use of intelligence Soldiers and units at the tactical level as the senior intelligence officer in U.S. Army Europe from 1975-1978. MG Dillard is a Thomas W. Knowlton Award for Intelligence Excellence recipient, a member of the Army's Military Intelligence Corps Hall of Fame (2012) and the Alabama Military Hall of Honor (2013), and symbolizes the promotion of esprit de corps and professionalism in military intelligence units throughout FORSCOM.

COL Ryan M. Janovic, FORSCOM Deputy Chief of Staff, G-2, officially designated Delta Company, 39th Brigade Engineer Battalion, 2nd Brigade Combat Team, 101st Airborne Division (Air Assault) Fort Campbell, Kentucky as the MG Oliver W. Dillard Award recipient for Fiscal Year 2016. Over the past year, CPT Brent Kurutz (Past), CPT Brandon Maguire (Present), and 1SG Jamey Watson led the Soldiers of the "Nighthawk" Company with a sense of exceptional commitment. As the best MI Company assigned to a brigade combat team, they maintained the highest state of readiness and a thorough understanding of potential environments worldwide. Team Nighthawk's foundations of excellence included varying operational and garrison oriented efforts to support combat operations, increase capabilities, and raise esprit de corps.

While training at the Joint Readiness Training Center prior to their Operation Inherent Resolve (OIR) rotation, they received high praise for having the best signals intelligence (SIGINT) section in the last three years. As the first and only U.S. Army Forces Command SIGINT section with digital network intelligence (DNI) converged analytics capability in support of OIR, they gained and maintained a reputation as a highly trained intelligence team. Their SIGINT section used its converged analytics cell to provide DNI support to multiple echelons above brigade and various organizations; the section supported both operations for OIR and Operation Spartan Shield (OSS).

Furthermore, the Nighthawk's human intelligence collection teams produced intelligence reports leading to multiple dynamic strike packets; all-source analysts working in the brigade intelligence support element produced 270 daily intelligence summaries disseminated throughout Iraq; the intelligence and electronic warfare section provided support to several outside organizations, facilitating key software and intranet capabilities for both OIR and OSS; and lastly the tactical unmanned aerial systems platoon flew thousands of successful flight hours supporting their organic brigade and separate task forces with full motion video and laser designator support. As a result of their thoroughness, a significant number of targets were destroyed.

Team Nighthawk serves as a role model for other U.S. Army Forces Command units and U.S. Army intelligence professionals. The company embodies the courage and dedication to duty representative of MG Oliver W. Dillard's service to U.S. Army Forces Command and the U.S. Army. ✨



Moments In MI History

Intelligence and the Japanese Attack on Pearl Harbor

by Lori S. Tagg, USAICoE Command Historian

In the months leading up to December 1941, with war raging in Europe, the President of the United States and the Japanese Emperor negotiated for peace in the Pacific. These efforts had been largely unsuccessful. On Dec. 6, 1941, the Army's Signal Intelligence Service (SIS) intercepted a communication from the Japanese government to its delegation in Washington, D.C. The SIS decrypted the first 13 parts of the message spelling out Japanese claims of American transgressions in the Far East. At 5:00 a.m. Dec. 7, the 14th and final part of the message arrived, declaring "The Japanese Government regrets to have to notify the American Government that in view of the attitude of the American Government it cannot but consider that it is impossible to reach an agreement through further negotiations." War was imminent.

The "Fourteen Part Message" had been transmitted using the Japanese diplomatic code referred to as the Purple system. Breaking this code had eluded the best efforts of SIS cryptographers until August 1940, when SIS was finally able to read Purple message traffic between the Japanese government and its official representatives in the United States. The process of decoding and translating Purple messages and disseminating the resulting intelligence (known as Magic) was long and tedious due to volume of traffic, the difficulty of the code, the limited number of cryptographers and Japanese linguists, and the security surrounding Purple. Of paramount concern was ensuring the Japanese did not learn the United States had broken the code, so access to the Magic material was granted to only a few top officials.

In the early morning of Dec. 7, SIS immediately recognized the import of the Fourteen Part Message, and after informing the President, the chief of staff of the Army alerted the commanders of both the Hawaiian and Philippine departments that the potential for a Japanese attack was high, although the target was still unknown. Given the sensitivity of the message, it had to be sent by telegraph, a process hampered by Sunday office closures. The message reached Honolulu at 7:33 a.m. Hawaii-time and was dispatched by bi-

cycle messenger to Fort Shafter. Half way to his destination, the messenger sought cover in a roadside ditch when the Japanese began its aerial bombardment. He did not reach Fort Shafter until 11:45 a.m. and, by the time the message was decoded and delivered to the adjutant general's office, the time was 2:58 p.m. and the attack was over. Eighteen U.S. ships and 188 aircraft were damaged or lost; human casualties included 2,335 service members and 68 civilians with another 1,178 wounded. Additional losses were suffered during simultaneous attacks on Thailand, Malaya, Singapore, Guam, Hong Kong, Wake, and the Philippine Islands.

Through the benefits of hindsight, much has been written about the intelligence failures leading to the attack on Pearl Harbor. To be clear, none of the Magic decrypts precisely laid out Japan's intent to attack Pearl Harbor. Nevertheless, U.S. communications security certainly contributed to the failure to inform ground commanders of the potential for attack in a timely manner. Yet, it was not the only contributing factor. Both the Army and Navy intelligence organizations had been undermanned since World War I, and growth in 1941 came too late to reap the advantages that would have been available from a long established intelligence collection effort. When Japan restricted accessibility to foreign military observers in 1941, the U.S. ambassador warned the State Department of its limited "ability to give substantial warning" of possible naval or military operations.

Additionally, the Army's Military Intelligence Division (MID) concentrated on the Japanese Army, leaving Japanese naval operations to the U.S. Navy. With all evidence indicating the Japanese Army would continue its aggression in the Southwest Pacific, MID intelligence estimates, myopically, focused on that region. Furthermore, dismissing its own recently approved doctrine of the period, MID admittedly overlooked Japanese capability to launch a carrier-borne air assault on Hawaii, instead evaluating the enemy's intentions. Fixated on a most likely course of action in the Southwest Pacific, neither MID nor the Office of Naval Intelligence ap-

parently presented an attack on Pearl Harbor as a real possibility. After the war, General Sherman Miles, the assistant chief of staff, G-2, lamented, “We underestimated Japanese military power...judged largely on her past record.... We had a yardstick. We had no reason to doubt our yardstick’s approximate accuracy. Yet it was wholly false.”

The blame for the attack on Pearl Harbor cannot be laid solely on intelligence failures. The Pearl Harbor investiga-

tions affixed plenty of blame to faulty leadership, inflexible policies and procedures, and overall complacency after more than two decades of peace. These same investigations, however, called attention to the long overlooked concepts that intelligence work not only required expert personnel and continuity in time of peace, but that it also should be recognized as an essential function of command. ✨



National Archives

The most iconic photo of the Pearl Harbor attack showing the USS Arizona listing after being hit during the Japanese air assault.



Contact and Article Submission Information



This is your professional bulletin. 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.
- ◆ 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 security officer/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.

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:

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: 201400-000